

Certification de réglementations régissant la sûreté des aéroports en utilisant l'environnement Focal

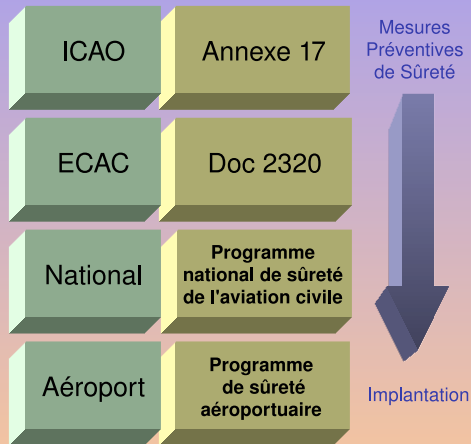
David Delahaye, Jean-Frédéric Étienne,
et Véronique Viguié Donzeau-Gouge

David.Delahaye@cnam.fr, etienneje@cnam.fr,
donzeau@cnam.fr

CEDRIC/CNAM, Paris

ANR SSURF & PPF «Logiciels Sûrs»

LIP6, Paris
7 novembre 2008



Caractéristiques

- Mesures de Sûreté : première ligne de défense contre les actes terroristes.
- La réglementation est organisée hiérarchiquement.
- Chaque niveau :
 - un ensemble de documents ;
 - une autorité de certification différente.
- Aspects essentiels au renforcement de la sûreté aérienne :
 - Processus de conformité ;
 - Qualité des documents normatifs.

Caractéristiques des normes

- Les documents normatifs sont :
 - Écrits en langage naturel ;
 - Bien structurés ;
 - Assez volumineux.
- Inconvénients du langage naturel :
Ambiguïtés, imprécisions, différentes interprétations.
- Conséquences :
 - Difficile de s'assurer qu'il n'y a pas d'incohérences dans la réglementation ;
 - Difficile d'analyser l'impact des changements sur la sûreté ;
 - Difficile d'évaluer la conformité envers les normes en vigueur.

Propriété fondamentale de l'Annexe 17

*4.1 Each Contracting State shall establish measures to prevent weapons, explosives or any other dangerous devices, articles or substances, which may be used to commit an act of unlawful interference, **the carriage or bearing of which is not authorized**, from being introduced, by any means whatsoever, on board an aircraft engaged in civil aviation. {Annexe 17}*



Interprétation (a)

*The carriage or bearing of weapons, explosives or any other dangerous devices is **NEVER** authorized on board.*



Interprétation (b)

*Weapons, explosives or any other dangerous devices may **not** be introduced on board **UNLESS** their carriage or bearing is authorized*

{Bonne Interprétation}

Objectifs

Intégrer et appliquer plusieurs techniques de RE et FM pour analyser des réglementations régissant la sûreté des aéroports :

- Améliorer la qualité des documents normatifs ;
- Faciliter la maintenance et l'évolution des normes ;
- Définir un processus rigoureux d'évaluation.

Contributions (thèse J.-F. Étienne)

- Construction et validation des modèles formels de l'Annexe 17 et de la Doc 2320 en utilisant l'environnement Focal ;
- Transformation automatique des modèles Focal vers UML (documentation graphique).

Cas d'étude

Un sous-ensemble significatif de la réglementation :

- Activités effectuées tout au long du processus d'embarquement (passagers, bagages, personnel au sol, équipages, avions en partance) ;
- Activités relatives au fret ou effectuées en vol ne sont pas considérées.

Application d'une méthode à la KAOS

- La réglementation est organisée en une hiérarchie de propriétés en :
 - Identifier les propriétés fondamentales de sûreté et voir comment elles se déclinent en sous-propriétés ;
 - Comprendre comment les sous-propriétés sont suffisantes pour satisfaire les propriétés fondamentales.
- Mise en évidence des hypothèses cachées.

Propriété fondamentale de sûreté

2.2.1 Se protéger contre des actes d'intervention illicite.

Étayée par les mesures préventives décrites dans le chap. 4 de l'Annexe 17 :

4.1 Il n'y a pas d'objets dangereux non autorisés à bord des avions.

La relation de causalité met en évidence l'hypothèse suivante :

Hypothèse (A1). *Les actes d'intervention illicite ne peuvent se produire qu'à l'aide d'un objet dangereux.*

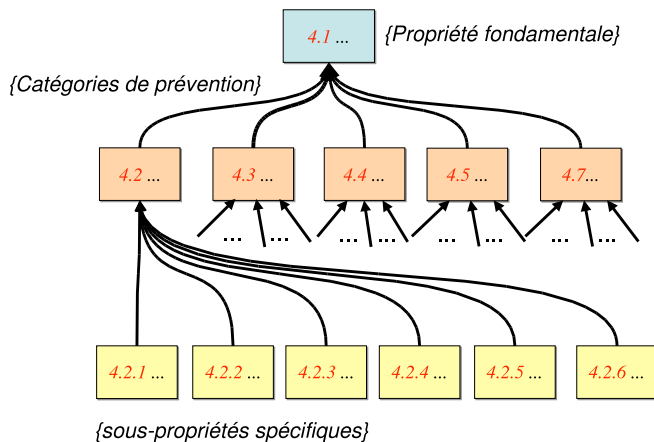
$$(4.1), (A1) \vdash (2.1.1)$$

Décomposition de la propriété 4.1

- Mesures relatives au contrôle d'accès (A17, 4.2) ;
- Mesures applicables aux avions (A17, 4.3) ;
- Mesures applicables aux passagers ordinaires (A17, 4.4) ;
- Mesures applicables aux bagages de soute (A17, 4.5)
- Mesures applicables aux frets et autres marchandises (A17, 4.6) ;
- Mesures applicables à des catégories spéciales de passagers (A17, 4.7).

(4.2), (4.3), (4.4), (4.5), (4.7) \vdash (4.1)

Différentes décompositions



Doc 2320 vs Annexe 17

- Le structure de la Doc 2320 suit celle du chapitre 4 de l'Annexe 17 ;
- De nouvelles propriétés ajoutées ;
- Chaque propriété de l'Annexe 17 est raffinée selon les cas suivants :
 - Est reformulée mais contient la même information ;
 - Devient plus précise et parfois plus restrictive ;
 - Est décomposée en plusieurs sous-propriétés ;
 - Est partiellement (ou pas) considérée (Annexe 17 toujours applicable).

Quelques exemples de raffinement

Propriété plus restrictive

A17, 4.2.6. Un échantillon représentatif de personnes (autres que les passagers) auxquelles est accordé un accès aux zones de sûreté doit être inspecté-filtré.

D2320, 2.3(a). Tous les membres du personnel, y compris l'équipage, doivent être inspectés-filtrés avant d'être autorisés à pénétrer dans les zones de sûreté.

$$(D2320, 2.3(a)) \sqsubseteq (A17, 4.2.6)$$

Raffinement partiel

A17, 4.2.3. L'identité des personnes et véhicules doit être vérifiée aux points de contrôle désignés avant d'autoriser l'accès à des zones de sûreté.

D2320, 2.2.1(viii). L'identité du personnel et les laissez-passer des véhicules sont contrôlés à tous les points d'accès aux zones de sûreté.

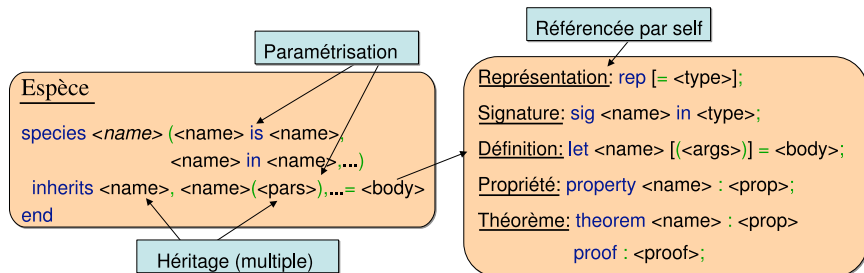
$$(D2320, 2.2.1(viii)) \not\sqsubseteq (A17, 4.2.3)$$

Modélisation : l'environnement Focal

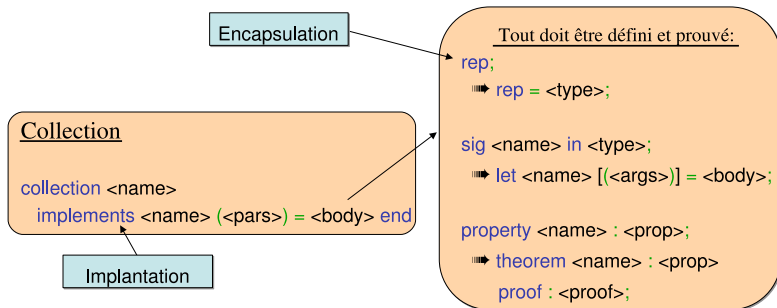
Qu'est-ce que Focal ?

- Système de développement d'applications certifiées ;
- Orienté objets (héritage et paramétrisation) ;
- Orienté spécifications algébriques (ensemble support) ;
- Prouveur automatique (Zenon), vérification (Coq).

Spécification : les espèces



Implantation : les collections



Le compilateur Focal : quatre types de sortie

- Code Ocaml pour l'exécution ;
- Code Coq pour la certification ;
- Code FocDoc (format XML) pour la documentation ;
- Graphes d'héritage et de dépendance.

Vocabulaire approprié

Modéliser l'environnement réglementé :

- Identifier les sujets/objets, leurs relations, propriétés et attributs.
- Déterminer une classification préservant la nomenclature des documents :
 - Traçabilité ;
 - Factorisation.

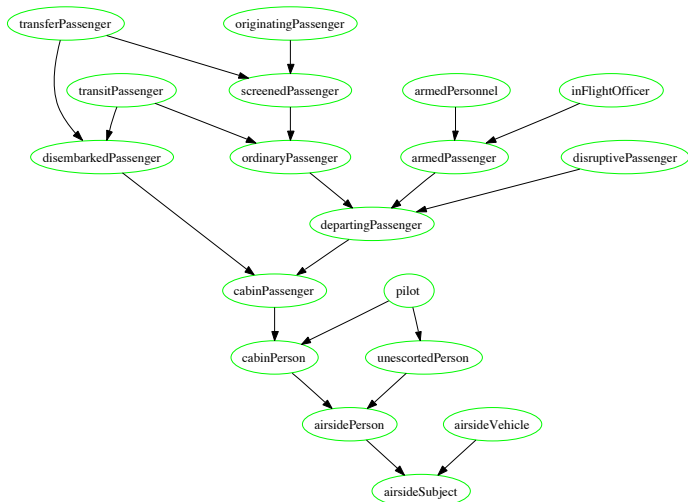
Un exemple

A17, 4.2.3 L'identité des **personnes** et **véhicules** doit être **vérifiée** aux points de contrôle désignés avant d'**autoriser** l'accès à des **zones de sûreté**.

Hiérarchie de sujets \equiv Hiérarchie Focal

- Chaque sujet \equiv une espèce
- Représentations et fonctions non définies

Sujets pouvant accéder aux zones «côté piste»



Sujets pouvant accéder aux zones situées «côté piste»

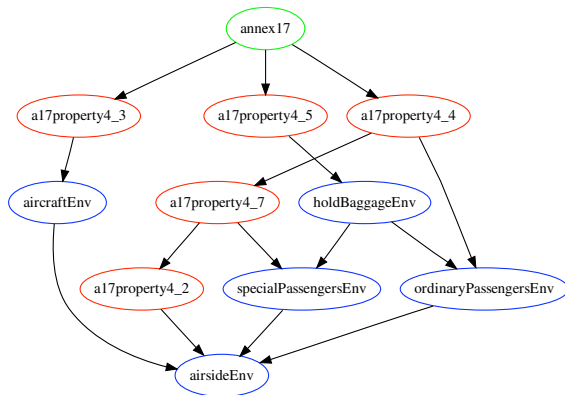
```
species airsideSubject (obj is object,  
                        obj_set is finite_set (obj)) inherits setoid =  
  sig identityVerified in self → bool;  
  sig objects_carried in self → obj_set; ...  
end
```

Zones de sûreté

```
species securityRestrictedArea  
  (obj is object, obj_set is finite_set (obj),  
   as is airsideSubject (obj, obj_set), as_set is finite_set (as), ...,  
   d_aircraft is departingAircraft (obj, obj_set, ...),  
   dep_ac_set is finite_set (d_aircraft)) inherits setoid =  
  sig airsideSubjects_in_sra in self → as_set;  
  sig access_authorized in as → self → bool;  
  sig departingAircraft_in_sra in self → dep_ac_set;  
  
  property depAircraft_subjects_in_sra : all s in self, all a in d_aircraft,  
    dep_ac_set!member (a, !departingAircraft_in_sra (s)) →  
      all p in as, d_aircraft!accessing_aircraft (p, a) →  
        as_set!member (p, !airsideSubjects_in_sra (s)); ...  
end
```

Structure du modèle \equiv Hiérarchie de propriétés établie

- Héritage et paramétrisation ;
- Espèce \equiv Catégorie de prévention (limité aux sujets réglementés) ;
- Propriétés de sûreté \equiv Invariants du modèle

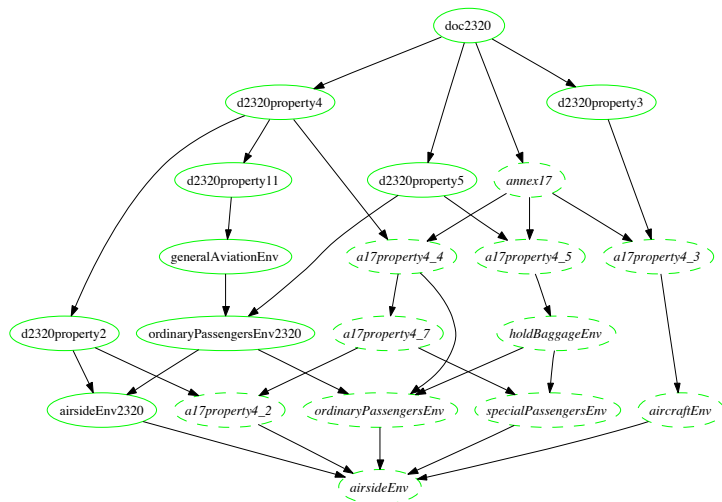


Raffinement du domaine de l'Annexe 17

- De nouveaux sujets ajoutés ;
- Les propriétés/attributs des sujets existants sont étendus.



Par extension du modèle de l'Annexe 17



Correction

Les mesures préventives de sûreté sont suffisantes pour satisfaire les fondamentales \equiv Une propriété fondamentale de sûreté est impliquée par ses sous-propriétés.

Complétude

Les mesures préventives de sûreté sont nécessaires pour satisfaire les fondamentales \equiv Une propriété fondamentale de sûreté n'est plus satisfaite lorsque l'une de ses sous-propriétés est omise.

Mesures relatives au contrôle d'accès

$(4.2.1), (4.2.3), (4.2.4), (4.2.5), (4.2.6) \vdash (4.2)$

4.2. Les personnes (autres que les passagers) et véhicules accédant aux avions sont dignes de confiance.

Hypothèses cachées

$(4.2.1), (4.2.3), (4.2.4), (4.2.5), (4.2.6), (A2), (A3), (A4), (A5) \vdash (4.2)$

(A2) Les personnes non accompagnées ne peuvent accéder aux avions que si leurs identités et antécédents sont vérifiés.

(A3) Les personnes non accompagnées sont considérées comme dignes de confiance et ne transportent pas d'objets dangereux non autorisés.

(A4) Les véhicules ne peuvent accéder aux avions que si leurs identités sont vérifiées.

(A5) Les véhicules identifiés sont considérés comme dignes de confiance et ne transportent pas d'objets dangereux non autorisés.

Théorèmes de raffinement

Ils assurent que les niveaux inférieurs ne sont pas moins restrictifs que les niveaux supérieurs.

$$(D2320, 2.3(a)) \sqsubseteq (A17, 4.2.6)$$

A17, 4.2.6. Un échantillon représentatif de personnes (autres que les passagers) auxquelles est accordé un accès aux zones de sûreté doit être inspecté-filtré.

D2320, 2.3(a). Tous les membres du personnel, y compris l'équipage, doivent être inspectés-filtrés avant d'être autorisés à pénétrer dans les zones de sûreté.

Objectifs

Un cadre formel pour la réalisation d'un outil de traduction automatique de Focal vers UML :

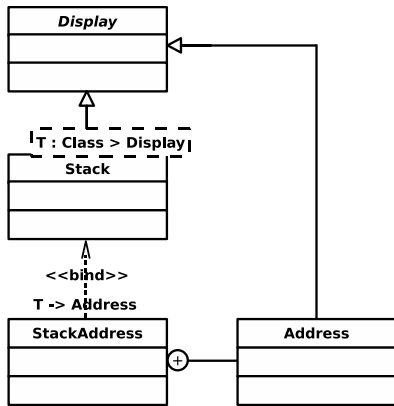
- 1 Formaliser un sous-ensemble des structures statiques d'UML 2.1 ;
- 2 Étendre le métamodèle d'UML pour considérer la sémantique de Focal ;
- 3 Décrire les règles de transformation de Focal vers UML.

Correction de la transformation

- 1 Les contraintes spécifiées dans le profil Focal n'invalident pas le métamodèle d'UML ;
- 2 Le modèle UML généré à partir d'une spécification Focal bien typée respecte :
 - Les règles de bonne formation d'UML ;
 - Les contraintes du profil Focal.

Définition d'une Syntaxe Abstraite pour UML

Notation UML



Syntaxe BNF

```
public abstract class Display = end
public class Stack ( T : class > Display )
    inherits Display = end
public class StackAddress
    binds Stack < T → Address > =
    public class Address
        inherits Display = end
end
```

Un profil pour Focal

- Besoin de considérer les spécificités sémantiques de Focal pour documenter correctement les modèles Focal en UML ;
- Utilisation d'un mécanisme de profil pour adapter le métamodèle d'UML :
 - Définir des stéréotypes pour refléter la sémantique de chaque construction Focal («Species», «Collection», «ParameterizedInheritance», ...);
 - Encoder la sémantique relative au template binding :
O. Caron et al. *An OCL Formulation of UML2 Template Binding* (UML04) ;
Extension pour considérer les *bound* classes imbriquées et les membres héritées ;
 - Introduire les classes Fun et Pair pour modéliser les types fonctionnels et produits.

Une spécification : l'espèce cabinPerson

```
species cabinPerson (cb is cabinBaggage) =  
  rep ;  
  sig equal in self → self → bool ;  
  sig identityVerified in self → bool ;  
  sig cabinBaggage in self → cb ;  
  property equal_reflexive :  
    all x in self, !equal (x, x); ...  
end
```

Une implantation : la collection cabinPerson_col

```
collection cabinPerson_col implements cabinPerson (bag) =  
  rep = string * bag * bool ;  
  let name (s in self) in string = #first (s) ;  
  let cabinBaggage (s in self) in bag = #first (#scnd (s)) ;  
  let identityVerified (s in self) in bool =  
    #scnd (#scnd (s)) ; ...  
end
```

Traduction

```
| CbT : Class  
| CbSelf : Class  
| <<Is>> Cb : Class >> CabinBaggage<CbT, CbSelf>  
| T : Class  
| TSelf : Class
```

<<Species>>
CabinPerson

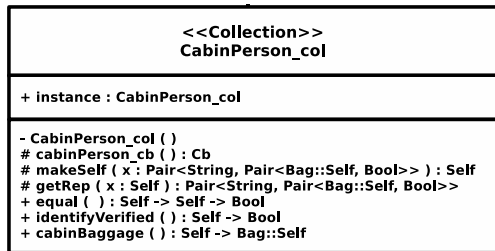
```
# cabinPerson_cb ( ) : Cb  
# makeSelf ( x : T ) : TSelf  
# getRep ( x : TSelf ) : T  
+ equal ( ) : TSelf -> TSelf -> Bool  
+ identifyVerified ( ) : TSelf -> Bool  
+ cabinBaggage ( ) : TSelf -> CbSelf
```

equal_reflexive
{all x in self, !equal(x, x)}

Traduction



CbT -> Int, CbSelf -> Bag::Self, Cb -> Bag,
T -> Pair<String, Pair<Bag::Self, Bool>>, TSelf -> CabinPerson_col::Self



FocDoc

Format XML utilisé par le compilateur Focal pour la documentation.
L'information est extraite :

- De la syntaxe abstraite de Focal ;
- Des commentaires structurés annotant les spécifications Focal ;
- De l'inférence de type et de l'analyse de dépendance effectué par le compilateur.

Deux parties

- 1 Profil UML pour Focal spécifié avec le plug-in UML2 d'Eclipse ;
 - Utilisation du vérificateur OCL intégré pour valider les contraintes du profil ;
 - Utilisation de la définition du profil statique pour fournir une implantation aux opérations et aux attributs dérivés caractérisant chaque stéréotypes du profil.
- 2 Stylesheet XSLT encodant les règles de transformation.
D'une spécification Focal en FocDoc vers un modèle UML en XMI.

Modèles Focal

- Structuration (héritage et paramétrisation)
 - Traçabilité avec les documents normatifs
 - Distinction entre les propriétés de sûreté et la mise en oeuvre
- Support de raisonnement automatique (Zenon)
 - 90% des obligations de preuves réalisées automatiquement
 - Théorèmes de correction et de raffinement :
 - clarifier certaines ambiguïtés ;
 - identifier des hypothèses cachées ;
 - démontrer que les propriétés de la Doc 2320 raffinent correctement l'Annexe 17.
- Développement
 - 10,000 lignes de code, 150 espèces, 200 propriétés/théorèmes

Schéma de transformation de Focal vers UML

- Une syntaxe abstraite pour un sous-ensemble d'UML 2.1 ;
- Une formalisation complète de la sémantique des structures Focal ;
- Documentation graphique pour les développeurs :
 - Interprétation commune des modèles formels ;
 - Autre forme de validation.
- Correction de la transformation.

Contradictions

- Théorèmes de correction/raffinement : pas une garantie d'absence de contradictions
- Une solution : essayer de dériver *faux* à partir des propriétés de sûreté avec Zenon
- Approche naïve mais pertinente pour considérer les scénarios d'attaques (autre forme de complétude) :
 - FocalTest (M. Carlier et C. Dubois) pour générer les scénarios
 - Zenon + techniques de déviations (analyse d'obstacles) pour simuler les attaques.

Diagrammes UML

- Modèles plus abstraits pertinents pour les autorités de certification
- Modèles dynamiques (diagrammes de séquences/états-transitions) à travers l'analyse statique