
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 - Septembre 2006



Rapport à mi-parcours

Yves Ledru

Référence : rapport à mi-parcours

Date : avril 2005



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 LIFC , Besançon Laboratoire LSR , IMAG, Grenoble

Rapport à Mi-Parcours du projet EDEMOI

Y. Ledru

Avril 2005

1 Rappel des objectifs du projet

Le projet EDEMOI (Elaboration d'une DEmarche pour la MOdélisation Informatique, la validation et la restructuration de réglementations de "sûreté" (sécurité)¹, et la détection des biais dans les aéroports) a pour objectif l'amélioration de la réglementation qui régit la sécurité des aéroports. L'aéroport est le dernier endroit où les passagers et leurs bagages peuvent être contrôlés avant d'embarquer dans un avion. Il constitue donc un maillon essentiel pour garantir la sûreté du trafic aérien. Sa sécurité est régie par diverses réglementations édictées par des autorités internationales et nationales. L'Annexe 17 [A17] est un de ces documents. Ces autorités assurent également l'inspection des aéroports pour évaluer leur conformité.

Ces réglementations sont des documents en langue naturelle et sont épais de plusieurs centaines de pages. De plus, dans le but d'améliorer constamment la sûreté (sécurité), ils doivent régulièrement évoluer. Les autorités de certification sont donc confrontées à deux types de situations :

- Comment garantir la cohérence de l'ensemble du document? N'existe-t-il pas des biais dans la sûreté (sécurité), ou de tels biais ne risquent-ils pas d'être introduits lors d'une évolution de la réglementation?
- Il arrive aujourd'hui que deux inspecteurs qui évaluent au même moment le même aéroport en ressortent avec des conclusions opposées quant à sa conformité. Cette situation est souvent mal vécue par les autorités de l'aéroport concerné et jette un doute sur le sérieux de l'inspection.

Le projet EDEMOI veut tirer parti des techniques informatiques de modélisation pour :

- construire des modèles de la réglementation et ainsi mettre en évidence les imprécisions ou biais éventuels,
- disposer d'un modèle précis pour y mener des analyses de cohérence,
- générer des cas de test destinés à supporter le travail des inspecteurs.

Les modèles construits par le projet sont de deux natures :

- des modèles graphiques semi-formels (UML), construits à l'aide de techniques d'analyse des exigences (Requirements Engineering). Ces modèles constituent un premier élément de formalisation qui se veut lisible à la fois par les informaticiens et par les autorités de l'aviation civile.

¹Dans le domaine de l'aviation civile, le terme "sûreté" est souvent employé là où les informaticiens utiliseraient le terme "sécurité".

- des modèles formels (en B, Z et Focal) qui expriment précisément les propriétés de la réglementation et se prêtent à des traitements automatiques pour vérifier leur cohérence et générer des cas de test.

La Fig. 1 présente les différents types de documents manipulés dans le projet et le rôle des principaux intervenants. Le lien entre les documents graphiques et les modèles formels bénéficie du support d'outils développés par les équipes du projet. Ces outils peuvent supporter la traduction du modèle graphique vers un modèle formel, ou reconstruire un diagramme à partir d'une spécification formelle.

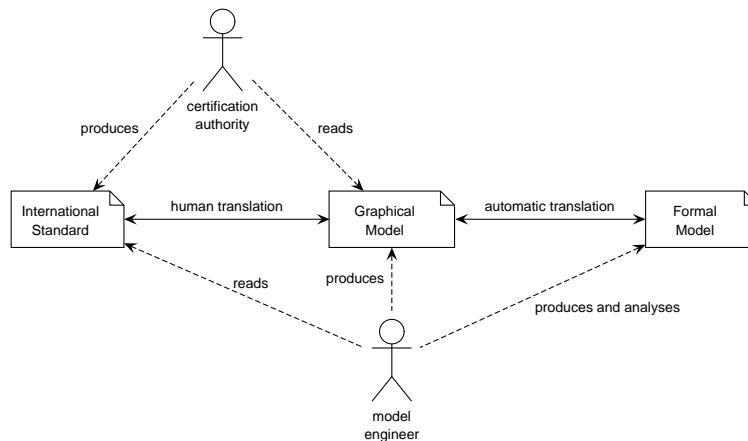


Figure 1: Acteurs et documents dans l'approche EDEMOI

2 Résultats obtenus

Cette première partie du projet s'est concentrée sur l'acquisition de connaissances sur le domaine modélisé, la production de modèles graphiques et la prise de contacts avec les autorités de l'aviation civile.

2.1 Activité 1 : Identification du problème

Le projet soumis à l'ACI Sécurité Informatique définissait les objectifs suivants pour cette activité.

1. Déterminer précisément les limites de l'étude, c'est-à-dire identification de tous les acteurs impliqués, des modes de fonctionnement réels, des procédures appliquées, etc. puis choix du périmètre.
2. La compréhension de la réglementation relative à cette partie de l'aéroport.

Plusieurs documents relatifs à la sûreté (sécurité) des aéroports ont été diffusés dans l'équipe. Leur étude a permis d'atteindre le deuxième objectif. Sur cette base, une première série de modèles UML a été réalisée et regroupée dans le livrable 1 [Liv1]. Ces modèles ont permis de préciser les

parties de l'aéroport concernées par notre étude, essentiellement la zone empruntée par le passager entre son enregistrement et son embarquement dans l'avion ². Le premier objectif est donc atteint.

2.2 Activité 2 : Identification des types de propriétés à modéliser et à analyser

Le projet soumis à l'ACI Sécurité Informatique définissait les objectifs suivants pour cette activité.

- *Etablir la liste des types de propriétés que comprend la réglementation de la sûreté des aéroports*
- *Pour chaque propriété, préciser dans quelle mesure elle sera prise en compte par le projet et identifier des techniques alternatives pour l'exprimer.*

Le livrable 2 [Liv2] part de l'annexe 17 [A17] et y identifie les propriétés qui s'appliquent à notre sous-ensemble de l'aéroport. Il organise ces propriétés dans une hiérarchie où apparaissent certaines propriétés implicites dans l'annexe 17. Chaque propriété importante est ainsi liée aux sous-propriétés qui permettent de l'établir. Cette hiérarchie se rapproche d'une activité de raffinement de propriétés.

Sur cette base, les propriétés ont été classées en quatre grandes catégories (invariants, propriétés dynamiques ou temporelles, propriétés statistiques, propriétés floues ou imprécises). Il faut noter que la partie de la réglementation qui intéresse le projet EDEMOI fait peu ou pas appel à des propriétés de connaissance qui correspondraient à une logique épistémique.

La plupart des propriétés correspondent à des invariants et à des propriétés dynamiques qui peuvent s'exprimer assez naturellement dans les langages formels du projet (en particulier la méthode B). Le support des propriétés statistiques et des propriétés imprécises (qui peuvent faire appel à de la logique floue) sera plus difficile dans le cadre du projet.

Le Livrable 2 remplit donc les objectifs de cette activité. Ce document s'avère très utile pour le projet car la hiérarchie des propriétés a été réutilisée pour l'activité 3, et pour les divers modèles formels produits dans les autres activités.

2.3 Activité 3 : Construction d'un référentiel semi-formel

Le projet soumis à l'ACI Sécurité Informatique définissait les objectifs suivants pour cette activité.

- *Modélisation semi-formelle de la réglementation*
- *Validation de ce référentiel par les experts de l'ECAC*
- *Définition d'un profil UML pour la sûreté des aéroports*

Le livrable 3 [Liv3] est une modélisation UML de l'annexe 17 [A17]. Il comprend 12 diagrammes de classes ainsi que la hiérarchie des propriétés du livrable 2. Ce livrable met en relation un modèle du domaine (classes et relations de l'aéroport) avec les propriétés apparaissant dans la hiérarchie.

Ce modèle est en cours de validation en interne du projet. Il sera ensuite discuté avec Patricia Reverdi, expert de l'ECAC.

Le modèle fait appel à divers stéréotypes qui constituent une première ébauche de profil UML. Cependant, dans l'état actuel ce profil est plutôt orienté vers une large gamme d'applications en sécurité/contrôle d'accès, qu'au seul domaine de la sûreté des aéroports. Suite à la validation du modèle nous aviserons sur l'opportunité de spécialiser le profil à ce domaine particulier.

²Il faut noter que le périmètre envisagé initialement s'arrêtait à la porte d'embarquement, mais des discussions avec les autorités de l'ECAC nous ont amenés à étendre ce périmètre jusqu'à la porte de l'appareil.

2.4 Autres tâches

Les autres tâches du projet concernent l'utilisation de méthodes formelles pour la modélisation de l'aéroport. Plusieurs actions exploratoires ont été menées à ce jour :

- La construction d'un modèle B, constitué de 4 étapes de raffinements, qui décrit les objets, leur dangerosité, et les opérations qui permettent de les embarquer dans la cabine ou dans la soute de l'avion. La construction de ce modèle a permis de détecter des ambiguïtés dans certains paragraphes de l'annexe 17. (Didier Bert, LSR)
- Un modèle proche de ce modèle a été construit en FOCAL. Une étude est en cours pour comparer ces deux modèles. Toutes les propriétés décrites dans le chapitre 4 de l'annexe 17 ont été modélisées en Focal à l'exception de la section 4.5 (Fret) et de la section 4.6 (passagers particuliers). La consistance de ces propriétés a été formellement prouvée. Ces propriétés ont été précisées et complétées par les informations contenues dans l'annexe 30. La consistance des propriétés supplémentaires a été formellement établie ainsi que la cohérence globale du système. (J.F. Etienne, CNAM)
- Le modèle B a également servi de base à la génération d'un premier jeu élémentaire de tests avec l'outil LTG. Dans le cadre de cette première génération de tests, le modèle B a été annoté pour assurer le lien entre les exigences de la réglementation et les tests générés (mise en oeuvre de la technique de traçabilité présentée dans [BJLPU05]). (F. Peureux, LIFC).
- Une expérimentation est en cours sur la traduction de ce modèle B vers des diagrammes UML, afin de faciliter sa validation. Un outil automatique pour cette transformation est en cours de construction. (A. Idani, LSR)
- Une expérimentation est en cours sur la traduction de certains diagrammes du livrable 3 vers une spécification Z, en utilisant l'outil RoZ, et l'animation de cette spécification avec l'outil Jaza. (Y. Ledru, LSR, en collaboration avec M. Utting visiteur au LIFC)

2.5 Contacts pris avec les autorités de l'aviation civile

Des contacts ont été pris avec l'ECAC et l'ICAO.

- L'ECAC (European Civil Aviation Conference, <http://www.ecac-ceac.org>) est l'organisation européenne responsable de la réglementation et de l'inspection des aéroports. Son siège est situé à Paris. Nous avons été reçus le 14 octobre 2004 par Monsieur R. Benjamin (secrétaire exécutif de l'ECAC), et Madame P. Reverdi (Expert, Audits de sûreté de l'aviation). Ils nous ont promis leur collaboration dans la validation des modèles élaborés par le projet et sont intéressés par diverses expérimentations (études d'évolutions de la réglementation, "check-lists" pour les inspecteurs).
- L'ICAO (International Civil Aviation Organisation) est l'organisation responsable de la réglementation au niveau mondial. Son siège est à Montréal (Canada). Nous y serons reçus le 15 avril 2005 par D. Antonini (Responsable de la section "Aviation Security").

D'autres contacts ont été pris avec l'aéroport de Toulouse, et un responsable de la sûreté des aéroports canadiens.

3 Conclusions

Une forte particularité du projet EDEMOI est l'application par des informaticiens de techniques de modélisation à un domaine nouveau : la sûreté (sécurité) de l'aviation civile. L'aviation civile est depuis de nombreuses années un domaine privilégié d'application de techniques innovantes en sécurité. Les attaques du 11 septembre ont renforcé ce besoin [911] et nous pensons que la qualité des documents qui règlementent ce domaine est primordiale pour garantir la cohérence des dispositifs mis en oeuvre. La démarche du projet EDEMOI est originale car à ce jour, nous ne connaissons qu'un autre projet similaire : le projet européen SAFEE qui s'intéresse à la sûreté (sécurité) de l'avion en vol [Saf04].

Un effort significatif a été nécessaire pour se familiariser avec le domaine. Michel Lemoine a joué à cet égard un rôle essentiel pour nous donner accès à la réglementation et établir des contacts avec les autorités qui édictent ces documents et contrôlent leur application. La connaissance du domaine s'est maintenant diffusée au sein de l'équipe et permet la construction des modèles qui jouent un rôle central dans le projet.

Depuis que le modèle UML [Liv3] est disponible, chaque équipe a commencé à aborder le problème avec ses propres outils. A ce stade, nous avons choisi de modéliser en priorité des documents non confidentiels qui correspondent à une partie de l'aéroport connue et accessible à tous. Ce choix permet la diffusion des résultats du projet. Il présente aussi une caractéristique intéressante : les descriptions de l'annexe 17 restent à un niveau d'abstraction suffisamment élevé pour permettre plusieurs réalisations. Certes, cela facilite notre tâche car les modèles sont plus abstraits et moins détaillés, ce qui les rend plus faciles à gérer. Cependant, le niveau d'abstraction requis rend la compréhension plus difficile car certaines phrases de la réglementation requièrent manifestement une connaissance de leur contexte. Cela permet au projet de mettre le doigt sur certaines imprécisions ou ambiguïtés de ces documents [LVL05].

Il est important de souligner que, par rapport à la demande faite dans le projet soumis à l'ACI, les moyens humains accordés au projet par l'ACI sont faibles (un ingénieur pendant 12 mois vs demande initiale de 12 mois ingénieur + 12 mois post-doc + 2 allocations recherche). Les résultats obtenus à ce jour proviennent donc, d'une part, du fort engagement des chercheurs ou enseignants chercheurs impliqués dans le projet, et d'autre part de doctorants, financés en dehors du projet, qui y trouvent un terrain d'application intéressant pour leurs techniques.

A ce stade du projet, les objectifs sont atteints : compréhension du domaine, contacts avec les autorités de l'aviation civile et premiers essais de formalisation. Deux publications issues des travaux du projet ont été préparées et soumises à des conférences [LLB05, LVL05]. Ces publications mettent notamment en évidence les ambiguïtés et imprécisions des textes en langue naturelle qui constituent la réglementation. D'autres publications, connexes aux activités du projet ont été réalisées [BJLPU05, DHV04, GPL04, IL04, IL05, ML04, RB04].

La compréhension du domaine acquise pendant cette première moitié du projet et la disponibilité de modèles (graphiques et formels) vont permettre l'application des techniques formelles maîtrisées par les divers partenaires lors de cette deuxième phase du projet. Nous espérons que ces techniques permettront de détecter de nouvelles imprécisions, voire erreurs, dans la réglementation et de proposer des techniques d'inspection plus rigoureuses aux autorités de l'aviation civile.

Annexes

A Réunions du projet

Le projet est rythmé par des réunions fréquentes qui permettent de programmer des objectifs à court terme et de conserver la dynamique du projet.

Date	Lieu
28 octobre 2003	Paris
18 décembre 2003	Paris
9 mars 2004	Toulouse
10 mai 2004	Audio Conférence
14 et 15 juin 2004	Besançon
17 septembre 2004	Audio Conférence
22 octobre 2004	Paris
15 et 17 novembre 2004	Toulouse
27-28 janvier 2005	Villard-de-Lans
31 mars 2005	Paris

B Infrastructure de travail collaboratif

Plusieurs outils ont été mis en place pour aider au travail collaboratif au sein du projet et permettre la diffusion de nos résultats.

- Un site web hébergé par le LSR/IMAG (<http://www-lsr.imag.fr/EDEMOI/>) donne accès aux documents publics du projet (livrables, articles).
- Une partie de ce site est sécurisée (protocole https) et accessible par un mot de passe. Elle comprend les documents internes au projet et certains éléments confidentiels.
- Un serveur de travail coopératif est hébergé par le wiki de l'ENST (<http://wiki.enst.fr>). Il est accessible aux seuls membres du projet et comprend des versions intermédiaires de documents de travail.
- Une liste de diffusion (edemoi@imag.fr) est réservée aux membres du projet et hébergée par l'IMAG.

En outre, des réunions à distance entre participants d'une même tâche sont organisées sous forme de réunions téléphoniques, ou en utilisant des outils de télé-travail (netmeeting, skype).

C Participants aux 18 premiers mois du projet

CEDRIC/CNAM	David Delahaye Véronique Donzeau-Gouge Catherine Dubois Jean-Frédéric Etienne	MCF CNAM PR CNAM PR CNAM Doctorant MAE
LACL	Régine Laleau	PR Univ. Paris-12
GET/ENST	Sylvie Vignes	MCF ENST
LIFC	Bruno LEGEARD Fabien PEUREUX Fabien NICOLET Mathilde REHFUSS	PR Univ. Franche-Comté MCF Univ. Franche-Comté Ingénieur Ingénieur
LSR/IMAG	Didier Bert Yves Ledru Akram Idani Hector Ruiz Ansem Ben Cheikh Olivier Bert Thi Thu Minh Nguyen	CR CNRS PR Univ. Joseph Fourier doctorant MENRT doctorant stagiaire Ecole Polytechnique de Tunisie stagiaire EPITA étudiante Master 2
ONERA/CdT	Michel Lemoine Olivier Carton	ONERA stagiaire CNAM

D Livrables et Publications

D.1 Livrables

[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>

[Liv3] Livrable 3 : Modèles UML de l'annexe 17 sous Rational Rose, Sylvie Vignes, Régine Laleau, Michel Lemoine, fichier modeleA17_30_01_05V7.6.mdl disponible sous le site wiki du projet EDEMOI, février 2005.

D.2 Publications

[BJLPU05] F. Bouquet, E. Jaffuel, B. Legeard, F. Peureux, M. Utting Requirement Traceability in Automated Test Generation. In *Proceedings of the ICSE International Workshop on Advances in Model-Based Software Testing (A-MOST'05)* St. Louis, USA, ACM Press, May 2005

[DHV04] C. Dubois, T. Hardin, V. Vigié Donzeau-Gouge, Focal: an environment for developing certified components *Trends in Functional Programming, vol 2, editor: Hans-Wolfgang Loidl* and also *Fifth Symposium on Trends in Functional Programming* Munich, Germany, November 25-26, 2004

- [**GPL04**] X. Ge, F. Polack, R. 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*, vol. 3084 of Lecture Notes in Computer Science, pp. 234-247, Riga, Latvia, June 2004. Springer.
- [**IL04**] A. Idani, 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)*, Linz, septembre 2004 (to appear as ENTCS volume)
- [**IL05**] A. Idani, Y. Ledru Dynamic Graphical UML views from Formal B Specifications. Accepté pour publication dans *Information and Software Technology Journal*, Elsevier.
- [**ML04**] A. Mammarr, R. Laleau Génération de code exécutable à partir d'une spécification B : applications aux bases de données. In J. Julliand, editor, *Approches Formelles dans l'Assistance au Développement de Logiciels, AFADL'04*, pp. 77-91, Besançon, France, Juin 2004.
- [**RB04**] H. Ruíz Barradas, D. Bert Propriétés dynamiques avec hypothèses d'équité en B événementiel. In *Actes de AFADL 2004*, Besançon, pp. 299-313, J. Julliand (ed.), LIFC, juin 2004.

D.3 Articles en cours de soumission

- [**LLB05**] Y. Ledru, M. Lemoine, D. Bert, V. Donzeau-Gouge, C. Dubois, R. Laleau, F. Peureux, S. Vignes, Modeling Airport Security: The EDEMOI Approach. janvier 2005.
- [**LVL05**] R. Laleau, S. Vignes, Y. Ledru, M. Lemoine, D. Bert, V. Donzeau-Gouge, C. Dubois, F. Peureux, Application of Requirements Engineering techniques to the analysis of civil aviation security standards. février 2005.

E Autres références bibliographiques

- [**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>
- [**A17**] *Annex 17 to the Convention on International Civil Aviation - Security - Safeguarding International Civil Aviation against acts of unlawful interference*, April 2002.
- [**Saf04**] *SAFE targets on-aircraft security*, 2004.
http://europa.eu.int/comm/research/aeronautics/info/news/article_681_en.html