*Action Concertée Incitative*

SECURITE INFORMATIQUE

*Elaboration d'une DEmarche et d'outils pour la Modélisation Informatique, la validation et la restructuration de réglementations de « sûreté » (sécurité), et la détection des biais dans les aéroports*

Octobre 2003 - janvier 2007

# EDEMOI

## Rapport Final

*Yves Ledru*

**Référence : rapport final**

**Date : octobre 2006**

ONERA CENTRE DE TOULOUSE — Cnam CONSERVATOIRE NATIONAL DES ARTS ET METIERS — TELECOM PARIS école nationale supérieure des télécommunications — lacl — LIFC — LSR-IMAG

**Informations sur le projet**

| | |
|---|---|
| Nom du projet | EDEMOI |
| Site Web | http://www-lsr.imag.fr/EDEMOI/ |
| Partenaires | DPRS, ONERA centre de Toulouse |
| | Laboratoire CEDRIC, CNAM Paris |
| | GET/ENST, Département Informatique et Réseaux, Paris |
| | Laboratoire LACL, Université Paris 12 |
| | Laboratoire LIFC, Besançon |
| | Laboratoire LSR, IMAG, Grenoble |

**Action Concertée Incitative - Sécurité Informatique**

***Projet EDEMOI***

*Elaboration d'une DEmarche et d'outils pour la MOdélisation Informatique, la validation et la restructuration de réglementations de "sûreté" (sécurité), et la détection des biais dans les aéroports.*

*An Approach to Model and Validate Airport Security*

# Final Report

*Yves Ledru (LSR/IMAG)*

October 30, 2006

# Contents

**1 Participants** **2**
1.1 Teams involved in the project . . . 2
1.2 Members of the teams who participated to the project . . . 3

**2 Summary of the project, results, and advances** **4**
2.1 Results . . . 5
2.2 Collaboration with civil aviation authorities . . . 6

**3 Project report** **6**
3.1 Activity 1 - Scope of the study . . . 6
3.2 Activity 2 - Identification of property types to model and analyze airport security . . . 7
3.3 Activity 3 - Graphical Models Engineering . . . 8
3.4 Activity 4 - Formal Models Engineering . . . 9
3.5 Activity 5: Animation and Test generation . . . 11
3.6 Activity 6: Impact analysis . . . 13

**4 Deliverables** **13**

**5 Visibility of the project** **14**
5.1 Visibility by the civil aviation authorities . . . 14
5.2 Visibility by the scientific community . . . 15

**6 Perspectives** **15**

**7 Conclusion** **15**

**8 Publications** **16**
8.1 Deliverables . . . 16
8.2 Publications directly linked to the project . . . 16
8.3 Related publications . . . 17

**9 Civil aviation documents** **20**

**10 Other References** **20**

# 1 Participants

## 1.1 Teams involved in the project

- Centre d'Etude et de Recherche en Informatique du CNAM (CEDRIC) équipe d'accueil 1395
- GET-ENST : Groupe des Ecoles des Télécommunications - Ecole Nationale Supérieure des Télécommunications
- Laboratoire d'Algorithmique, Complexité et Logique (LACL), Université Paris 12
- Laboratoire d'Informatique de l'Université de Franche-Comté (LIFC) - CNRS - INRIA Projet Cassis
- Laboratoire LSR/IMAG - Université Joseph Fourier, Equipe VASCO
- ONERA, Centre de TOULOUSE, Département Prospective et Synthèse (DPRS)

**Significant change in the consortium** Régine Laleau was initially affiliated with CEDRIC/CNAM and joined the LACL laboratory.

**Significant change in the project duration** The project was extended until january 2007.

## 1.2 Members of the teams who participated to the project

| | | |
|---|---|---|
| **CEDRIC/CNAM** | David Delahaye | MCF CNAM |
| | Véronique Donzeau-Gouge | PR CNAM |
| | Catherine Dubois | PR CNAM |
| | Jean-Frédéric Etienne | PhD Student MAE |
| | *Title of the thesis* | *Formalisation de réglementations concernant la sécurité des aéroports en Focal* |
| | *Dates* | *January 2004 - PhD defense planned in 2007* |
| **LACL** | Régine Laleau | PR Univ. Paris-12 |
| **GET/ENST** | Sylvie Vignes | MCF ENST |
| **LIFC** | Bruno LEGEARD | PR Univ. Franche-Comté (until december 2005) |
| | Fabien PEUREUX | MCF Univ. Franche-Comté (until december 2005) |
| | Fabrice Bouquet | MCF Univ. Franche-Comté (since september 2005) |
| | Séverine Colin | PhD Student |
| | *Title of the thesis* | *Procédures de recherche en génération de tests à partir de modèles de spécifications.* |
| | *Dates* | *January 2004 - November 2005* |
| | Fabien NICOLET | Engineer (2003-august 2004) |
| | Mathilde REHFUSS | Engineer (2003-December 2005) |
| **LSR/IMAG** | Didier Bert | CR CNRS |
| | Yves Ledru | PR Univ. Joseph Fourier |
| | Lydie du Bousquet | MCF Univ. Joseph Fourier (since october 2005) |
| | Akram Idani | PhD Student MENRT |
| | *Title of the thesis:* | *B/UML : Mise en relation de spécifications B et de descriptions UML pour l'aide à la validation externe de développements formels en B* |
| | *Dates* | *October 2003 - PhD defense planned in December 2006* |
| | Hector Ruiz | PhD Student |
| | *Title of the thesis:* | *Sémantique des systèmes d'événements. Application à la spécification de systèmes distribués avec la méthode B.* |
| | *Dates* | *October 2002 - PhD defense planned in 2006* |
| | Ansem Ben Cheikh | Student of the Ecole Polytechnique de Tunisie (9 months in 2004 and 2005) |
| | Olivier Bert | EPITA Student (3 months in 2004) |
| | Thi Thu Minh Nguyen | Master 2 Student (4 months in 2004) |
| **ONERA/CdT** | Michel Lemoine | ONERA |
| | Olivier Carton | stagiaire CNAM (12 mois 2003-2004) |

## 2 Summary of the project, results, and advances

The security of civil aviation is governed by international standards and recommended practices, such as Annex 17 of the International Civil Aviation Organisation (ICAO). A key element of aviation security is airport security, which prevents weapons and other dangerous objects from being brought on-board an airplane. The quality of airport security depends on

(a) the quality of these standards

(b) the conformance of a given airport to these standards.

The EDEMOI project[1] was sponsored from 2003-2006 by the ACI Sécurité Informatique. EDEMOI aimed at applying modeling techniques from the Computer Science community to address these two problems. The EDEMOI approach builds on two kinds of models (Fig. 1):

- Graphical models, such as UML class diagrams, are prepared by model engineers on basis of the international standard. Certification authorities, i.e. experts in civil aviation, are expected to read and validate such models.
- Formal models, i.e. B and Focal specifications, are prepared by the model engineers and used for in depth analysis of the standard, and the generation of test scenarios. Formal models are not expected to be understood by certification authorities, therefore, there must exist a strong link between them and the graphical models.

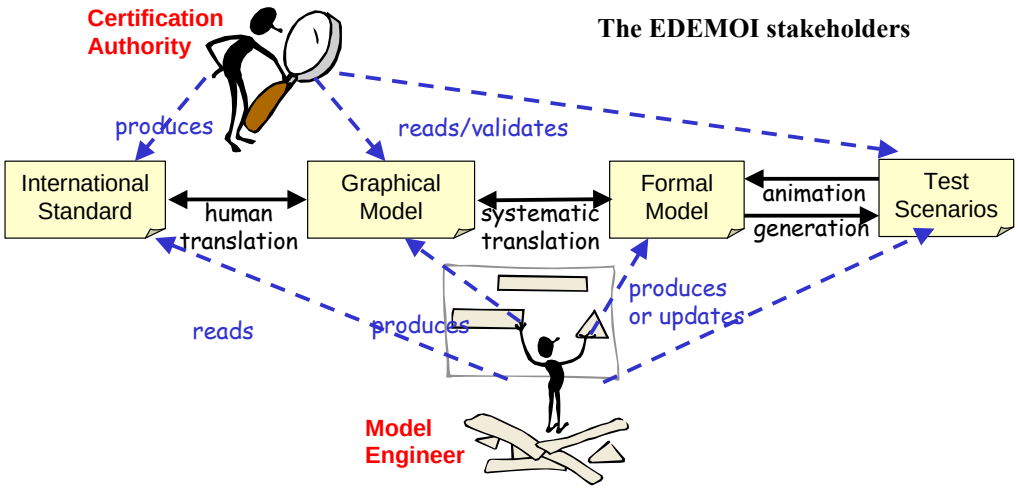


Figure 1: The EDEMOI stakeholders

A difficult point in the EDEMOI approach is the validation of models by certification authorities. Our interactions with experts of two international organisations (ICAO/OACI, International Civil Aviation Organisation, and ECAC/CEAC, European Civil Aviation Conference) showed that these experts have various backgrounds ranging from lawyers to engineers, and that a sufficient proportion of them were able to read

[1] http://www-lsr.imag.fr/EDEMOI

elementary constructs of class diagrams (classes, relations). They can also understand test scenarios, which appeared during the project as a second way to validate the formal models.

EDEMOI focused on the modelisation of Annex 17 [ICA02], which is the ICAO standard that rules all international airports for commercial aviation. It proposed a process (Fig. 2) for the identification of security properties, the production of graphical (UML) [BRJ99] and formal (B and Focal) models of this document, and initiated a test generation activity from the formal model.

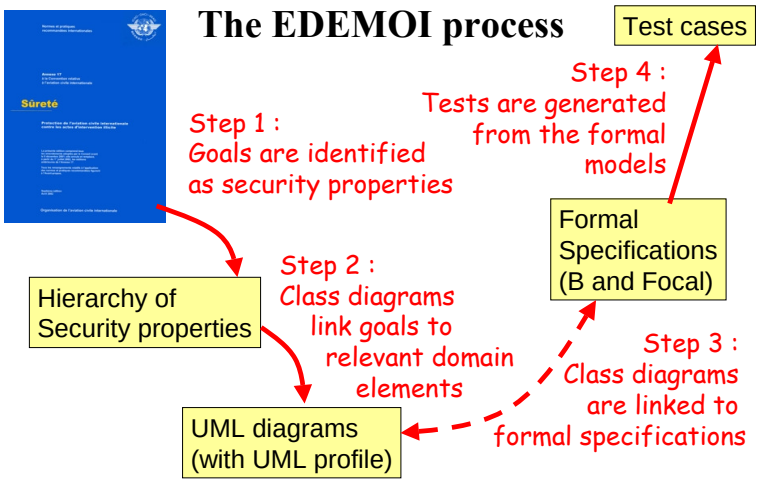


Figure 2: The EDEMOI process

Special efforts were dedicated to the first two steps, in order to improve the validation of the graphical model. It led to the definition of a requirements engineering approach dedicated to aviation security.

## 2.1 Results

These activities addressed the two goals mentioned above: modeling Annex 17 led to the discovery of natural language ambiguities and hidden hypotheses. Further analyses of the formal models helped to assess the quality of the standard. And test generation addressed the conformance problem. The project members also developed contacts and fruitful interactions with the international civil aviation authorities (ICAO and ECAC). One of these interactions with ICAO led us to model the latest evolution of Annex 17 and evaluate its non-regression with respect to the current standard. This led to the identification of two regressions in the new standard (these regressions were known by ICAO/OACI). The major scientific results of EDEMOI were:

- the modeling approach which leads to the identification of goals and the production of graphical models [LVL$^+$05, LVL$^+$06],
- the formal models of Annex 17 [DÉDG06a, DDDG06b, BBLV06]
- and the generation of conformance tests for Annex 17 [BBLV06].

Scientific by-products of this project include the development of tools that link B specifications back to UML diagrams [ILB05] and the experimentation of the Focal language as a formal modeling language [DÉDG06a]. These works led to two PhD theses.

Finally, it appears that regulation modeling not only applies to aviation security but to a variety of domains (E-business, E-government, Transport, Finance, Health,...). Therefore the EDEMOI project members initiated a workshop dedicated to REgulation MOdeling Validation and Verification (REMO2V) which was held in conjunction with CAISE'06 [LL06].

### 2.2 Collaboration with civil aviation authorities

In the EDEMOI project, the actions of ONERA, which is one of the members of the consortium, allowed us to take contacts with international organisations in charge of civil aviation. First, this helped us understand the regulations and their context, as well as their future needs.

In 2005, ICAO gave us access to the draft of the next revision of Annex 17. We took this opportunity to compare the old and the new versions, using our graphical modeling techniques. The results of this comparison were sent to ICAO. They highlight several regressions of the new version, as well as expected progresses. They also show some ambiguities in the new standard. Although these regressions and progresses were already known by the ICAO experts, we believe that our approach provides a systematic technique to identify and to present these evolutions based on the clear identification of links between the models.

Other applications of the EDEMOI techniques have been identified. They are mainly based on the exploitation of the tests generated from the models.

## 3 Project report

### 3.1 Activity 1 - Scope of the study

*Authors : Michel Lemoine & Sylvie Vignes (ONERA & ENST)*

This first activity aimed at precisely identifying the scope of the project. In the context of EDEMOI, we have considered as main topic the modeling of Airport Security. In the following sections we will introduce first of all what the security is from a regulation point of view, and then how the airport can be described in order to support the security regulations.

#### Introduction: the airport security

In an international airport, the security must follow some very specific rules described in various documents.

- International Standards and Recommended Practices to Security (Annex 17) [ICA02], which represents the general rules that have been accepted by all the countries in the world.
- Security Manual for Safeguarding Civil Aviation against Acts of Unlawful Interference [AVS96], which can be considered as some recommendation for implementing Annex 17 at a national level.
- Policy statement in the field of Civil Aviation Security, (European Civil Aviation Conference [ECA01]), which represents the way Europe implements Annex 17, whereas [AVS96] is for the rest of the world.

The ICAO Security Manual [AVS96], and ECAC Doc 30 [ECA01] are restricted access documents. Annex 17 [ICA02] is a public document that can be purchased from ICAO. Moreover, parts of Doc 30 are publicly available as a European Union Regulation [ECA02].

Annex 17 applies to all elements of civil aviation security, including the reactions to attacks. It also defines the various responsibilities in security activities. Therefore, we only addressed a part of the document, mainly Chapter 4, dedicated to airport security measures.

During the project we got access to most of these documents. In particular, we received an official copy of the ICAO Security Manual [AVS96] from the chief of ICAO AViation SECurity division (AVSEC).

**Modeling security from a static and dynamic point of view**

Another important objective was to identify the kind of graphical descriptions which are of interest for the EDEMOI project. This was based on some preliminary modeling work carried out at ONERA on a small subset of the airport (the screening/check point).

For that purpose it has been decided to use the UML notations, which allow to represent both static and dynamic aspects.

The static aspects are relative to the description of the airport, its components (boarding room and passengers for instance), and all their relationships. Still at this level, a first question was: what regulations can be attached or described statically?

The dynamic aspects are relative to all the elements to which security regulations are applied: mainly passengers and their luggage, and all the vehicles that can move in an airport. The important point was the fact that when items move their state can change. It was important to detect where the arrival states are conformant to the security regulations or not.

**Extent of Airport Security Modeling**

A first set of static models was elaborated [Liv1]. It allowed to identify the **areas of the airport covered by our study**. We decided to follow the path of passengers and their luggages, from their entry in the airport until their boarding in the plane. Actually, this scope was further refined after our discussions with ECAC experts.

Moreover, we decided to focus on public standards, i.e. mainly Annex 17 [ICA02] and to some extent Reg. 2320 [ECA02].

## 3.2 Activity 2 - Identification of property types to model and analyze airport security

*Author: Didier Bert, LSR-IMAG*

The objectives of this activity are:

1. To list the types of properties that are present in the regulation documents for airport security.
2. For each property, to determine how it will be taken into account by the project, and to identify various techniques to express it.

The main results of this activity are reported in Deliverable 2 [Liv2]. The work started from Annex17 [ICA02] and identified 30 properties that apply to the subset of the airport which is modeled. The deliverable manages properties following a **property hierarchy** (i.e. set of trees) where the property at a node holds if all the properties of the child nodes hold. So, each property is connected to the subproperties that are necessary and sufficient to satisfy it. The notion of *sufficient property* is strongly dependent on the security policy. For dealing with that, we have put in evidence the **hypotheses**, that are implicit in the documents, to assert that the required properties in Annex17 are indeed sufficient to ensure the security of the aircraft.

On this basis, properties have been classified into four categories (invariant, dynamic, statistic, fuzzy). We can notice that the part of regulation addressed by the EDEMOI project does not contain knowledge properties (unlike we could expect).

Most of the properties are invariant properties. They are expressed very easily in formalisms like B or Focal. It is much more difficult to express and to analyze statistic or fuzzy properties.

Deliverable 2 fulfills the objectives of this activity. This document was very useful for the project, because the property hierarchy is used in Activity 3 (graphical/UML models) and Activity 4 (formal specification of the airport security properties).

## 3.3 Activity 3 - Graphical Models Engineering

*Authors : Régine Laleau & Sylvie Vignes, LACL & ENST*

The initial project set the following objectives for Activity 3:

- semi-formal modeling of the regulation
- validation of the model by ECAC's experts
- definition of a UML profile dedicated to airport security

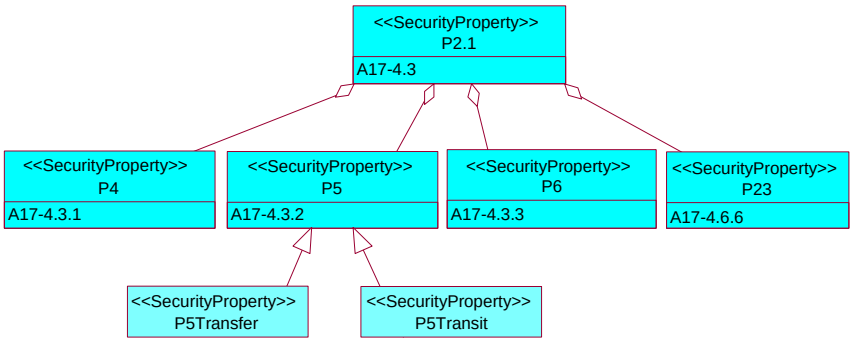


Figure 3: Hierarchical graph of security properties

Deliverable 3 is a UML model of Annex 17. It includes three kinds of diagrams. The first one is a hierarchical graph of the security properties identified in Deliverable 2 (e.g. Fig. 3). The second one includes 10 diagrams. Each class diagram corresponds to the domain model of a set of security properties, that is, the different kinds of objects in an airport that are relevant to express a security property. An agent model has also been elaborated. It captures responsibility links between agents and security properties. An agent can be a human or an organization and plays a role towards the satisfaction of some properties. Finally the last kind of diagrams corresponds to the **conceptual model of an abstract airport** as described in Annex 17 (e.g. Fig. 4). This class diagram is obtained by merging all the domain diagrams, by incorporating additional information describing airport configuration, and by specifying the operations that correspond to the functionalities defined in Annex 17. To improve traceability, each operation is associated with the security property that it must establish.

All the non standard UML concepts have been introduced in diagrams by using stereotypes. 11 stereotypes have been defined.

This model has been validated by ECAC and ICAO during several meetings where we met their experts. The graphic notations capturing airport entities, their relationships and the related security properties were easily adopted by the experts. Diagrams were very helpful to clarify operational subtleties (e.g. transfer passenger versus transit passenger) and to highlight differences between two versions of regulation standards (e.g. risk assessment).

The last objective has been revisited and upgraded. Rather than defining a UML profile dedicated to airport security, we have defined a **new requirements engineering method to analyze civil aviation security standards** [LVL$^+$06]. Since none of the existing requirements engineering methods were able to consider the specifics of the project, we turned to situational method engineering, and have defined a new method based on this approach. Several adaptations/extensions have been brought to relevant RE techniques necessary to take into account the specific features of the project. We have chosen goal-oriented

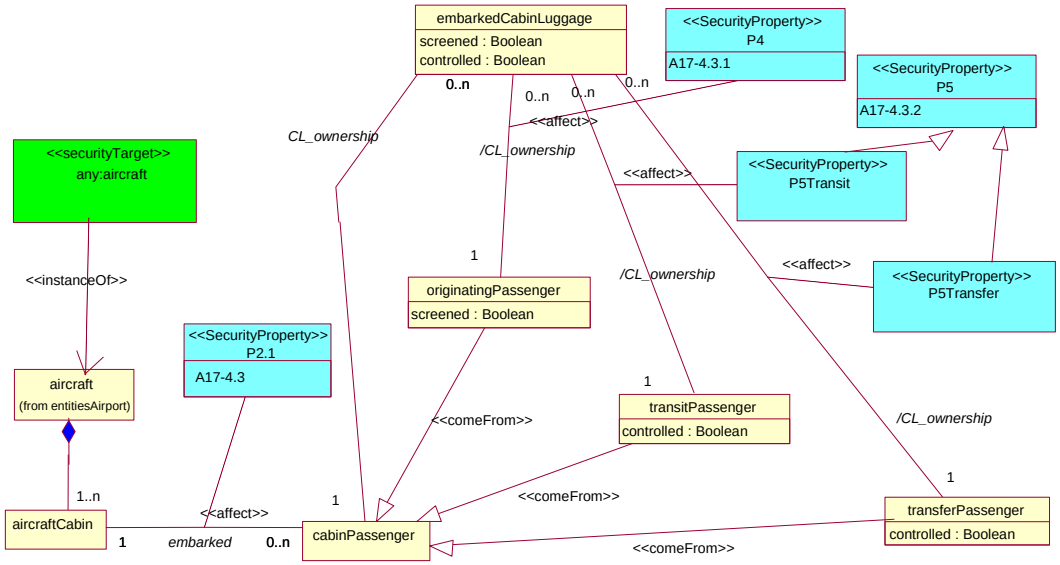


Figure 4: A class diagram with security properties

requirements methods and a meta-modeling technique to define our method. A method is defined by two models: the process model and the product model. Each model is specified by a meta-model described by using a UML activity diagram for the former and a class diagram for the latter. Links between the two meta-models represent the results generated, in terms of the elements of the product model, by activities of the process model. Thus the UML model of Annex 17 is an instantiation of the product meta-model. This allows us to give semantics to the different stereotypes introduced in the model.

As a result, this activity produced 19 UML diagrams for the first version of Annex 17, and 23 for its evolution (+ a traceability diagram between models).

## 3.4 Activity 4 - Formal Models Engineering

*Author: Catherine Dubois & Didier Bert, CEDRIC/CNAM & LSR/IMAG*

The CEDRIC team was in charge of activity 4 devoted to the ≪Definition of an approach for modeling and analyzing security in the airports≫. In this activity, the objective was to formalize static and dynamic entities occurring in the airports, together with their properties. Two series of formal models have been produced by the project:

- B models by the LSR team (4 models whose typical size is 800 lines of specification, 4 refinements, 250 proofs),
- Focal models by the CEDRIC team (10000 lines of specification, 150 modules, 200 proofs).

The formal modelisation activity has focused on the preventive security measures described in chapter 4 of Annex 17. For simplification reasons we do not cover measures about taxiing and parked aircraft and measures about cargo, mail, stuff intended for carriage on commercial flights. Furthermore some of the refinements proposed by the European Doc 2320 have been taken into account in the Focal formalization.

**Formalization within B**

A model in B (event B more precisely), in our context, is a first abstract specification that describes the main properties and a list of refinements which introduce more and more details.

A B component contains static declarations of sets and constants, together with their axiomatization. For example, the global sets of baggages, passengers. It contains also a state, defined by a set of variables, which describe the dynamic entities, e.g. the passengers currently in the airport, the baggages of the passengers etc. A component also contains a list of events defining the behavior and the dynamic evolution of the state variables. An event is guarded by a condition: it can be executed if the condition is true. The events are related to the management of the flights, the introduction of categories of passengers (originating, transit and transfer passengers) and the different procedures acting in an airport (check-in registration, passing the screening point and the control point, boarding in the aircraft cabin).

Security properties are introduced as the invariant of the model. The main property states that dangerous objects are admitted on board a departing aircraft only if they are authorized. It is expressed as invariant in the model. Invariant properties must always hold. I.e. we have to prove that it is really a conservative property during the dynamic evolution of the component. Proof obligations stating that the events preserve the invariant are automatically generated. They all have been proved.

A refinement introduces details and specific security properties. They must be proved correct with respect to its abstraction.

Four B models all based on Annex 17 have been produced :

- a model that studies the flows of passengers in an airport,
- a model closer to Annex 17,
- a model that describes all kinds of passengers,
- a model based on the new amendment (that arose last year) and focusing on passengers and baggage.

All these models have been proved. No security failure has been put in evidence.

The B models are also used as a starting point for animating specifications, for the generation of state transition diagrams (with the GeneSyst tool) and for a test generation process (with the BZTT tool, see next section).

**Formalization within Focal**

Focal is the specification and programming language of the Focal environment whose aim is to produce certified code. The Edemoi project was the reason for experimenting the Focal language in another application domain (it was designed with computer algebra applications in mind). It was also used for the first time with the aim to produce only an automated support for the analysis of the regulatory documents and not executable certified code.

A Focal specification is a hierarchy of structures, species or collections. Species contain functions -defined or only declared- and properties, -just stated or proved-. The proofs are done with Coq or Zenon. Species are combined via inheritance and parameterization. Collections are built from complete species where all functions are defined and all proofs discharged. These collections are not used in the context of the Edemoi project, except as parameters of parameterized species (because some items describing basic items, such as passengers, luggage, objects are not precisely defined).

The Focal specification produced by the Edemoi project (J.F. Étienne PhD thesis) first contains species that describe the model domain. Subjects such as originating passenger, cabin luggage, aircraft, object, security area are to be formalized. Each subject identified by the first activity of the project is associated to a species that describes its attributes and properties. Inheritance is very useful here: e.g. the 3 species dedicated respectively to ordinary passengers, armed passengers and obliged passengers inherit from the species that describe the cabin passengers (persons eligible to travel on board an aircraft).

To model the preventive security measures, the Focal specification follows the decomposition of chapter 4 of Annex 17. The security measures corresponding to reachable objectives are specified as invariant properties. Contrary to the B approach, the properties establishing that the properties must be satisfied by the security procedures are manually written in the specification. The top of the hierarchy, the species called *annex17*, formulates the main security property that states dangerous objects are admitted on board a departing aircraft only if they are authorized. It is proved that this property can be derived from the other preventive security measures described in the other parts of chapter 4 of Annex 17, hence described in other Focal species. This property ensures the consistency of the regulatory document but not the absence of contradictions.

The Zenon automatic prover provided by the environment Focal has discharged most of the proofs. It appears as very appropriate to deal with abstract specifications such as Edemoi's specifications.

**Conclusion**

Both approaches, B and Focal, have given adequate formal supports to reason about regulatory documents. Focal inheritance and parameterization have allowed us to produce specifications whose structure sticks to the informal document (chapter 4 of Annex 17). One of the by-product of the project was to evaluate Focal on such an application. It is in evidence well adapted [DÉDG06a].

This activity has **revealed some ambiguities and raised different interpretations of a same item** which were clarified by further interactions with ICAO. The formalization also put **emphasis on some implicit hypotheses**.

**The (missing link) between graphical and formal models**

Since certification authorities are not able to validate formal models (Fig. 1), it is crucial to establish strong links between the formal models and the validated ones. The original EDEMOI proposal planned to take advantage of existing translation tools from UML class diagrams to B specifications. Unfortunately, it quickly appeared that the available translation tools would be unable to translate the models produced by activity 3. Difficulties in this translation process include the EDEMOI-specific stereotypes as well as the size of the models [LLL+06].

Therefore, two alternate routes were followed:

- the automatic generation of conformance tests from the formal B specification; it appears that such tests are easily understood by certification authorities which can validate their conformance to the modeled standard.
- the use of reverse engineering techniques to reconstruct UML models from formal specifications. Automatic tools have been developed: a general tool for B [ILB05], a more specific tool for Focal exploiting specificities like those appearing in the Edemoi project. The latter is a first attempt for producing UML diagrams from Focal specifications.

## 3.5 Activity 5: Animation and Test generation

*Author: Fabrice Bouquet, LIFC*

The formal models offer inputs for a test generation process. EDEMOI exploited the B models as input for the LTG/BZTT Test Generator tool. Since this tool only takes a single B machine as input, a specific tool was developed by Didier Bert at LSR to compile the EDEMOI B specifications into a single machine.

Fig. 5 presents the test generation process. It is decomposed into three steps:

1. Decomposition of the model into behaviors.
2. Each behavior is used to compute test targets with respect to coverage criteria

3. A preamble (a sequence of operations) is computed to put the system into the state defined by the test target.

It must be noted that the evolution of the LTG tool allows to take as input a set of UML models: Class Diagram, for the data structure, Object Diagram, for initial state, and StateCharts, for the dynamic part. This feature was not used in the EDEMOI project but can be considered for future work.

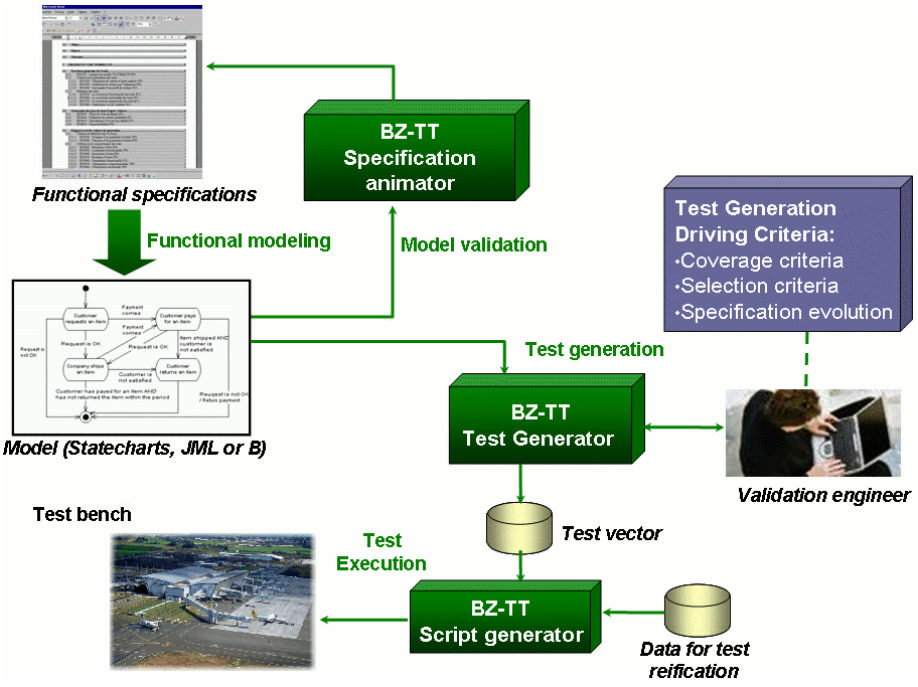


Figure 5: Architecture of LTG/BZTT

Test scenarios are either generated from the model, or designed by the model engineer to animate the models. It appeared during the project that these scenarios can be presented to the certification authorities for further validation of the models, or evaluation of the significance of the tests.

### Conformance tests for airport security

The LTG tool allowed to produce **21 conformance tests from the B models** [BBLV06]. Such tests mainly check that the airport lets passengers reach the airplanes in the absence of abnormal situations. Unfortunately, these techniques do not generate attack scenarios, which would help evaluate the response of the airport to attacks.

The main reason for this is that international standards, and hence their corresponding formal models, express high level security goals, but do not detail the kinds of attacks that may happen.

Further research is thus needed to adapt robustness testing techniques to the context of airport security. Some preliminary experiments were carried out by mutating preconditions of B operations. They led to the generation of **19 additional robustness tests**.

### 3.6 Activity 6: Impact analysis

*Author: Yves Ledru - LSR/IMAG*

The original goal of this activity was to evaluate the consequences of non-conformance to the standard with respect to security. It aimed to decide whether some stated non-conformance led to serious consequences, and hence needed significant reactions, or on the contrary had little impact on security and could be dealt with easily.

Two studies were performed within EDEMOI to address this goal.

- Regression testing for impact analysis
- Regression analysis in the evolution of Annex 17

Moreover, the LTG/BZTT testing tools of LIFC, that were used in activity 5 include facilities to trace between tests and requirements, allowing to identified which requirements are impacted by the failure of some test execution.

#### Regression testing for impact analysis

In her Master's thesis[2], Nguyen Thi Thu Minh at LSR studied how regression testing could be used for impact analysis. She first set up a test suite for the B model. The test suite was prepared using the BZTT tools, as well as animation tools for B. It included conformance tests, such as the ones developed in activity 5, but also variants of these tests as well as tests derived directly from Annex 17 or from domain knowledge. The tests of this resulting test suite could then be classified into normal behaviours, attacks to the airport, or "anomalies", i.e. non-conformant behaviours which don't correspond to a possible reality. These tests were shown to certification authorities and it appeared that they can easily associate such tests with some level of danger.

The regression test suite was then executed on variants of the B model. One of the variants did simplify the security procedures, the other one did strengthen them. The results of the regression test suite directly show which behaviours differ between the versions. This technique can be used (a) to identify breaches in security when simplified procedures are adopted, and (b) to identify conformant behaviours which become forbidden by strengthened security measures. Based on the evaluation of the level of danger, one can evaluate the impact of simplifications on security.

#### Regression analysis in the evolution of A17

This study was shared with Activity 3. It refers to the regression analysis performed on an evolution of Annex 17. The technique used here was to produce two UML models for Annex 17 and its evolution, then to identify links between the properties expressed in both models. These links fall into several categories: <<same Scope>>, <<same Property>>, <<split Property>>, <<property Modified by Precision>>, <<property Modified by Extension>>.

The study of these links shows that some properties of the older model no longer appear, which leads to identify regressions in security. Other properties appear only in the new model. They correspond to improvements in security. Other properties are more precise, or apply to more items.

This study allowed to write a detailed report of the evolutions and regressions, which was confirmed by the ICAO expert.

## 4 Deliverables

Deliverables were produced for each activity. Some of these deliverables are public and appear on the EDEMOI web site. Other public deliverables are available on request by e-mail to the project coordinator.

[2]NGUYEN Thi Thu Minh, "Analyse d'impacts d'anomalies de sécurité", Master 2 Recherche Systèmes et Logiciels, Université Joseph Fourier (Grenoble 1), 2005

Deliverable 2, and parts of deliverable 3 (comparison between two versions of A17) include confidential information. For each of these deliverables, two versions are available (public and a confidential ones).

Since the project was extended until January 2007, versions of all deliverables will be available by end of November 2006, and updates of some deliverables may appear in January 2007.

[**Liv1**] Livrable 1 : Identification du sous-ensemble de la réglementation "sûreté des aéroports", M. Lemoine, S. Vignes, juillet 2004
`http://www-lsr.imag.fr/EDEMOI/LivrablesPublics/Livrable1Public-V1.0.pdf`

[**Liv2**] Livrable 2 : Identification des propriétés pour la sûreté des aéroports - portée de la démarche EDEMOI, Didier Bert, Yves Ledru, juin 2004
`http://www-lsr.imag.fr/EDEMOI/LivrablesPublics/07-04-livrable-2-public.pdf`

The following deliverables will be available on request by email to Yves.Ledru@imag.fr.

[**Liv3**] Livrable 3 : Modèles UML de l'annexe 17 sous Rational Rose, Sylvie Vignes, Régine Laleau, Michel Lemoine, février 2005.

[**Liv4**] Livrable 4 : Modèles formels de la sécurité des aéroports en B et Focal, Catherine Dubois, Didier Bert, Jean-Frédéric Etienne, Véronique Donzeau-Gouge, novembre 2006

[**Liv5**] Livrable 5 : Animation et génération de tests pour la sécurité des aéroports
Fabrice Bouquet, Didier Bert, Fabien Peureux, Yves Ledru, novembre 2006

[**Liv6**] Livrable 6 : Analyse d'impact, Yves Ledru, Thi Thu Minh Nguyen, Sylvie Vignes, Régine Laleau, Michel Lemoine, novembre 2006.

# 5 Visibility of the project

## 5.1 Visibility by the civil aviation authorities

Contacts were established from the beginning of the project with ECAC/CEAC and ICAO/OACI which are in charge of writing the international standards at the european and international levels, and in charge of inspecting airports. Four meetings were held with these organisations or their representatives:

- October 2004: meeting at ECAC headquarters in Paris, with R. Benjamin (head of ECAC) and P. Reverdi (Expert in charge of airport inspections)
- April 2005: meeting at ICAO headquarters in Montreal with D. Antonini (head of AViation SECurity division) and several colleagues
- July 2005: meeting at ENST Paris with P. Reverdi to discuss the UML models of Annex 17
- September 2005: full-day meeting at IMAG Grenoble with D. Antonini to present the EDEMOI project

Further email interactions were done with D. Antonini on the regression evaluation of an evolution of Annex 17.

Other informal contacts were established with local airport authorities, and with European Union representatives.

An article which presents the EDEMOI project very informally is under preparation by ONERA for inclusion in the ICAO journal.

### 5.2 Visibility by the scientific community

The results of the project were published in international conferences and journals. These include direct results of the project resulting from the cooperation of the project teams [BBLV06, DDDG06b, LVL+05, LVL+06, LLL+06] but also results from the project participants which developed underlying techniques (see section 8.3) that have been or can be applied to the project. Other papers are currently under preparation or submission.

**The REMO2V workshop [LL06]** (International Workshop on Regulations Modeling and their Validation & Verification) was organized by the EDEMOI consortium as a workshop at CAISE'06. The workshop was chaired by M. Lemoine (General chair) and R. Laleau (Programme Chair). Our goal was to identify other application domains for the EDEMOI approach, and alternate approaches to model regulations. The workshop showed that the need for trustworthy regulations exists in a wide variety of domains: E-activities (E-business, E-government), Transport (air, railways), Finance, Health,... Several teams base their approach on a model that can be understood by all stakeholders (tabular notations, goal decomposition, diagrammatic notations). Then, formal techniques can be applied to support V&V activities (model-checking, theorem proving, simulation/animation, deviational analysis,...). The success of REMO2V'06 leads us to plan a second edition of the workshop in 2008.

## 6 Perspectives

At short term, the EDEMOI project led to the submission of a new project, named MICSA, to the 2006 SETIN call. The results of this submission are expected in november 2006.

The MICSA project aims at strenghtening two computer science techniques that were underestimated in EDEMOI: the links between graphical and formal models, and the generation of robustness tests from the models. MICSA also includes activities specific to the airport security domain, such as the generation of checklists for airport inspectors.

At short term, ONERA has decided to continue this trend of research by funding a thesis on regulation modeling.

At longer term, the REMO2V workshop has allowed us to identify potential academic partners for european projects. Moreover, we have set up contacts with several certification authorities at european and international levels which may lead to further collaborations.

## 7 Conclusion

The EDEMOI project has shown that computer science techniques, dedicated to security modeling, analysis and testing, could be used fruitfully outside the computer science domain. Its results apply both to the specific domain of airport security, but also to the more general domain of regulation modeling. Moreover, these new application domains result in new research questions for the underlying modeling techniques.

From an airport security point of view, EDEMOI has produced the following results:

- the production of graphical and formal models of Annex 17
- the identification of ambiguities and hidden assumptions in this document
- a validation approach where formal models are indirectly validated by the certification authorities through the inspection of graphical models and generated test cases
- a detailed regression analysis of two successive versions of Annex 17

From a computer science point of view, EDEMOI contributed to both the Focal, B and LTG/BZTT efforts.

- Experiments with Focal showed that it can be used as a modeling language, without leading to a subsequent implementation.
- Experiments with B confirmed its ability to construct and prove models using a stepwise approach based on refinements. We also experimented new techniques that allow to extract UML descriptions from the B specifications.
- Experiments with LTG/BZTT confirmed its ability to produce conformance tests, even in a context where the B specification does not describe software.

EDEMOI also helped to identify new research directions, related to the establishment of strong links between graphical and formal specifications, or the the need for further research in robustness test generation.

Finally, it tried to initiate a research community around regulation modeling, an emerging research area where Validation and Verification play a central role and can benefit from years of research in Computer Science.

### A successful consortium

The participants of the project have learned (and enjoyed) to work together in the previous project. Most activities have been the result of cooperations as shown by several publications of the project [LVL$^+$06, LLL$^+$06, BBLV06, LVL$^+$05] and the organisation of the REMO2V workshop. EDEMOI held about 15 (plenary) project meetings in less than three years, and numerous additional meetings which involved a subset of the partners. These frequent meetings helped us keep a good work tempo inside the project.

## 8 Publications

### 8.1 Deliverables

see section 4

### 8.2 Publications directly linked to the project


[**BBLV06**] D. Bert, F. Bouquet, Y. Ledru, and S. Vignes. Validation of regulation documents by automated analysis of formal models. In *REMO2V workshop [LL06]*, 2006.

[**DÉDG06a**] David Delahaye, Jean-Frédéric Étienne, and Véronique Donzeau-Gouge. Certifying airport security regulations using the Focal environment. In *FM'06 - 14th International Symposium on Formal Methods*, LNCS 4085, Springer, 2006.

[**DDDG06b**] J.-F. Etienne D. Delahaye and V. Viguié Donzeau-Gouge. Modeling airport security regulations in Focal. In *REMO2V workshop [LL06]*, 2006.

[**DÉDG06c**] David Delahaye, Jean-Frédéric Étienne, and Véronique Donzeau-Gouge. Reasoning about airport security regulations using the Focal environment. In *2nd International Symposium on Leveraging Applications of Formal Methods, Verification and Validation, Isola 2006, Cyprus*, 2006.

[**LLL$^+$06**] Y. Ledru, R. Laleau, M. Lemoine, S. Vignes, D. Bert, V. Donzeau-Gouge, C. Dubois, and F. Peureux. An attempt to combine UML and formal methods to model airport security. In N. Guelfi N. Boudjlida, editor, *CAISE Forum 2006 - Proceedings of the Forum of the 18th International Conference on Advanced Information Systems Engineering, Luxembourg, June 9, 2006*, pages 47–50, 2006.

[**LVL$^+$05**] R. Laleau, S. Vignes, Y. Ledru, M. Lemoine, D. Bert, V. Donzeau-Gouge, C. Dubois, and F. Peureux. Application of requirements engineering techniques to the analysis of civil aviation security standards. In *First International Workshop on Situational Requirements Engineering Processes (SREP'05)*, pages 91–106, published by Univ. of Limerick (Ireland), 2005.

[**LVL+06**] R. Laleau, S. Vignes, Y. Ledru, M. Lemoine, D. Bert, V. Donzeau-Gouge, C. Dubois, and F. Peureux. Adopting a situational requirements engineering approach for the analysis of civil aviation security standards. *Software Process: Improvement and Practice (SPIP)*, 11(5):487–503, 2006.

**Proceedings**

[**LL06**] R. Laleau and M. Lemoine. *Proceedings of the Int. Workshop on Regulations Modelling and their Validation and Verification (REMO2V'06)*, in conjunction with CAiSE'06, Presses Universitaires de Namur; ISBN 2-87037-525-5, Luxembourg, 6 june 2006.

## 8.3 Related publications

[**BBC+06**] E. Bernard, F. Bouquet, A. Charbonnier, B. Legeard, F. Peureux, M. Utting, and E. Torreborre. Model-based testing from UML models. In *MBT'2006, Model-based Testing Workshop, INFORMATIK'06*, volume P-94 of *LNI, Lecture Notes in Informatics*, pages 223–230, Dresden, Germany, October 2006. ISBN 978-3-88579-188-1.

[**BCD+06**] F. Bouquet, F. Celletti, G. Debois, A. De Lavernette, E. Jaffuel, J. Julliand, B. Legeard, J. Lidoine, J.-C. Plessis, and P.-A. Masson. Model-based security testing, application to a smart card identity applet. In *eSmart 2006, 7th Int. Conf. on Smart Cards*, Sophia-Antipolis, France, September 2006.

[**BDG05**] F. Bouquet, F. Dadeau, and J. Groslambert. Checking JML Specifications with B Machines. In H. Treharne, S. King, M. Henson, and S. Schneider, editors, *Procs of the Int. Conf. on Formal Specification and Development in Z and B, (ZB'05)*, volume 3455 of *Lecture Notes in Computer Science*, pages 435–454, Guildford, UK, April 2005. Springer.

[**BDL05a**] F. Bouquet, F. Dadeau, and B. Legeard. How Symbolic Animation can help designing an Efficient Formal Model. In *Procs of the 7-th Int. Conf. on Formal Engineering Methods (ICFEM'05)*, volume 3785 of *Lecture Notes in Computer Science*, pages 96–110, Manchester, UK, November 2005. Springer.

[**BDL05b**] F. Bouquet, F. Dadeau, and B. Legeard. Using Constraint Logic Programming for the Symbolic Animation of Formal Models. In J. Marques-Silva and M. Velev, editors, *Procs of the Int. Workshop on Constraints in Formal Verification (CFV'05) – Co-located with the Int. Conf. on Automated Deduction (CADE'05)*, pages 32–46, Tallinn, Estonia, July 2005.

[**BDL06**] F. Bouquet, F. Dadeau, and B. Legeard. Automated boundary test generation from JML specifications. In *FM'06, 14th Int. Conf. on Formal Methods*, volume 4085 of *LNCS*, pages 428–443, Hamilton, Canada, August 2006. Springer-Verlag.

[**BJL+05**] F. Bouquet, E. Jaffuel, B. Legeard, F. Peureux, and M. Utting. Requirement Traceability in Automated Test Generation - Application to Smart Card Software Validation. In *Procs. of the ICSE Int. Workshop on Advances in Model-Based Software Testing (A-MOST'05)*, St. Louis, USA, May 2005. ACM Press.

[**BLLP04**] E. Bernard, B. Legeard, X. Luck, and F. Peureux. Generation of Test Sequences from Formal Specifications: GSM 11-11 Standard Case-Study. *International Journal on Software Practice and Experience*, 34(10):915–948, 2004.

[**BLP04**] F. Bouquet, B. Legeard, and F. Peureux. CLPS-B: A Constraint Solver to Animate a B Specification. *International Journal of Software Tools for Technology Transfer, STTT*, 6(2):143–157, August 2004.

[**BLPT04**] F. Bouquet, B. Legeard, F. Peureux, and E. Torreborre. Mastering Test Generation from Smart Card Software Formal Models. In *Post proceedings of the Int. Workshop on Construction and Analysis of Safe, Secure and Interoperable Smart devices (CASSIS'04)*, volume 3362 of *Lecture Notes in Computer Science*, pages 70–85, Marseille, France, March 2004. Springer. Selected paper.

[**BPS05**] Didier Bert, Marie-Laure Potet, and Nicolas Stouls. GeneSyst: A Tool to Reason about Behavioral Aspects of B Event Specifications. Application to Security Properties. In *ZB2005 Conference*, pages 299–318. LNCS 3455, Springer-Verlag, 2005.

[**CLP04**] S. Colin, B. Legeard, and F. Peureux. Preamble computation in automated test case generation using Constraint Logic Programming. *The Journal of Software Testing, Verification and Reliability*, 14(3):213–235, 2004. Selected papers from the 2003 UK-Test Workshop.

[**DHD04**] Catherine Dubois, Therese Hardin, and Veronique Viguie Donzeau Gouge. Building certified components within FOCAL. In Hans-Wolfgang Loidl, editor, *Trends in Functional Programming*, volume 5, pages 33–48, Bristol, UK, 2004. Intellect.

[**DJPP04**] Catherine Dubois, Mathieu Jaume, Olivier Pons, and Virgile Prevosto. L'atelier Focal. In J. Julliand, editor, *Actes du 6eme Atelier sur les Approches Formelles dans l'Assistance au Développement de Logiciels (AFADL 2004)*, pages 321–324, Université de Franche-Comté, Besançon 2004, 2004.

[**GPL04a**] Xiaocheng Ge, Fiona Polack, and Regine Laleau. Secure database development and the Clark-Wilson security model. In *Atelier SSI'04 Sécurité des Systèmes d'Information, INFORSID 2004*, Biarritz, France, Mai 2004.

[**GPL04b**] Xiaocheng Ge, Fiona Polack, and Regine Laleau. Secure databases: an analysis of Clark-Wilson model in a database environment. In Persson A. and Stirna J., editors, *16th International Conference on Advanced Information Systems Engineering, CAiSE 2004,*, volume 3084 of *Lecture Notes in Computer Science*, pages 234–247, Riga, Latvia, June 2004. Springer.

[**Ida06**] Akram Idani. Couplage de spécifications B et de descriptions UML pour l'aide aux développements formels des systèmes d'information : Approche par méta-modélisation. In *Actes du 24ème congrès INFORSID*, Tunisie, Juin 2006.

[**IL04**] A. Idani and Y. Ledru. Object Oriented Concepts Identification from Formal B Specifications. In *Proceedings of 9th Int. Workshop on Formal Methods for Industrial Critical Systems (FMICS'04)*, pages 159–174, Linz, September 2004. ENTCS 133 (2005), Elsevier.

[**IL06a**] A. Idani and Y. Ledru. Dynamic Graphical UML Views from Formal B Specifications. *International Journal of Information and Software Technology*, 48(3):154–169, Mars 2006. Elsevier.

[**IL06b**] Akram Idani and Yves Ledru. Object Oriented Concepts Identification from Formal B Specifications. *International Journal of Formal Methods in System Design, Springer*, 2006. Special issue FMSD/FMICS2004, to appear.

[**ILB05**] A. Idani, Y. Ledru, and D. Bert. Derivation of UML Class Diagrams as Static Views of Formal B Developments. In *Formal Methods and Software Engineering, 7th International Conference on Formal Engineering Methods, ICFEM 2005*, volume 3785 of *Lecture Notes in Computer Science*, pages 37–51, Manchester, UK, November 2005. Springer-Verlag.

[**ILB06a**] Akram Idani, Yves Ledru, and Didier Bert. A Reverse-Engineering Approach to Understanding B Specifications with UML Diagrams. In *Proceedings of 30th Annual IEEE/NASA Software Engineering Workshop (SEW-30)*, USA, April 2006. IEEE Computer Society Press.

[**ILB06b**] Akram Idani, Yves Ledru, and Didier Bert. Analyse formelle de concepts pour la génération de diagrammes de classes UML à partir de spécifications B. In *Actes de la 7ème conférence AFADL - Approches Formelles dans l'Assistance au Développement de Logiciels*, pages 9–23, 2006.

[**KLPU04**] N. Kosmatov, B. Legeard, F. Peureux, and M. Utting. Boundary Coverage Criteria for Test Generation from Formal Models. In *Proc. of the 15th Int. Symp. on Software Reliability Engineering (ISSRE'04)*, pages 139–150, Saint-Malo, France, November 2004. IEEE Computer Society Press.

[**LdB06**] Yves Ledru and Lydie du Bousquet. Tobias-Z: An executable formal specification of a test generator. In *21st IEEE/ACM International Conference on Automated Software Engineering (ASE 2006), 18-22 September 2006, Tokyo, Japan*, pages 353–354. IEEE Computer Society, 2006.

[**Led06a**] Y. Ledru. A formalisation of the soccer substitution rules. In *REMO2V'06, Int. Workshop on Regulations Modelling and their Validation and Verification (in conjunction with CAiSE'06)*, Luxembourg, June 2006.

[**Led06b**] Yves Ledru. Using Jaza to animate RoZ specifications of UML class diagrams. In *Proceedings of Int. Z User Meeting (ZUM'06)*, USA, April 2006. IEEE Computer Society Press.

[**LM06**] Régine Laleau and Amel Mammar. From UML Diagrams to B Specifications. In Marc Frappier and Henri Habrias, editors, *Software Specification Methods : an Overview Using a Case Study*. Hermes Science Publishing, ISTE London, 2006.

[**LPA+03**] B. Legeard, L. Py, F. Ambert, F. Bouquet, and F. Peureux. Génération de tests à partir de spécifications: Concepts, méthodes et outils. *Génie Logiciel*, 67:27–36, December 2003.

[**LPU04**] B. Legeard, F. Peureux, and M. Utting. Controlling Test Case Explosion in Test Generation from B Formal Models. *The Journal of Software Testing, Verification and Reliability*, 14(2):81–103, 2004.

[**ML04**] Amel Mammar and Regine Laleau. UML2SQL : un environnement intégré pour le développement d'implémentations relationnelles à partir de diagrammes UML. In J. Julliand, editor, *Approches Formelles dans l'Assistance au Développement de Logiciels, AFADL'04*, pages 333–336, Besançon, France, Juin 2004.

[**ML06a**] Amel Mammar and Régine Laleau. A formal approach based on UML and B for the specification and development of database applications. *Automated Software Engineering*, 13(4):497-528, 2006.

[**ML06b**] Amel Mammar and Régine Laleau. From a B formal specification to an executable code: application to the relational database domain. *Information & Software Technology*, 48(4):253–279, 2006.

[**ML06c**] Amel Mammar and Régine Laleau. UB2SQL: A Tool for Building Database Applications Using UML and B Formal Method. *Journal of Database Management*, 17(4):70–89, 2006.

[**RB04a**] H. Ruíz Barradas and D. Bert. Propriétés dynamiques avec hypothèses d'équité en B événementiel. In J. Julliand, editor, *Approches Formelles dans l'Assistance au Développement de Logiciels, AFADL 2004*, pages 299–313, LIFC, Besançon, juin 2004.

[**RB04b**] H. Ruíz Barradas and D. Bert. Specification and Proof of Liveness Properties under Fairness Assumptions in B Event Systems. In *17ème Workshop on Algebraic Development Techniques, WADT'04*, Barcelone, march 2004.

[**RB05**] Héctor Ruíz Barradas and Didier Bert. A Fixpoint Semantics of Event Systems with and without Fairness Assumptions. In *IFM 2005 Conference*. LNCS 3771, Springer-Verlag, November 2005.

[**RB06a**] Héctor Ruìz Barradas and Didier Bert. Développement et preuve de vivacité de l'algorithme distribué de Ricart-Agrawala. In *Actes de la 7ème conférence AFADL - Approches Formelles dans l'Assistance au Développement de Logiciels*, pages 161–178, 2006.

[**RB06b**] Héctor Ruíz Barradas and Didier Bert. Propriétés dynamiques avec hypothèses d'équité en B événementiel. *Technique et Science Informatiques*, 25(1):73–102, 2006.

**Proceedings**

[**VVDG06**] S. Vignes and V. Viguié-Donzeau-Gouge, Actes d'AFADL'06 : Approches Formelles dans l'Assistance au développement de Logiciels. *ENST, 2006 S 002*, Paris, 2006

# 9 Civil aviation documents

[**911**] *The 9/11 Commission Report - Final Report of the National Commission on Terrorist Attacks Upon the United States.* `http://www.gpoaccess.gov/911/pdf/fullreport.pdf`

[**AVS96**] AVSEC. Security manual for safeguarding civil aviation against acts of unlawful interference. Technical report, OACI, 1996.

[**ECA01**] ECAC (European civil aviation conference). Policy statement in the field of Civil Aviation Security - Doc 30 9th edition, December 2001.

[**ECA02**] ECAC (European civil aviation conference). Règlement (ce) n$^o$ 2320/2002 du parlement européen et du conseil. Technical report, European Union, December 2002.

[**ICA02**] ICAO. *Annex 17 to the Convention on Int. Civil Aviation - Security - Safeguarding International Civil Aviation against acts of unlawful interference*, 2002.

# 10 Other References

[**BRJ99**] G. Booch, J. Rumbaugh, and I. Jacobson. *The Unified Modeling Language user guide.* Addison Wesley Longman Publishing Co., Inc., 1999.