
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



Identification des propriétés pour la sûreté des aéroports Portée de la démarche EDEMOI

Didier Bert, Yves Ledru

LSR-IMAG

Référence : Livrable 2, version 1.1

Date : 25 juin 2004

Diffusion publique



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

Projet EDEMOI

Identification des types de propriétés à modéliser et à analyser Portée de la démarche EDEMOI

Résumé : Le livrable 2 porte sur l'identification des propriétés pour assurer la sûreté dans les aéroports, sur leur typologie et sur les moyens de les exprimer formellement – ce qui sera fait dans le livrable 4.2. Il précise la portée de l'étude EDEMOI. L'état du livrable à T0+6 (version 1) est un recensement structuré des propriétés telles qu'elles apparaissent essentiellement dans l'annexe 17. Le rapport donne les relations de causalité entre ces propriétés et met en évidence les hypothèses implicites qui ont conduit à formuler ces propriétés. Il analyse ensuite brièvement quels sont les « types » des propriétés rencontrées.

Livrable 2

Version 1.1, 25 juin 2004

Diffusion publique

Planning du livrable 2

Date de livraison	Version	Eléments du contenu
T0+6	1	Mise en évidence de diverses propriétés de sûreté (principalement pour ce qui concerne l'annexe 17)
T0+12	2	
T0+24	3	
T0+36	4	

1 - Introduction

Ce rapport (version 1.1) présente et classe les propriétés requises pour assurer la sécurité des passagers, de l'équipage, du personnel au sol et du public dans toutes les matières liées à la protection contre les « actes d'intervention illicite¹ » avec l'aviation civile.

Il a pour but de comprendre la politique de sûreté qui est décrite dans les documents officiels, de lier les actions de vérification à un objectif, de mettre en évidence les hypothèses sous-jacentes et enfin de disposer de moyens pour faciliter la mise à jour de cette politique de sûreté en fonction de nouvelles menaces ou de nouvelles dispositions réglementaires. Conformément au domaine du projet EDEMOI, l'étude ne concerne que la sûreté des aéroports et les mesures prises à l'intérieur de celui-ci.

2 - Propriétés statiques : analyse descendante

Le principe de cette analyse est de partir de la propriété « de sûreté » la plus fondamentale et de voir comment cette propriété peut se décliner en sous-propriétés. Dans cette décomposition, le fait de satisfaire les sous-propriétés implique la satisfaction de la propriété initiale (cf. paragraphe 3). La propriété fondamentale de sûreté du transport aérien international est :

Se protéger contre les actes d'intervention illicite (1)

Ces actes sont ceux qui peuvent mettre en danger les passagers, l'équipage d'un vol ainsi que le personnel au sol et le public (A17, 2.1.1).

Hypothèse 1 (induction sur les étapes d'un vol): chaque pays s'assure que les règles de sûreté sont bien prises dans le pays d'où vient un avion (A17, 4.2.1).

Hypothèse 2 : les actes d'intervention illicite avec l'aviation civile ne peuvent se produire qu'avec l'aide d'une arme, d'un explosif ou d'un autre engin dangereux et/ou lorsqu'une personne se trouve dans un endroit vulnérable (critique pour la sûreté). D'où les deux nouvelles propriétés de sûreté :

Il n'y a pas d'objets non autorisés dans les avions (A17, 4.1) (2)

Les personnes non autorisées ne peuvent pas entrer dans la cabine de pilotage (A17, 4.2.3) (3)

La propriété (3) ne concerne pas directement les contrôles faits dans l'aéroport. Dans la suite, nous étudions comment la propriété (2) peut être vérifiée.

A ce niveau, le document A17 distingue cinq situations en ce qui concerne les objets qui peuvent être introduits dans les avions, les personnes qui sont impliquées (passagers, employés, etc.) :

1. les passagers ordinaires et les bagages de cabine (A17, 4.3)
2. les bagages de soute des passagers (A17, 4.4)

¹ Pour le choix des termes techniques, voir le lexique en fin de rapport.

3. le fret, courrier et autres marchandises acheminés par avion (A17, 4.5)
4. les catégories spéciales de passagers (A17, 4.6)
5. les personnes et les objets qui ont accès aux zones de sûreté à accès réglementé (A17, 4.7)

2.1 – Les passagers ne doivent pas avoir en cabine des objets dangereux par nature (armes, explosifs) ou par destination (ciseaux, copie d'arme, etc.). D'où les trois conditions :

Les passagers et les objets emmenés en cabine doivent être inspectés (screened) avant embarquement (4.3.1). (4)

Par la suite, quand le document A17 utilise le mot *screened*, alors on mettra le terme *inspecté* par contre, lorsqu'il parle de « subjected to security controls », on utilisera le terme *contrôlé* ou *sujet à des contrôles* (sous-entendu « de sûreté ») souvent qualifiés d'*adéquats* ou *appropriés* (par exemple, dans les propriétés 5 et 7).

Les passagers en transit ou en transfert sont sujets à des contrôles adéquats (4.3.2) (5)

Il n'y a pas de contact entre les passagers qui ont été inspectés pour embarquer et ceux qui ne l'ont pas été (4.3.3) (6)

Cet article (4.3.3) prévoit les procédures à prendre lorsqu'il y a eu « mélange » de tels passagers. C'est un des rares cas où la norme indique une procédure de remise dans un état cohérent du point de vue des règles de sûreté. Nous y reviendrons au paragraphe 5.

2.2 – Il y a un ensemble de mesures pour assurer qu'il n'y a pas d'objets non autorisés dans les bagages de soute. Néanmoins, les mesures ne sont pas formellement précisées. Elles reposent essentiellement sur l'hypothèse 3 et sur l'inspection :

Les bagages de soute doivent être sujets à des contrôles appropriés avant embarquement (4.4.1). (7)

Il n'y a pas d'intervention non autorisée entre le moment de prise en charge d'un bagage (check in) et l'embarquement en soute (4.4.2). (8)

Les zones d'entrepôt de bagages mal acheminés, non réclamés sont sûres (4.4.4). (9)

Hypothèse 3 : les bagages (à main et en soute) sont sûrs si leur propriétaire est à bord :

Les opérateurs ne transportent pas de bagage en soute dont le propriétaire n'est pas à bord de l'avion, sauf si le bagage a été soumis à un contrôle de sûreté approprié qui peut inclure l'inspection (4.4.3). (10)

Un passager ne doit pas laisser quoi que ce soit (items) à bord d'un avion quand il quitte cet avion aux arrêts de transit (4.2.2). (11)

Affaiblissement de l'hypothèse 3 et renforcement de l'inspection :

A partir du 1^{er} janvier 2006, tous les bagages de soute doivent être inspectés (4.4.8). (12)

2.3 – Le fret, courrier et autres marchandises acheminés par avions de passagers rentrent dans le même cas que les bagages non accompagnés :

Le fret, courrier ou autres marchandises acheminés par avion doivent être soumis à un contrôle de sûreté approprié (4.5.2, 4.5.4). (13)

Des « regulated agents » peuvent certifier la sûreté des envois de marchandise (fret, courrier, etc.) par avion de passagers auprès des exploitants :

Le fret, courrier ou autres marchandises acheminés par avion peuvent être certifiés par des agents de réglementation (4.5.3). (14)

2.4 – Les catégories spéciales de passagers sont, d'une part, ceux qui sont obligés d'embarquer pour des raisons administratives ou judiciaires et, d'autre part, ceux qui sont habilités à porter des armes. Les états doivent informer le commandant de bord du nombre de ces personnes et de leur numéro de siège dans l'avion. La présence d'armes dans un avion est en contradiction avec la propriété (2). Néanmoins, cette présence est régie par les règles suivantes :

Des mesures et procédures doivent être prises pour assurer la sûreté à bord dans le cas de personnes obligées à voyager pour des raisons administratives ou judiciaires (4.6.3). (15)

Les agents de sécurité qui portent des armes doivent être des personnes dûment habilitées par les états et spécialement autorisées (4.6.4). (16)

L'autorisation pour des personnes de porter des armes dans un avion doit être accordée par les pays dans lesquels l'avion fait escale (4.6.5). (17)

Si des armes sont transportées seules, alors elles ne doivent pas être chargées, ni être accessibles par les passagers (4.6.6). (18)

2.5 – Les zones de sûreté à accès réglementé (zsar) sont celles qui permettent d'accéder aux avions ou à tout autre lieu critique pour la sûreté (points vulnérables). Elles sont contrôlées par inspection/filtrage pour les passagers. Elles doivent être contrôlées pour les personnes, autres que les passagers, qui accèdent à ces zones.

Il y a un système d'identification des véhicules et des personnes qui accèdent aux zones de sûreté à accès réglementé (4.7.1). (19)

Les personnes (autres que les passagers) qui sont admises dans les zsar doivent faire l'objet de contrôles appropriés incluant des vérifications d'antécédents (background checks) (4.7.2) (20)

Il y a des mesures de supervision des mouvements des personnes et des véhicules dans les zsar (4.7.3) (21)

Hypothèse 4 : Les personnes qui sont affectées aux contrôles de sûreté sont sûres.

De plus, elles doivent être entraînées de manière appropriée. D'où une série d'articles ou de propriétés de « méta-niveau » pour valider cette hypothèse.

Les personnes qui mettent en œuvre les contrôles de sûreté doivent être sujettes à des vérifications d'antécédents et à des procédures de sélection (3.4.1) (22)

Les personnes qui mettent en œuvre les contrôles de sûreté doivent être entraînées et posséder toutes les compétences nécessaires pour remplir leurs fonctions (3.4.2) (23)

Les personnes qui réalisent les inspections sont certifiées selon les exigences du programme national de sûreté de l'aviation civile (3.4.3) (24)

3 – Relations de satisfaction entre les propriétés

Comme il apparaît clairement, le fait de satisfaire certaines propriétés assure (au moins dans une mesure quantitative ou statistique à déterminer) que d'autres propriétés sont satisfaites. On note par exemple :

$$(2)(3) \models (1)$$

ce qui signifie que les propriétés 2 et 3 entraînent la propriété 1. Les autres propriétés répondent à certaines catégories de prévention de danger. La propriété (2) se décline suivant six cas identifiés par les paragraphes de l'annexe. Ces cas ne sont pas explicites dans les articles de l'A17 :

Les passagers ordinaires ne possèdent pas d'armes, d'explosifs ou d'engins non autorisés en cabine (2.1)

Il n'y a pas d'explosifs ni d'engins incendiaires dans les bagages de soute (2.2)

Il n'y a pas d'explosifs ni d'engins incendiaires dans le fret, courrier et autres marchandises transportées (2.3)

Les personnes obligées² de prendre un avion ne peuvent pas mettre en péril la sûreté de celui-ci (2.4)

Les personnes armées en cabine sont habilitées (2.5)

Les personnes (autres que les passagers et le personnel de bord) qui peuvent accéder aux avions sont habilitées (2.6)

² Pour des raisons administratives ou judiciaires donc, peut-être, contre leur gré.

Cette décomposition permet de mettre en évidence directement la satisfaction de (2)

$$(2.1)(2.2)(2.3)(2.4)(2.5)(2.6) \models (2)$$

On voit maintenant les liens entre chaque sous-propriété et les articles de l'annexe, sous réserve de la validité de l'hypothèse 4 :

$$(4)(5)(6)(18) \models (2.1)$$

$$(7)(8)(9)(10)(11)(12) \models (2.2)$$

$$(13)(14) \models (2.3)$$

$$(15) \models (2.4)$$

$$(16)(17) \models (2.5)$$

$$(19)(20)(21) \models (2.6)$$

Cette notation permet de réaliser une traçabilité des propriétés et d'identifier leur impact sur le schéma général de la sûreté.

4 – Raffinement des propriétés

Les articles de l'annexe A17 sont souvent assez imprécis, par exemple (12) : « Un bagage non accompagné doit être soumis à un contrôle approprié ». Ces articles ou propriétés sont (généralement) raffinés dans les documents décrivant les mesures de sûreté prises par les états, puis par les aéroports. Il est important de pouvoir déterminer si une propriété d'un certain niveau est suffisamment explicite ou si elle mérite d'être raffinée. Il est alors intéressant de vérifier si les normes et recommandations du niveau inférieur raffinent bien la propriété abstraite.

Un exemple particulièrement complexe est le raffinement de l'article correspondant à la première partie de la propriété (10) : « *Les opérateurs ne transportent pas de bagage en soute dont le propriétaire n'est pas à bord de l'avion* ». Les documents nationaux et des aéroports développent ce point et rendent explicites diverses techniques pour vérifier la propriété en question (enregistrement des bagages, procédures de réconciliation, etc.).

5 – Typologie des propriétés rencontrées

La propriété fondamentale du transport aérien (1) est une propriété qui exprime un *souhait* et une *exigence* : « Se protéger contre les actes d'intervention illicite ».

Cette exigence est supposée remplie lorsque d'autres propriétés, exprimées comme des propriétés logiques, sont des *invariants*³ du transport civil international. C'est le cas en particulier de la propriété (2) : « Il n'y a pas d'objets non autorisés dans les avions ».

1. ³ Notons que les propriétés invariantes dans les spécifications sont appelées « propriétés de sûreté ».

D'autres propriétés sont exprimées sous forme de *procédure*. C'est le cas de la propriété (4) dont une partie peut s'exprimer par : « Les passagers doivent être inspectés avant embarquement ». On peut transformer cela en une propriété logique invariante : « Les passagers embarqués ont été inspectés ». Cependant, il est clair que la première formulation insiste sur le fait qu'il faut que les passagers (avant embarquement) passent d'un état où ils n'ont pas été inspectés à un état où ils l'ont été, ce changement d'état étant produit par une certaine procédure à définir. On a donc, d'une part une implication logique :

$$\textit{passagers embarqués} \Rightarrow \textit{passagers inspectés}$$

dont la contraposée est plus explicite :

$$\textit{passagers non inspectés} \Rightarrow \textit{passagers non embarqués}$$

mais aussi le fait que l'on a une propriété temporelle à vérifier (si l'on veut finalement embarquer des passagers, sachant dans un certain état « initial », un passager n'a pas été inspecté) :

$$\textit{passagers non inspectés} \rightsquigarrow \textit{passagers inspectés}$$

Cette propriété est notée comme une propriété temporelle « *leads to* ». Elle conduit, dans les textes, à préciser en détail la procédure d'inspection/filtrage.

D'autres types de propriétés se trouvent (ou pourraient se trouver) dans les documents :

1. Il est admis qu'un pourcentage de bagages à main doit être fouillé manuellement, en plus de l'inspection aux rayons X. Ce pourcentage pourrait être une propriété statistique à vérifier.
2. L'article (A17 4.3.3) formule la propriété (6) et ajoute « si un mélange ou un contact a lieu, les passagers concernés et leurs bagages à main seront re-inspectés avant embarquement »

On est en présence d'un cas de défaut explicite de sûreté, où la norme indique un mécanisme pour restaurer l'invariant de sûreté sur les passagers qui embarquent. Cela donne l'idée d'identifier les cas où les règles de sûreté peuvent être violées et, alors, définir une action de reprise.

6 – Autres propriétés

Nous avons déjà remarqué l'absence de propriétés statistiques, même si elles peuvent être sous-entendues ici ou là. Il n'y a pas, par exemple, de pourcentage minimum du nombre de bagages de soute à inspecter par rapport au nombre total de bagages ; l'A17 ne donne que la date à laquelle tous les bagages de soutes devront être inspectés.

Les propriétés de sûreté sont exprimées vis-à-vis de trois sortes de personnes :

1. les passagers (ordinaires ou exceptionnels) et leurs bagages,
2. les employés de l'aéroport qui ont accès aux zones à accès réglementé,
3. les personnes qui réalisent les contrôles de sûreté.

Pour les catégories 2 et 3, on trouve la notion de « vérifications d’antécédents » ou de certification par « les autorités compétentes », qui introduisent un niveau de contrôle plus ambitieux. Néanmoins, il n’est pas fait appel de manière évidente à des propriétés de la *logique épistémique* (connaissance et croyance des acteurs) qui pourraient être utiles, mais qui sont difficilement vérifiables.

Il semblerait qu’une étude dans ce sens pourrait faciliter l’expression de certaines propriétés et permettre d’élaborer des contrôles de sûreté basés sur des procédures de déduction différentes de celles de la logique classique. Enfin, l’aspect imprécis de certains articles gagnerait peut-être à trouver une formalisation avec les mécanismes des « logiques floues ».

Tous les articles de l’A17 sont de la forme « Each Contracting State shall ensure... » ou « shall require... » ou encore « shall establish measures to ensure... ». Nous n’avons pas tenu compte de cette formulation dans nos propriétés de sûreté. En fait, il s’agit d’une forme de logique qui pourrait s’apparenter à la *logique déontique* (ce qui est permis, interdit, obligatoire,...). Dans notre cas, il s’agit d’obligations de type juridique (et non de type moral ou légal), plus ou moins contraignantes, qui lient l’Etat contractant (signataire de la Convention on International Civil Aviation), de telle sorte qu’en cas d’accident, il soit possible de déterminer l’échelon qui a éventuellement failli et qui en porte la responsabilité civile.

7 – Langages et outils pour l’analyse des propriétés

Si l’on s’en tient aux propriétés rencontrées dans le paragraphe 5 (propriétés invariantes, propriétés temporelles, propriétés statistiques, propriétés floues) les outils actuels du projet qui peuvent s’utiliser sont répartis suivant le tableau ci-après :

Propriété	Outil et/ou langage
invariantes	B, Z, VDM, Focal
Temporelles / dynamiques	B événementiel
statistiques	-
floues ou imprécises	-

Pour les lignes 1 et 2 du tableau, les formalismes permettent l’expression des propriétés. Certains d’entre eux donnent les moyens de preuve de ces propriétés de manière déductive ainsi que l’assistant de preuve automatique ou de conduite de preuve interactive (par exemple l’atelier B et l’assistant Coq pour Focal).

Lexique de quelques termes techniques employés dans ce rapport et leur correspondant en anglais.

Le terme anglais est celui utilisé dans l'Annexe 17 [A17].

acte d'intervention illicite	act of unlawful interference
agents de réglementation	regulated agents
bagage de soute	hold baggage
cabine de pilotage	flight crew compartment
contrôles de sûreté	security controls
inspecter	to screen
points d'inspection/filtrage	(security) screening points
vérifications d'antécédents	background checks
zones de sûreté à accès réglementé	security restricted areas

Bibliographie

[A17] Annex 17 to the Convention on International Civil Aviation, 7th Edition, April 2002, International Civil Aviation Organization.

[CEDE] Proposition contractuelle EDEMOI, V1.0, octobre 2003

Table des matières

1 – Introduction	5
2 – Propriétés statiques : analyse descendante	5
3 – Relation de satisfaction entre propriétés	8
4 – Raffinement de propriétés	9
5 – Typologie des propriétés rencontrées.....	9
6 – Autres propriétés	10
7 – Langages et outils pour l’analyse des propriétés.....	11
Lexique de quelques termes techniques	12
Bibliographie.....	12