LSR

Modeling Airport Security: the EDEMOI project

Yves Ledru

LSR/IMAG et Univ. Grenoble-1

Participants :

- Cedric/CNAM et LACL
- GET/ENST Paris
- LIFC
- LSR/IMAG
- ONERA /Centre de Toulouse

Journées PariStic
Bordeaux
22 novembre 2005

ACI Sécurité & Informatique

« The last line of defence »

LSR

- Despites the 9/11 attacks, commercial aviation remains one of the safest and most secure ways of transportation.
- The EDEMOI project focuses on airport security.

« CATSA is the last line of defence before passengers and their belongings board an aircraft. »
Jacques Duchesneau, C.M., President and CEO, Canadian Air Transport Security Authority,
Senate Special Committee on the Anti-Terrorism Act
November 14, 2005

« airport security screeners - the people on the front lines of protecting our airports and the traveling public »
Congresswoman Diana DeGette of Colorado

Crédit photo : FOTAIR

... against teddy bears!

LSR

Credit photo : TSA

Airport screeners find loaded gun in teddy bear

From Patty Davis and Beth Lewandowski

CNN, July 17th 2003

WASHINGTON (CNN) -- Screeners at a passenger checkpoint at the Orlando International Airport last Friday found a loaded handgun hidden inside a stuffed teddy bear belonging to a 10-year-old boy, the Transportation Security Administration has told CNN.

And also…

Credit photo : TSA

And also… (2)

Credit photo : TSA

Quelques chiffres

LSR

The Transportation Security Administration, a federal agency formed in November 2001, oversees 45,000 airport screeners.

Every month, those screeners find

175,000 knives,

more than 2,000 rounds of live ammunition,

70 guns,

and hundreds of razor blades, swords and box cutters,

according to the TSA.

(CNN, Jan 18th 2005)

A stack of responsibilities

LSR

Documents which describe airport security are organized hierarchically

ICAO/ OACI	Annex 17
ECAC/ UE AC	Document 30, Règl. 2320
National bodies	National laws
Airport	Safety programs

Credit Photo : FOTAIR

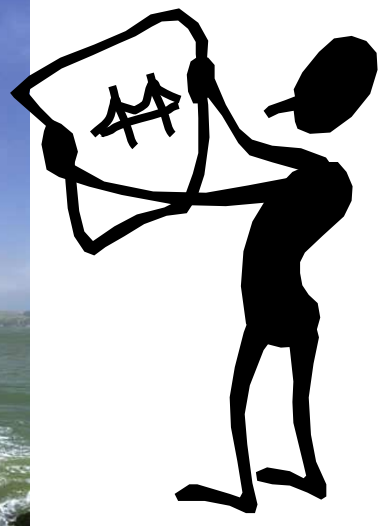
Two key elements to achieve security:

- –Conformance to the standards
- –Quality/Consistency/Completeness of the standards

The EDEMOI approach

LSR

- Engineers build models to reason about their artefacts.



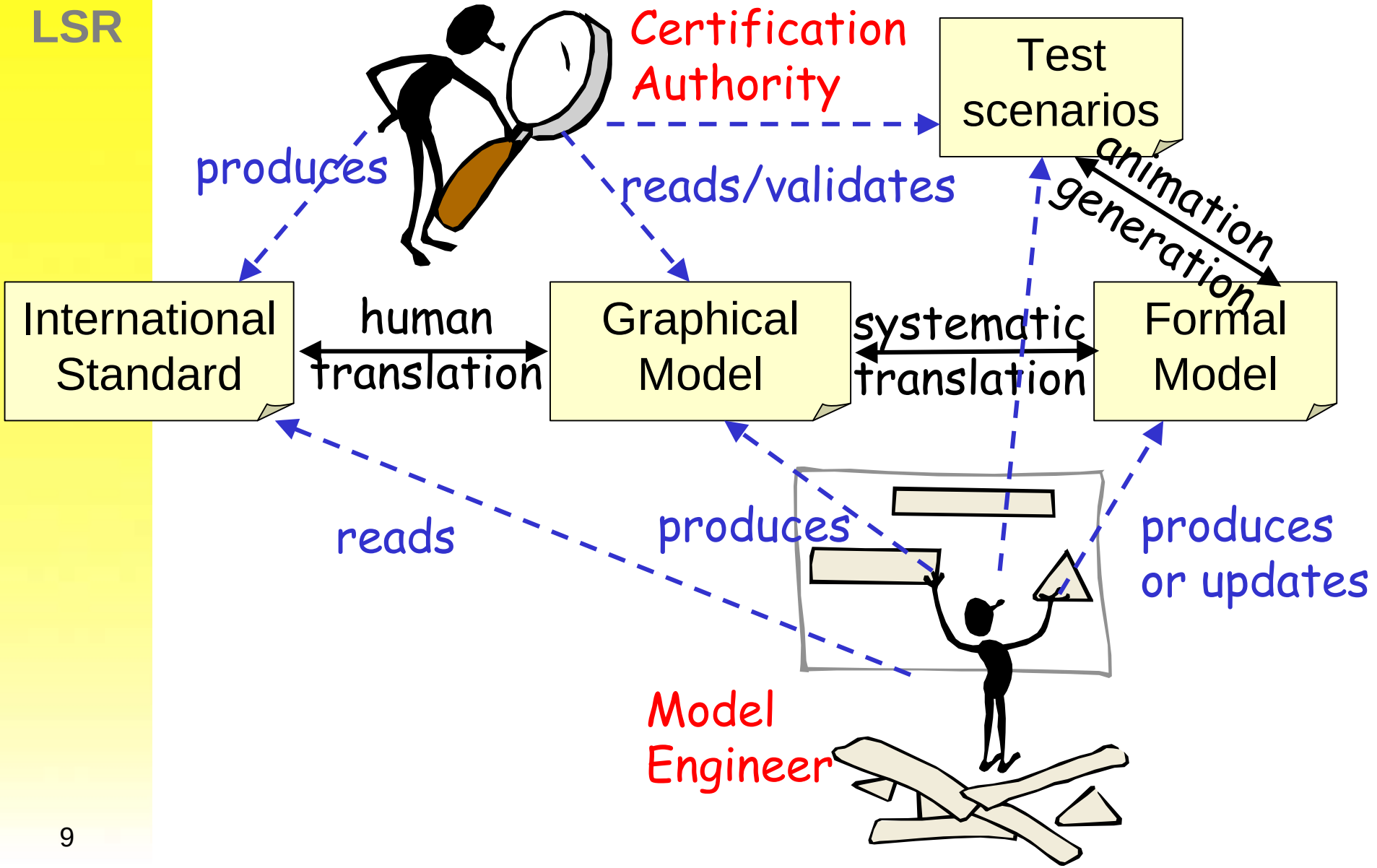
- Goal of the project:

  To express parts of standards as a set of precise models

  – Using modeling techniques from the computer science community
  – Using tools to assess the consistency of models and to extract « test cases »

The EDEMOI stakeholders

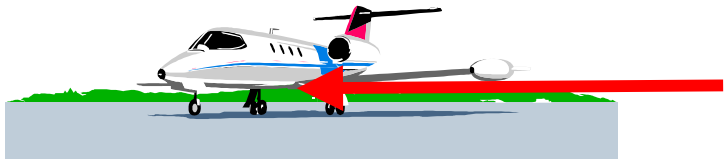
LSR



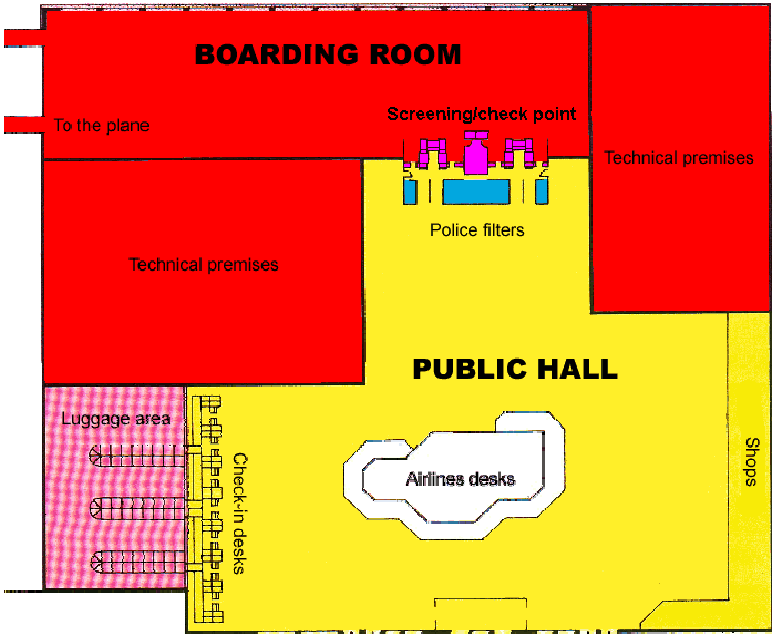
Scope of the project

LSR

- A significant subset of the airport:
  - The areas crossed by passengers from check-in to boarding gate
  - + from the boarding gate to the aircraft



Crédit Photo : Eric Saillet



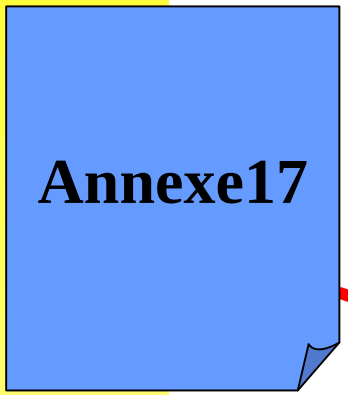
Goals of the project

LSR

- Motivation/objectives:
  - Provide a formal and structured reference document
  - Check/Test for the absence of errors
- Usefulness of the approach for certification authorities
  - Reference model and support for tutorial activies
  - Identification of hidden assumptions
  - Support the evolution of standards
  - Show the correctness of simplified procedures
  - Provide support for conformance checking of a given airport to the international standards (through test generation)

The EDEMOI process

LSR



Step 1 :
Goals are identified
as security properties

Hierarchy of
Security properties

Step 2 :
Class diagrams
link goals to
relevant domain
elements

UML diagrams
(with UML profile)

Step 3 :
Class diagrams
are linked to
formal specifications

Formal
Specifications
(B and Focal)

Step 4 :
Tests are generated
from the formal
models

Test cases

Step 1 : identification of security properties

LSR

The primary security property can be stated as follows:

P1 : Passengers, crew, ground personnel and the general public must be safeguarded against acts of unlawful interference (article 2.1.1, 2nd chapter of Annex 17)

Set of preventive measures to achieve this goal (article 4.1, 4th chapter of Annex 17)

Each Contracting State shall establish measures to prevent weapons, explosives or any dangerous devices 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 international civil aviation.

Security Properties Identification (2)

LSR

•Translated by the following property :

P2 : There are no unauthorized objects on board an aircraft.

•P2 refines P1 assuming two hypotheses :

H1 : Acts of unlawful interference can only be committed with weapons, explosives or any other dangerous devices.

(**IMPLICIT

H2 : Each St
performed in

(clearly sta

Projets d'attentats en France selon Le Figaro

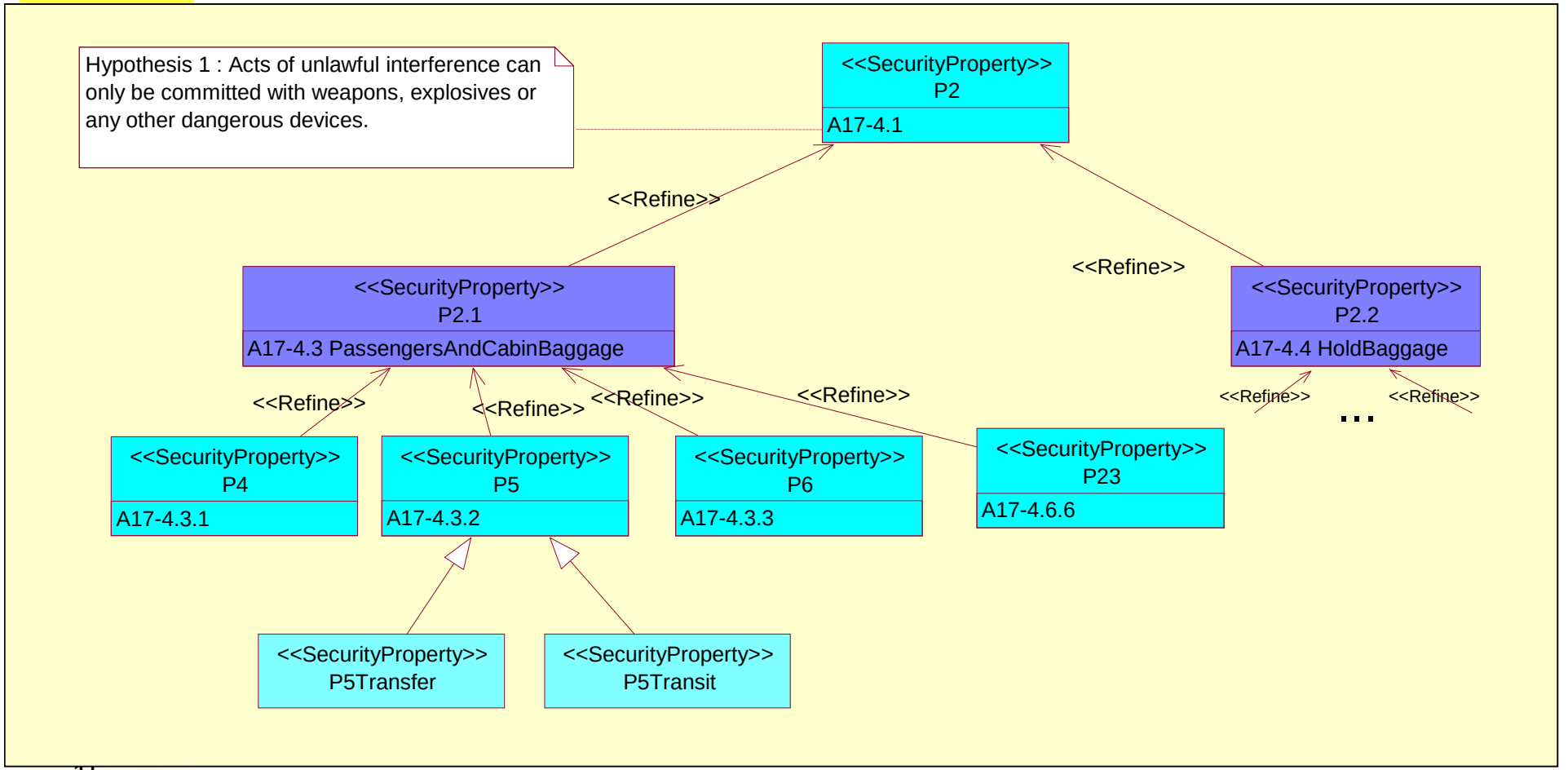
AFP - (lalibre.be, Mis en ligne le 28/10/2005)

« Des islamistes français ont l'intention de commettre des attentats contre des avions civils en France à l'aide de deux missiles sol-air, a affirmé vendredi le quotidien français Le Figaro, alors que de source proche du dossier on a estimé ce risque à zéro. »

A tree of properties

LSR

Expressed as UML stereotyped classes.



Natural Language imprecision

LSR

*"4.1 Objective -- Each Contracting State shall establish measures to prevent weapons, explosives or any other dangerous devices 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 international civil aviation."*

The french translation is not ambiguous…

*4.1 Chaque Etat contractant prendra des mesures pour empêcher que des armes, explosifs ou tous autres engins dangereux pouvant être employés pour commettre un acte d'intervention illicite, **et** dont le port ou le transport n'est pas autorisé, ne soient introduits, par quelque moyen que ce soit, à bord d'un aéronef effectuant un vol d'aviation civile internationale.*

Step 2 : UML Class Diagram

LSR

Use of a goal-oriented requirements process

- identification of goals (security properties) :
  - identification of the main goals
  - identification of their sub-goals
  - construction of a *refinement* graph

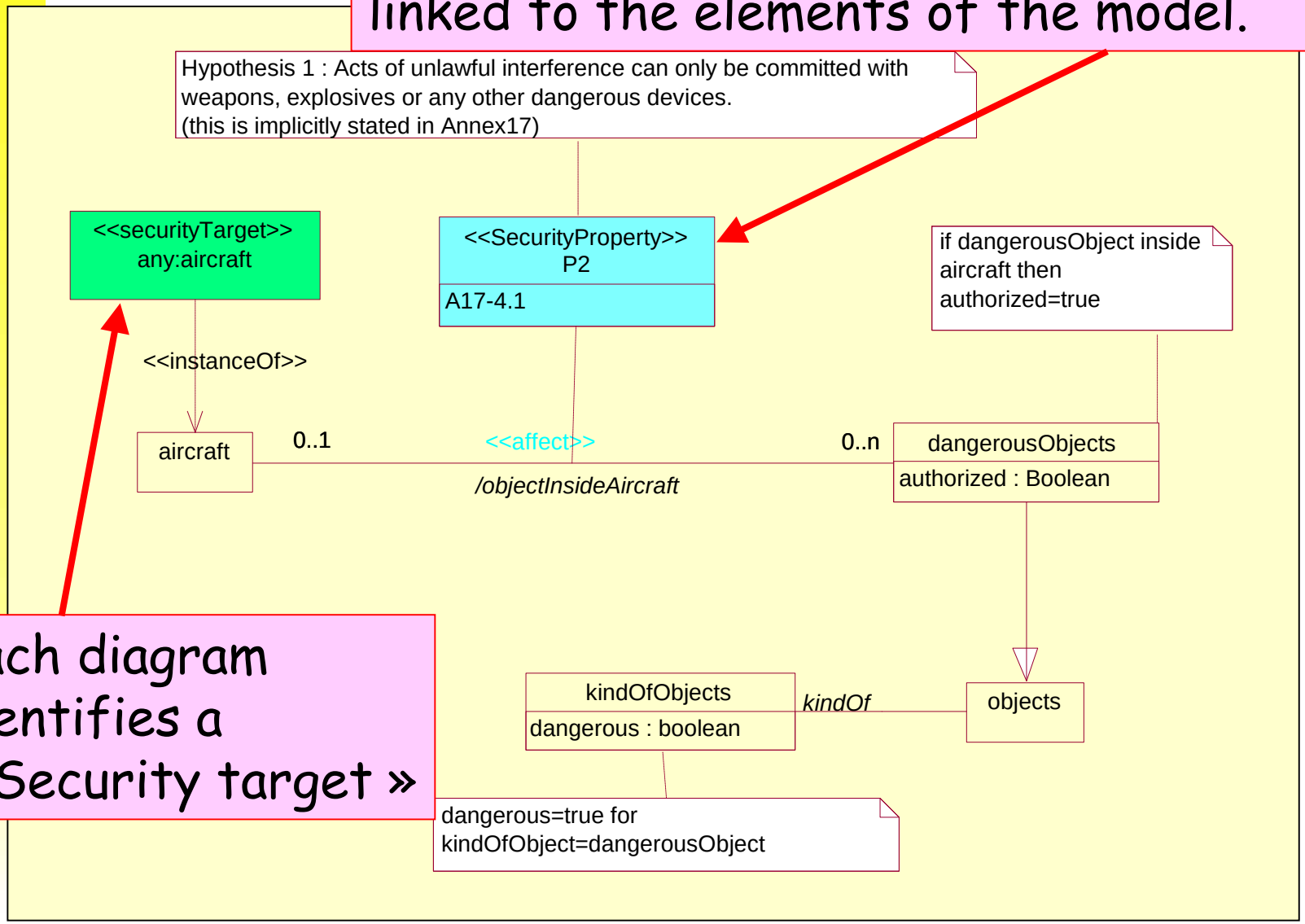
- construction of the domain model :
  - determination of the domain objects, their relationships and attributes
  - links with the security properties

- construction of the agent model : an agent is responsible for the satisfaction of security properties.

Step 2 : UML class diagrams

LSR

Properties appear as stereotyped classes linked to the elements of the model.

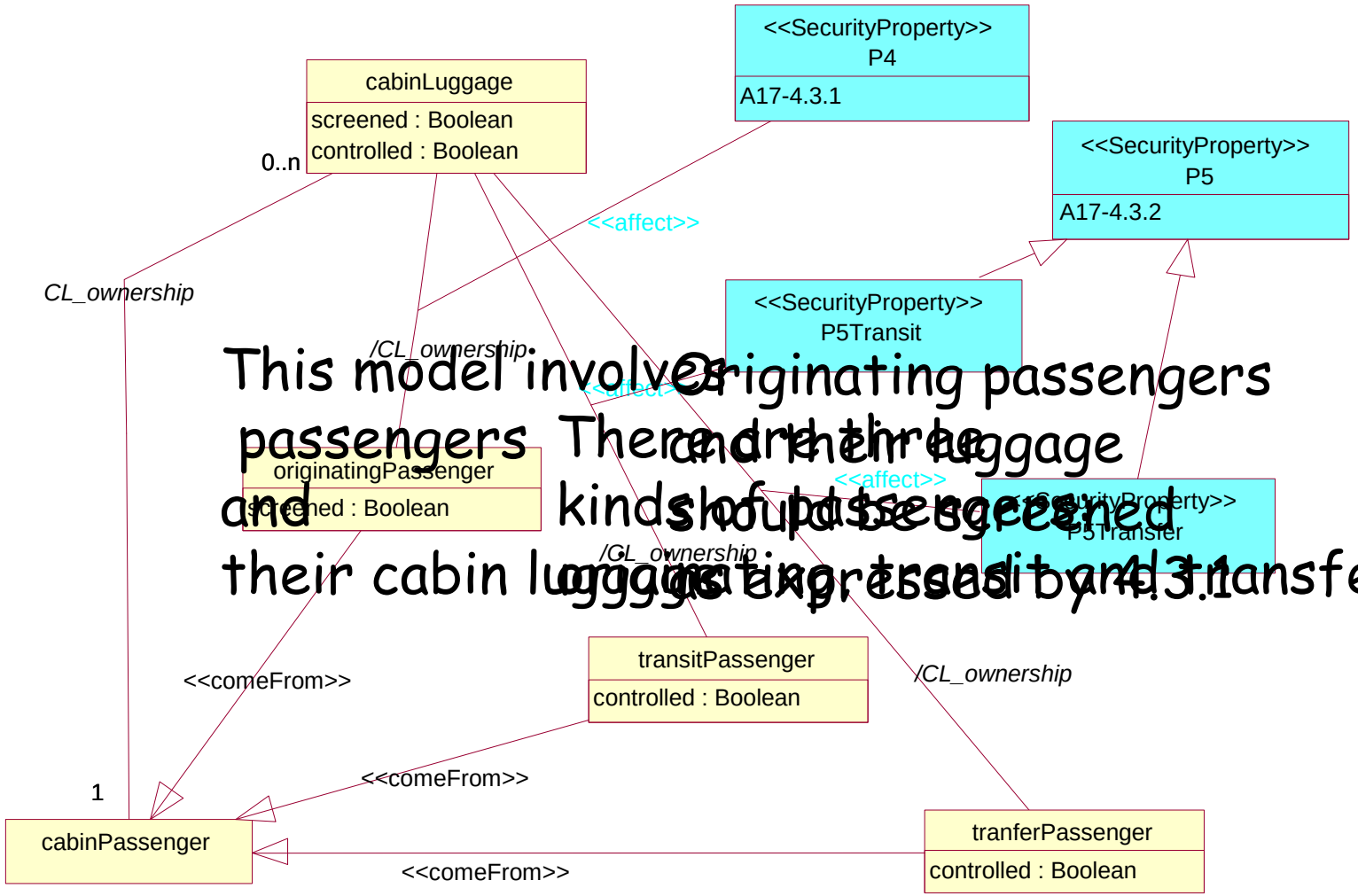


Each diagram identifies a « Security target »

Another diagram

LSR

Other passengers and luggage are controlled (4.3.2)

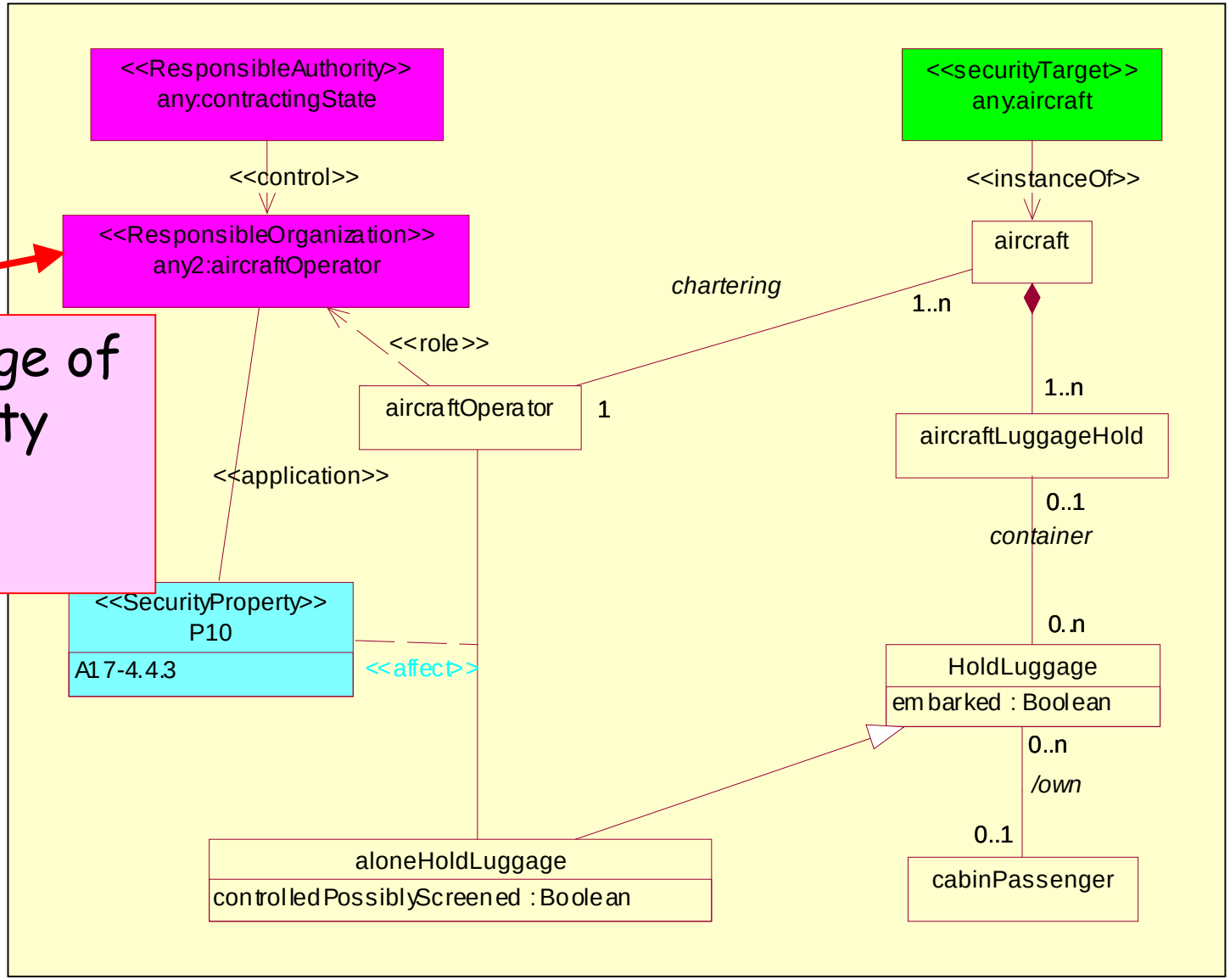


This model involves originating passengers and their luggage and transit passengers. There are three kinds of passengers and should be screened their cabin luggage is expressed by 4.3.1

Identification of agents

LSR

Agents in charge of applying security properties are identified



Step 3 : Formal Specifications

LSR

- Two formal models are under development
  - A B model focusing on Annex 17
  - A Focal model which links several levels of abstraction (in connection with the ModuLogic project)
- Both models have been extensively proven.
- Link between Formal Models and UML:
  - B/UML tool based on concept formation techniques
  - Focal/UML tool
  - The forward link (UML to Formal methods) remains a difficult problem!
    - Due to the size of the model
    - Due to extensive use of stereotypes in our UML profile.

Step 3 : Formal specifications (B)

LSR

- 4 modules (1 spec + 3 refinements)
- 827 lines
- 253 proofs

```
boarding_in_cabin =
ANY fl, pp WHERE
  fl ∈ departure_flights ∧ pp ∈ Passengers ∧
  pp ∈ dom(passenger_flight) ∧ passenger_flight(pp) = fl ∧
  pp ∉ dom(passenger_on_board)
THEN
  IF (hand_baggage(pp) ∩ dangerousObjects) ⊆
    authorized_in_cabin(passenger_flight(pp))^-1 [{ok}]
  THEN
    passenger_on_board := passenger_on_board ∪ {pp → fl}
  END
END
```

```
MACHINE
    SecureFlight_syst
SETS
    Objects
CONCRETE_CONSTANTS
    unauthorized_in_cabin,
    unauthorized_in_hold
PROPERTIES
    unauthorized_in_cabin ⊆ Objects ∧
    unauthorized_in_hold ⊆ Objects
VARIABLES
    in_cabin, in_hold
INVARIANT
    in_cabin ⊆ Objects ∧
    in_hold ⊆ Objects ∧
    in_cabin ∩ unauthorized_in_cabin = ∅ ∧
    in_hold ∩ unauthorized_in_hold = ∅
INITIALISATION
    in_cabin, in_hold := ∅ , ∅
OPERATIONS
    loading_in_cabin =          /* loading objects in cabin */
    ANY oo WHERE
        oo ⊆ Objects ∧ oo ∩ unauthorized_in_cabin= ∅
    THEN
        in_cabin := in_cabin ∪ oo
    END ;
    loading_in_hold =           /* loading objects in hold */
    ANY oo WHERE
        oo ⊆ Objects ∧ oo ∩ unauthorized_in_hold= ∅
    THEN
        in_hold := in_hold ∪ oo
        END
END
```

Step 3 : Formal Specifications (Focal)

LSR

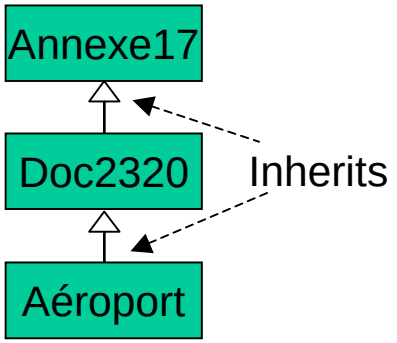
- Covers three levels of abstraction
- 16 modules
- 4157 lines
- 35 proofs using Coq or Zenon (Modulogic)

```
letprop property_4_3_1_2(s in self) =
    all bp in brd_passenger,
        brd_set!member(bp,!get_boardingPassengers(s)) ->

((ex p in o_passenger,
   op_set!member(p,!get_originatingPassengers(s)) and
    not(#is_failed(!control_originating(p))) and
    brd_passenger!equal(#non_failed(!control_originating(p)),bp)) or

(ex p in ts_passenger,
   ts_set!member(p,!get_transitPassengers(s)) and
    not(#is_failed(!control_transit(p))) and
     brd_passenger!equal(#non_failed(!control_transit(p)),bp)) or

(ex p in tf_passenger,
   tf_set!member(p,!get_transferPassengers(s)) and
    not(#is_failed(!control_transfer(p))) and
      brd_passenger!equal(#non_failed(!control_transfer(p)),bp)));
```



Step 4 : Test generation

LSR

- Testing based on the B specification
- 2 approaches :
  - Generation of conformance tests with BZTT
    - Will be turned into checks for airport inspectors
    - Or self evaluation of airports
  - User defined test cases to validate the models
    - Modeling « attacks »
    - Used to detect regressions in evolutions
- Experiences have shown that test cases can be validated by certification authorities

Step 4 : Test generation (BZTT)

LSR

Here is a set of test cases generated from a early version of the B specification.

	Preamble	Body
1		*check_in_desk_registration(pp=p_1,bbb={b_2})* *check_in_desk_registration(pp=p_1,bbb={b_2,b_4})*
2	*check_in_desk_registration(pp=p_1,bbb={b_2})*	*passing_the_screening_point(pp=p_1)*
3	*check_in_desk_registration(pp=p_1,bbb={b_2})* *passing_the_screening_point(pp=p_1)*	*loading_in_cabin(pp=p_1)*
4	*check_in_desk_registration(pp=p_2,bbb={b_1})*	*controling_baggage(bb=b_1)*
5	*check_in_desk_registration(pp=p_2,bbb={b_1})*	*screening_baggage(bb=b_1)*
6	*check_in_desk_registration(pp=p_2,bbb={b_1})* *screening_baggage(bb=b_1)*	*loading_in_hold(bb=b_1)*
7	*check_in_desk_registration(pp=p_1,bbb={b_2})* *passing_the_screening_point(pp=p_1* *loading_in_cabin(pp=p_1)* *controling_baggage(bb=b_2)*	*loading_in_hold(bb=b_2)*

Current Results

LSR

- A requirements engineering approach based on a specific UML profile (published at SREP'05)
- Detection of several NL imprecisions.
- 3 models of Annex 17 of ICAO/OACI
  - 17 UML diagrams
  - B specification (4 Composants, 827 Lines, 253 Proofs)
  - Focal specification (16 Modules, 4157 Lines, 35 Proofs)
- Significant investment of the project members to adapt to a new domain.
- On-going contacts with the certification authorities ICAO/OACI and ECAC/CEAC

Further work

LSR

- Model the next release of A17
  - Evaluation of non-regression
  - Collaboration with ICAO/OACI
- Refinements of A17
  - European 2320 and Security Manual of ICAO
- Focus on testing activities
  - Generate checklists for inspectors
    - Two inspectors should not reach contradictory conclusions about the same airport
  - Autoevaluation toolkit
    - To prepare for audits and inspections
- Better link between UML and formal models
  - Forward tools must be revisited
  - Promising reverse engineering tools
- Adapt the EDEMOI approach to other application domains

Credits

LSR

- The photos used in this presentation were provided by
  - L’aéroport de Lyon Saint Exupéry
  - TSA (Transport Security Administration, USA)