Une étude de cas pour la vérification formelle de propriétés temporelles

Frédéric Boniol & François Carcenac
ONERA CERT / DTIM

FAC 2002

(travail réalisé dans le cadre d'une étude financée par Dassault Aviation)

Introduction

- **Objectif de l'exposé :**
  - proposer **une étude de cas** aux groupes SVF et SE de FéRIA

  => intéressante pour
    - étudier la formalisation du temps dans un système embarqué
    - étudier la vérification de systèmes à forte combinatoire

- **L'étude de cas**
  - **Origine** : Dassault Aviation (projet GENIE en collaboration avec INRIA)
  - **Fonction** : pilotage de l'atterrisseur d'un avion de type Mirage

  => purement réactif avec des contraintes de temps importantes

Introduction

- **Les tentatives de vérification sur l'étude de cas…**
  - 20 propriétés à démontrer
  - **échec** de la tentative de vérification pour 2 d'entre–elles avec les model checker des langages synchrones…

  (Remarque : les 18 autres ont été démontrées correctes avec ces mêmes model checker)
  - **réussite** de la vérification pour ces 2 propriétés avec SMV, …

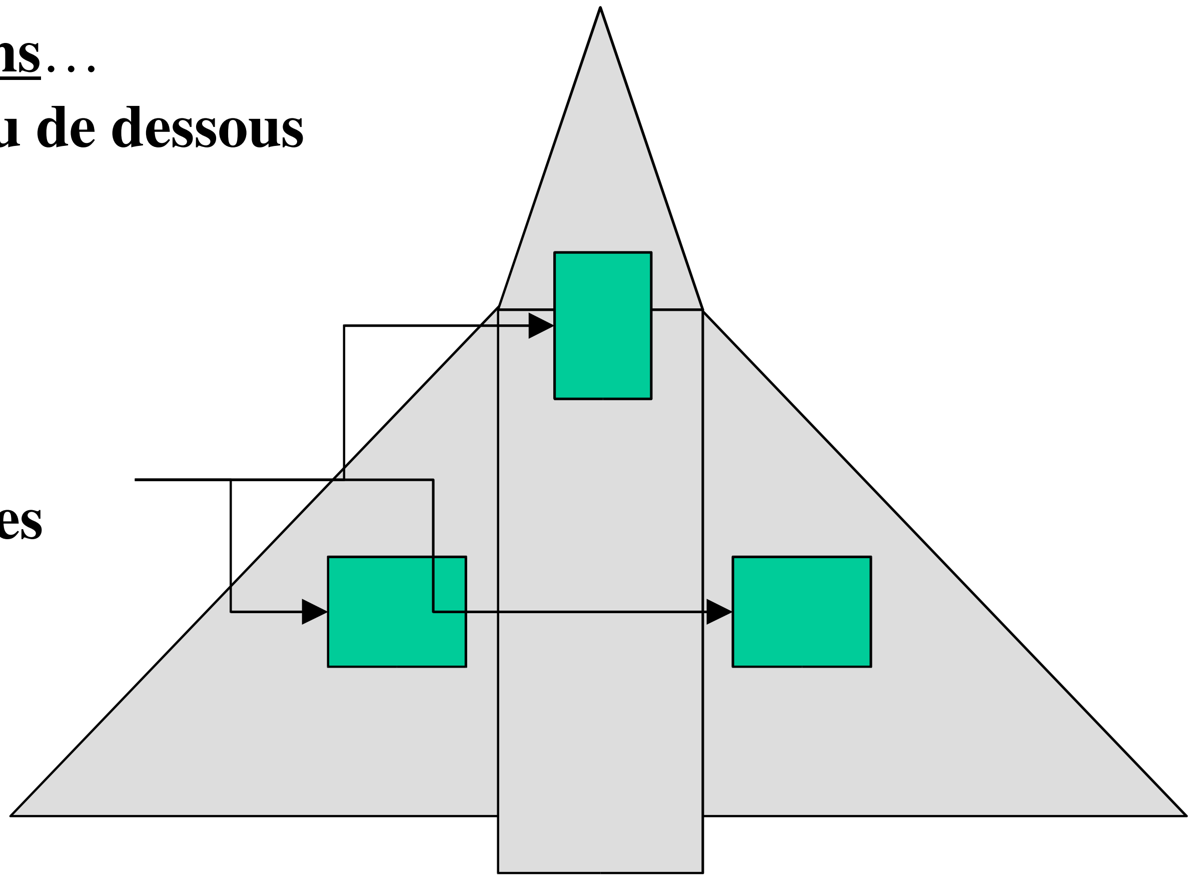
  => **autres pistes ?**
    - **Vérification compositionnelle ?**
    - **model checking "temporisés" ?**
    - … **?**

1. L’étude de cas…

L'étude de cas… en image

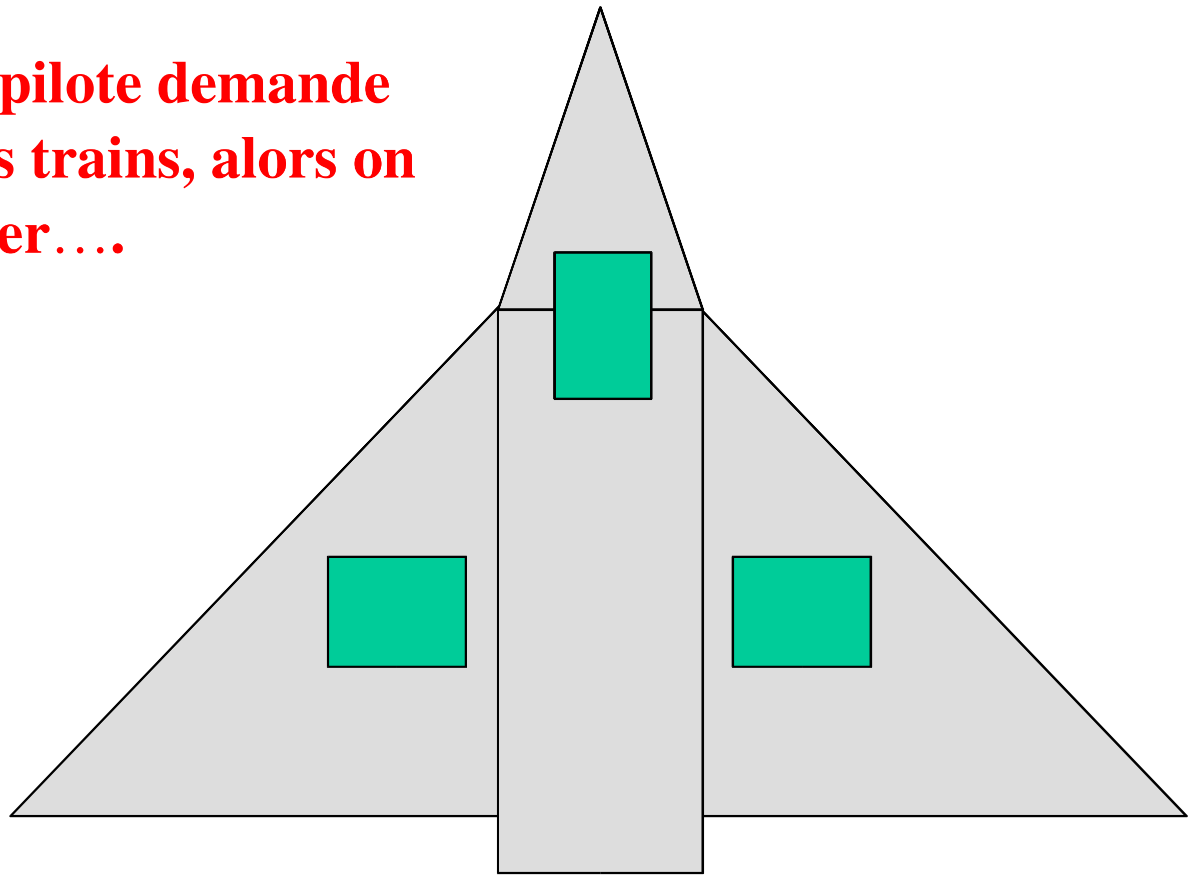
<u>Considérons</u>…
un avion vu de dessous

Trappes fermant le logement des trains



L'étude de cas… en image

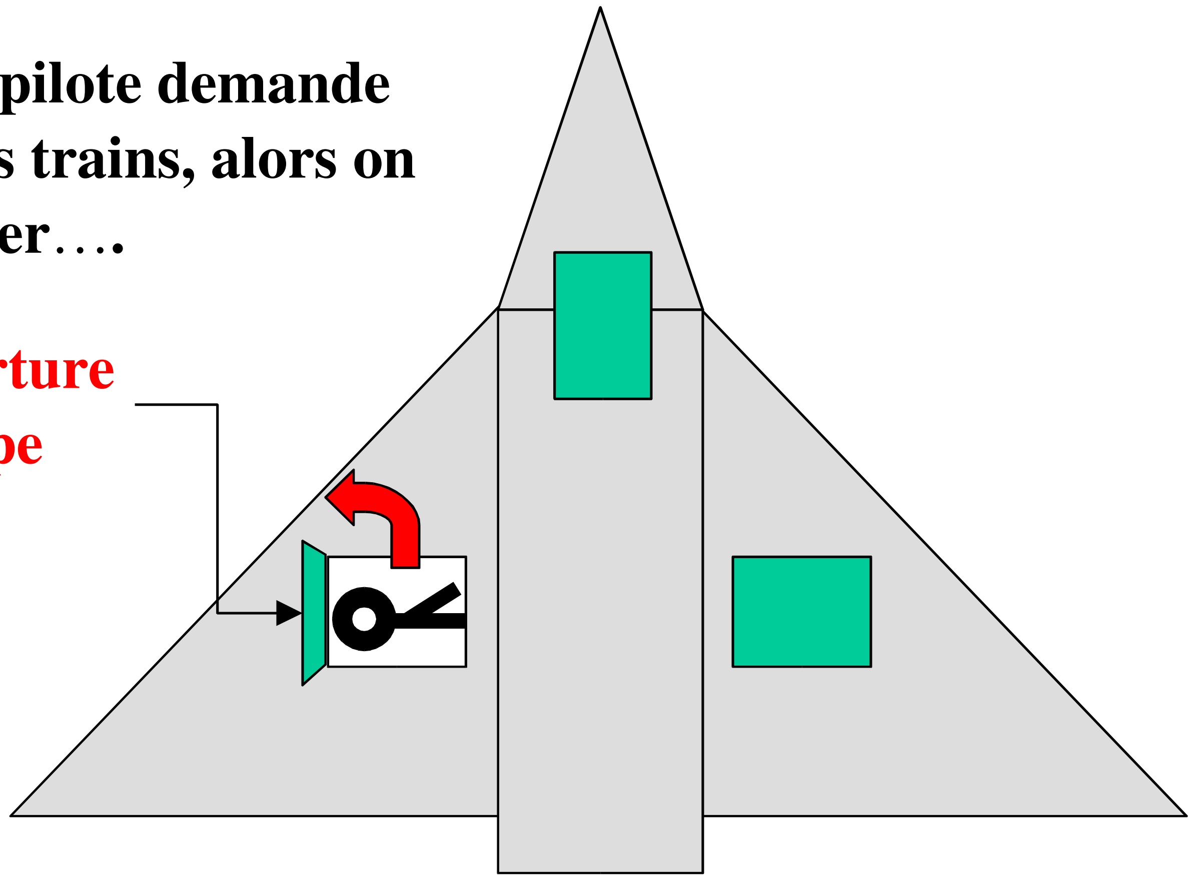
Lorsque le pilote demande la sortie des trains, alors on doit observer….



L’étude de cas… en image

Lorsque le pilote demande la sortie des trains, alors on doit observer….

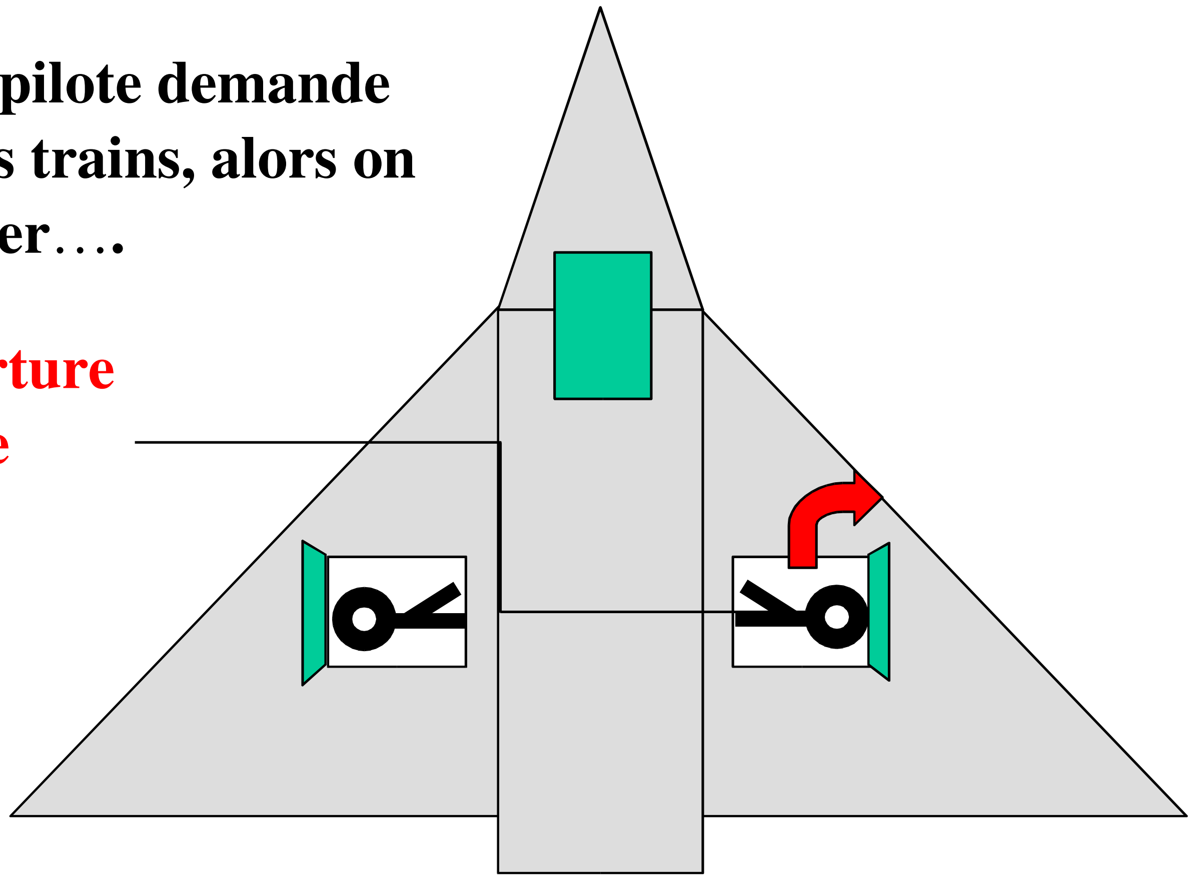
1.1 L’ouverture d’une trappe



L’étude de cas… en image

Lorsque le pilote demande la sortie des trains, alors on doit observer….

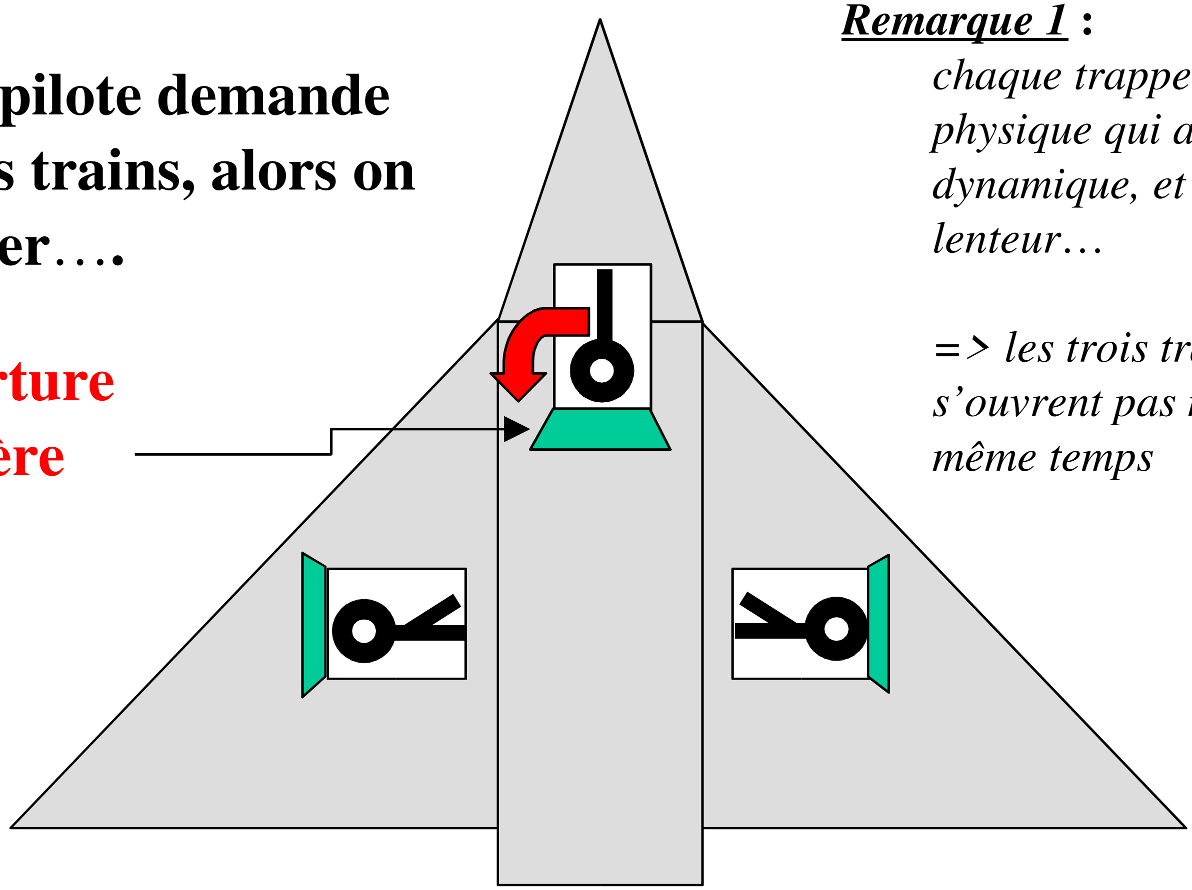
1.2 L’ouverture d’une autre trappe



L'étude de cas… en image

Lorsque le pilote demande la sortie des trains, alors on doit observer….

1.3 L'ouverture de la dernière trappe



Remarque 1 **:**

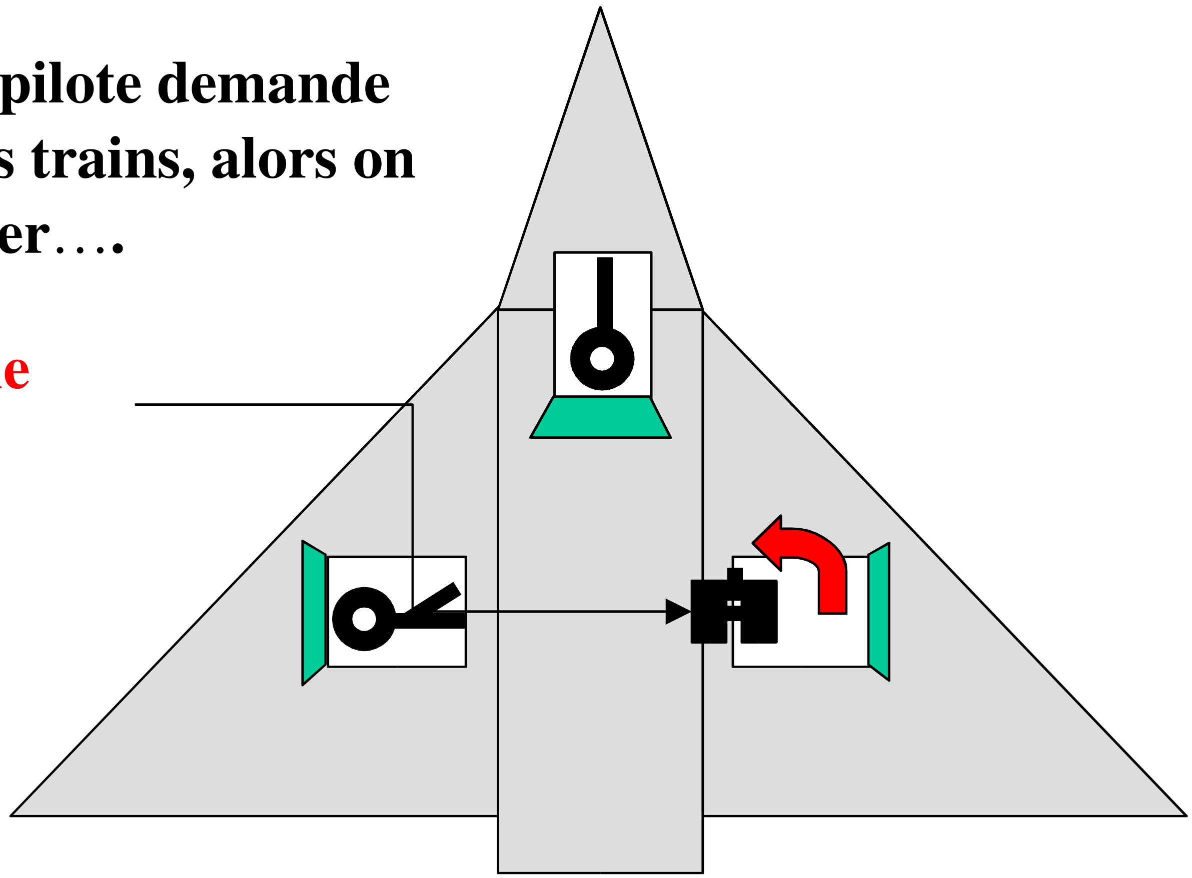
chaque trappe est un dispositif physique qui a sa propre dynamique, et sa propre lenteur…

=> les trois trappes ne s'ouvrent pas nécessairement en même temps

L’étude de cas… en image

Lorsque le pilote demande la sortie des trains, alors on doit observer….

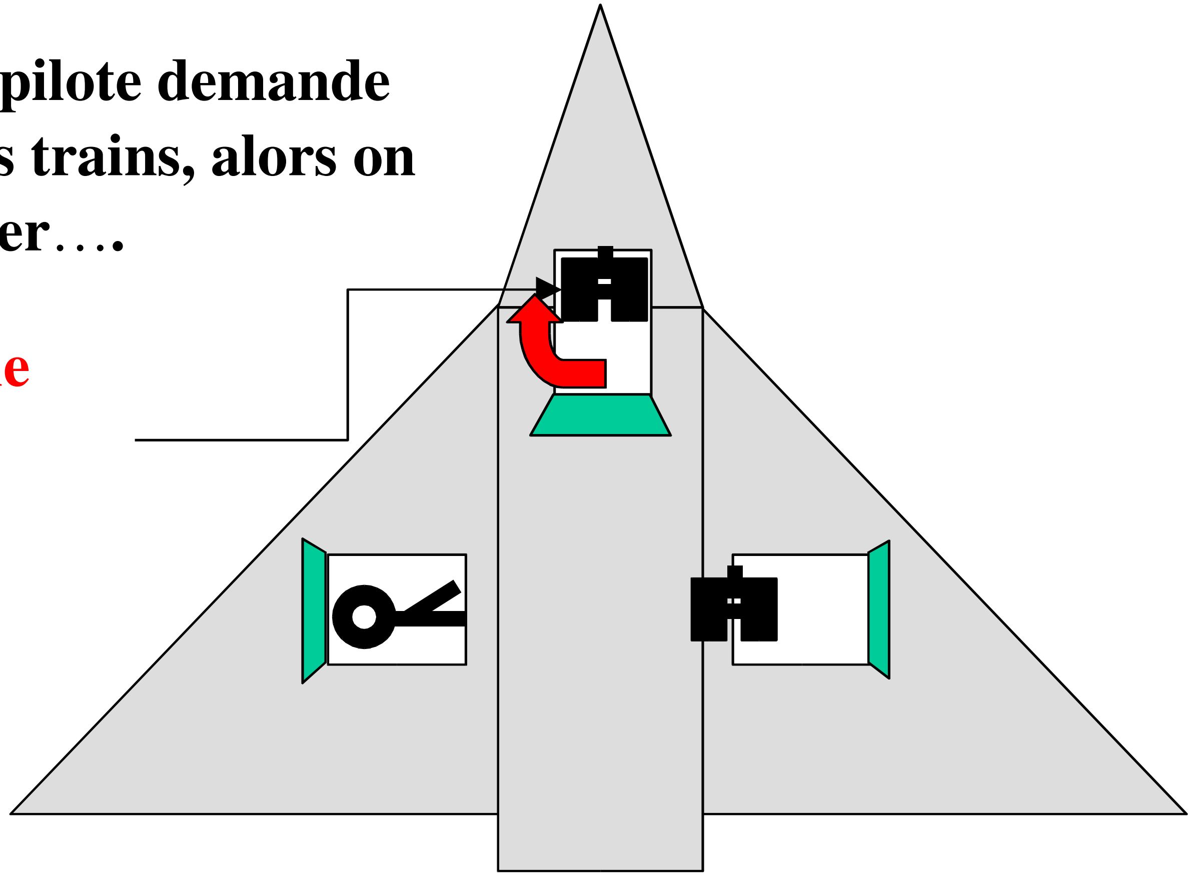
2.1 La sortie d’un train



L'étude de cas… en image

Lorsque le pilote demande la sortie des trains, alors on doit observer….

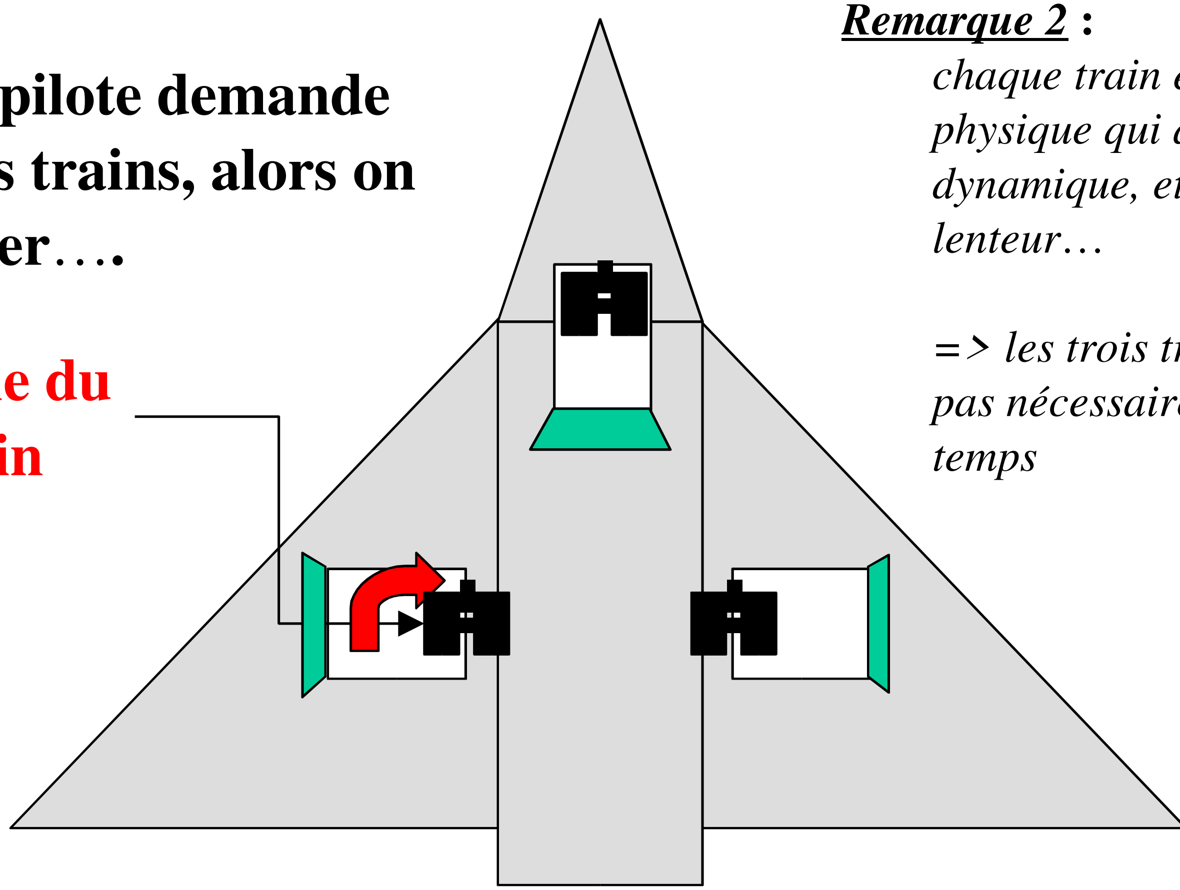
2.2 La sortie d'un autre train



L’étude de cas… en image

Lorsque le pilote demande la sortie des trains, alors on doit observer….

2.3 La sortie du dernier train



Remarque 2 **:**

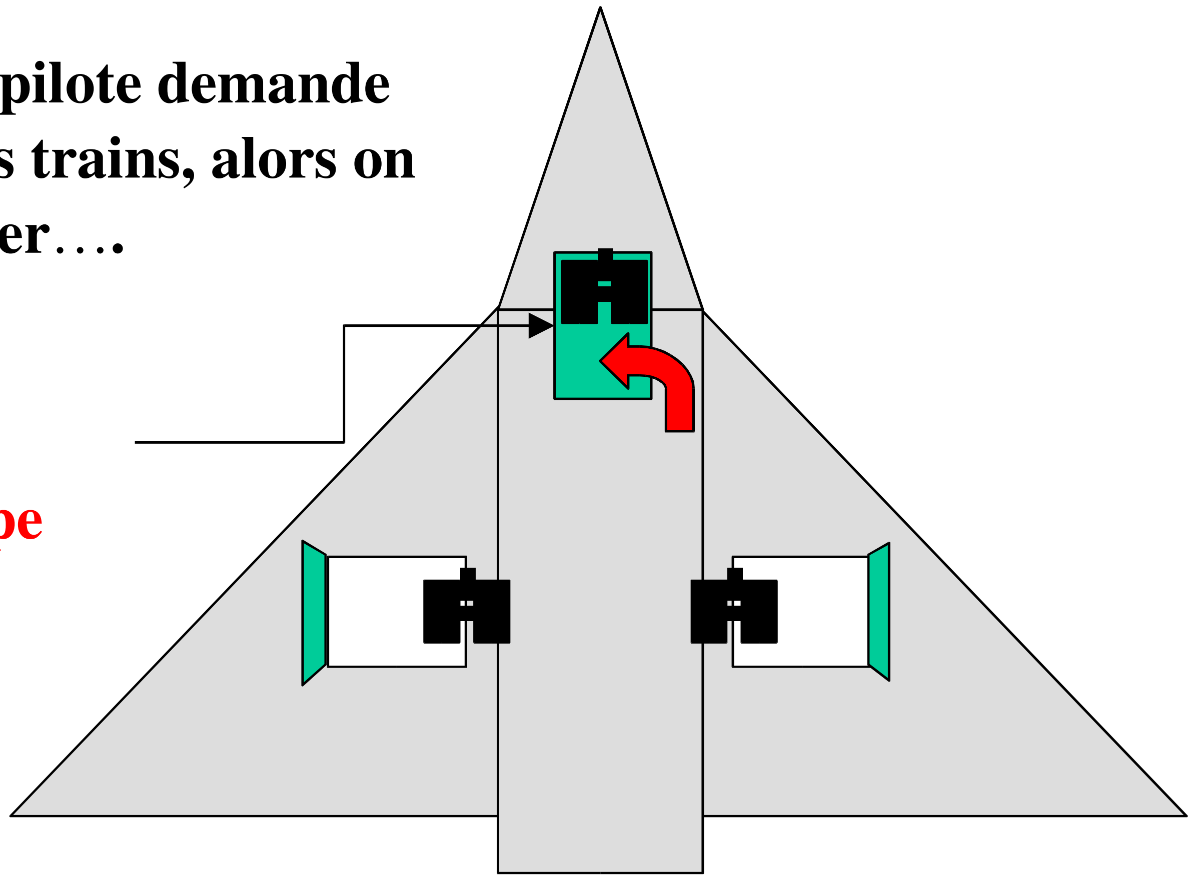
chaque train est un dispositif physique qui a sa propre dynamique, et sa propre lenteur…

=> les trois trains ne sortent pas nécessairement en même temps

L'étude de cas… en image

Lorsque le pilote demande la sortie des trains, alors on doit observer….

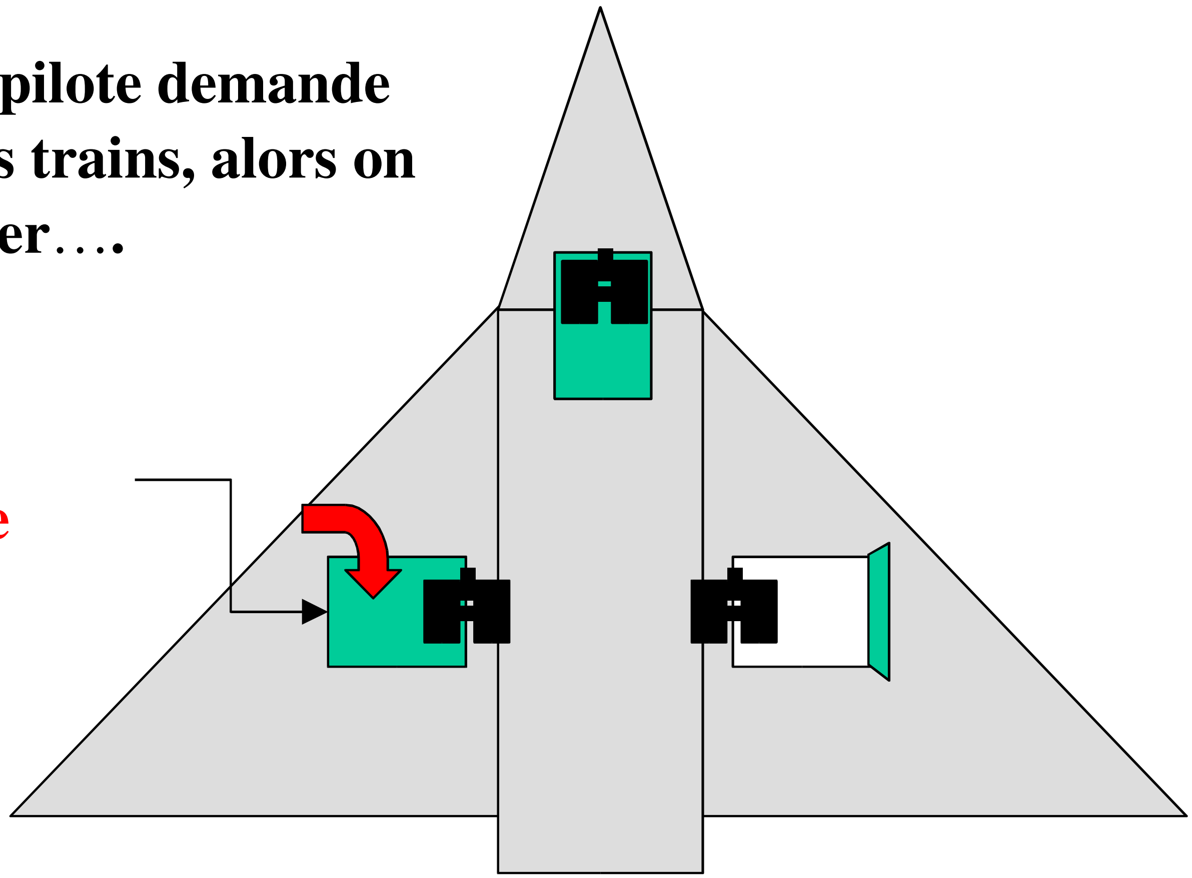
3.1 La fermeture d'une trappe



L'étude de cas… en image

Lorsque le pilote demande la sortie des trains, alors on doit observer….

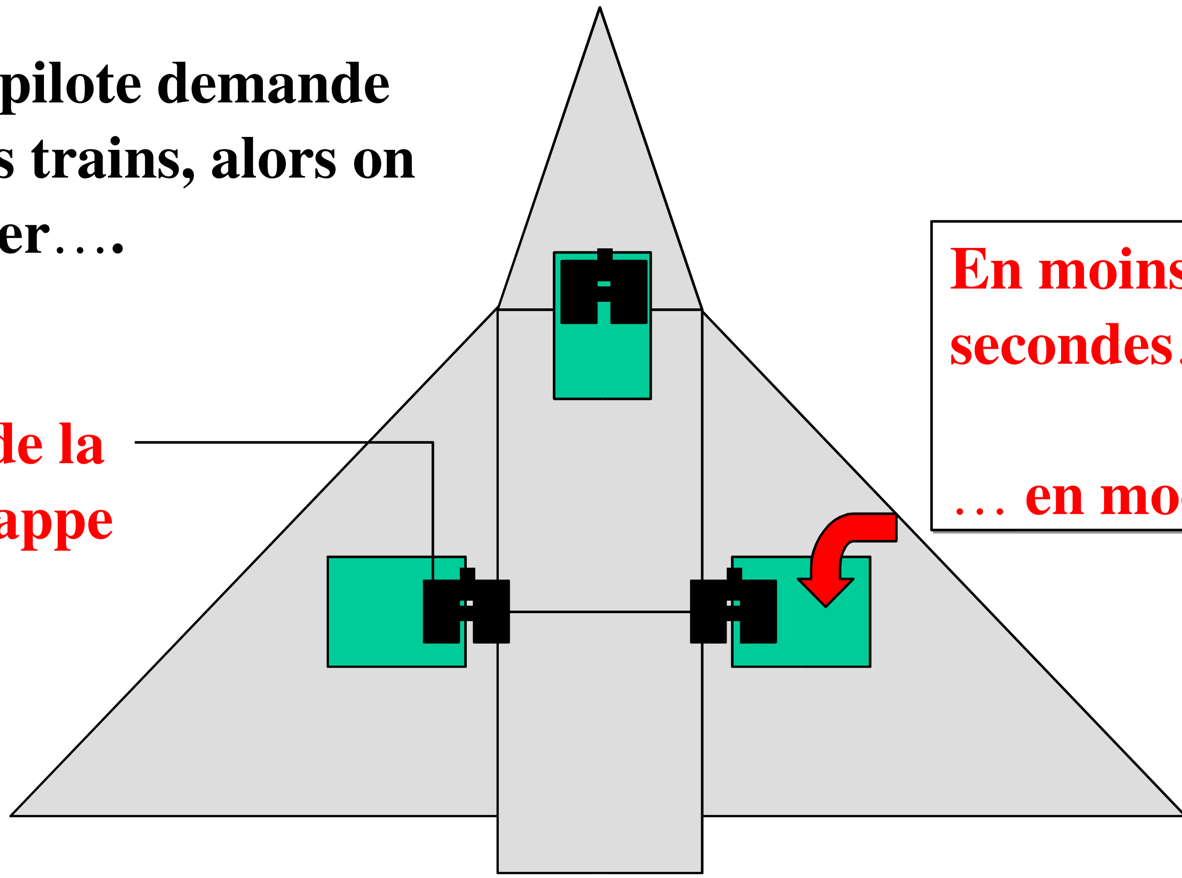
3.2 La fermeture d'une autre trappe



L'étude de cas… en image

Lorsque le pilote demande la sortie des trains, alors on doit observer….

3.3 La fermeture de la dernière trappe



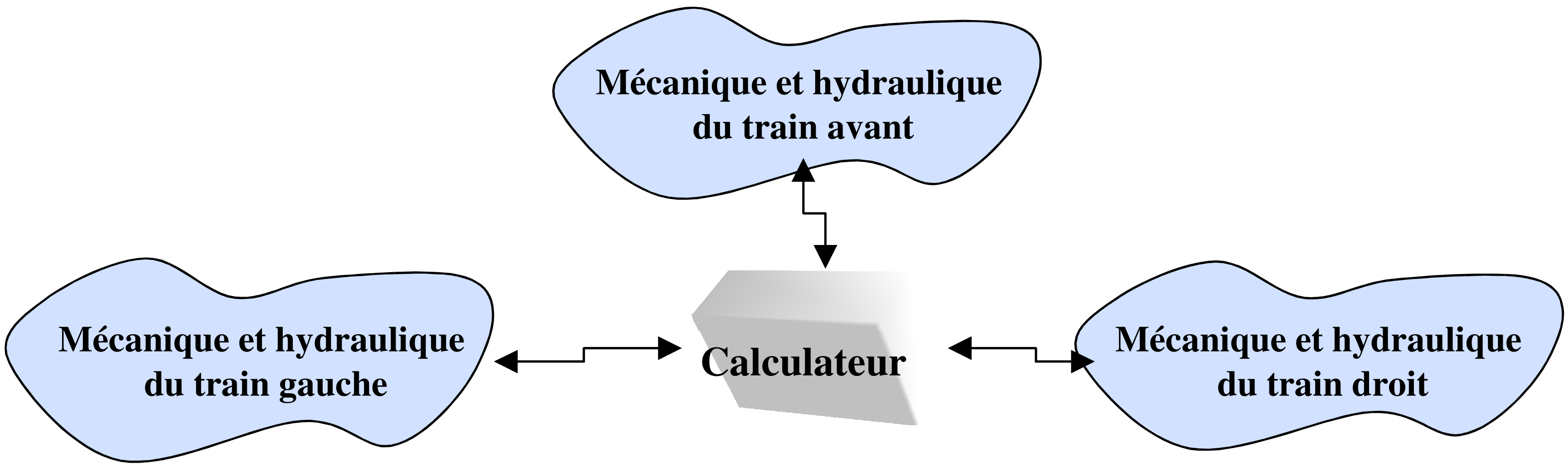
En moins de 14 secondes…

… en mode nominal !

L'étude de cas…

Pour cela, le système est composé de :

- **un calculateur**
- **3 ensembles "train/trappe"** actionnés par des vérins hydrauliques
- des capteurs de position des trains, trappes...



=> en fonction de la position des trains, des trappes, et de l'état de l'avion, le calculateur élabore **une séquence d'ordre** à destination des vérins hydraulique…

L'étude de cas…

Or…

- **les trains, trappes, vérins… sont des dispositifs physiques à <u>dynamiques lentes</u>**

=> il est nécessaire de respecter certaines <u>temporisations</u> entre deux commandes successives

=> <u>temps</u> = notion centrale de la modélisation, puis de la vérification

=> une des origines de l'explosion combinatoire…

L'étude de cas… : description plus détaillée

Fonction du système :

– gérer la procédure de descente et de relevage des trains
– les ordres sont donnés par le pilote ou le mécanicien

Les entrées (capteurs) du système

– palette de commande (UP ou DOWN) actionnée par le pilote
– crochet de fermeture de trappe (trappe fermé / non fermé)
– crochet de verrouillage du train en position haute (train haut / non haut)
– vérin de manœuvre de trappe (trappe ouverte / non ouverte)
– contrefiche de train en butée (train bas / non bas)
– mano–contacteur (pression hydraulique / non pression)
– amortisseur de train (train détendu / non détendu)

L'étude de cas… : description plus détaillée

Les sorties (actionneurs) du système

- **électro–robinet** : fournit l'énergie hydraulique au circuit
- **électro–vanne de fermeture** : déclenche la fermeture de la trappe
- **électro–vanne d'ouverture**: déclenche l'ouverture de la trappe
- **électro–vanne de montée** : déclenche la montée du train
- **électro–vanne de descebte** : déclenche la descente du train

=> **rôle du système** = piloter les électro–robinet et électro–vannes en fonction des informations retournées par les capteurs…

=> **impératif** = tenir compte de la dynamique lente des mécanismes physiques…

L'étude de cas… : description plus détaillée

Architecture interne de la fonction :

– 3 modules communicants

=> Cohérence :

- détermine si les entrées du système sont cohérentes. Sinon déclare l'atterrisseur et berne et passe en mode secours

Mais : non intégré dans l'étude de cas

=> Surveillance fonctionnelle :

- détermine si les organes mécaniques et hydrauliques répondent comme attendus. Sinon, déclare l'atterrisseur en berne

Mais : non intégré dans l'étude de cas

=> on ne s'intéresse qu'au mode nominal

=> Elaboration de la commande :

- élabore et réalise la séquence d'ordres à envoyer aux organes physiques

L'étude de cas… : description plus détaillée

Architecture interne de la fonction :

Mais… l'élaboration de la commande est centralisé

=> une seule commande pour

- les 3 électro–vannes de fermeture
- les 3 électro–vannes d'ouverture
- les 3 électro–vannes de montée
- les 3 électro–vannes de descente…

=> Exemple : avant d'ordonner la descente des trains, on attend que les 3 trappes soient ouvertes…

=> système non modulaire !

=> difficulté pour la vérification compositionnelle

L'étude de cas… : description plus détaillée

La dynamique :

Si ordre de descente : Palette **DOWN**

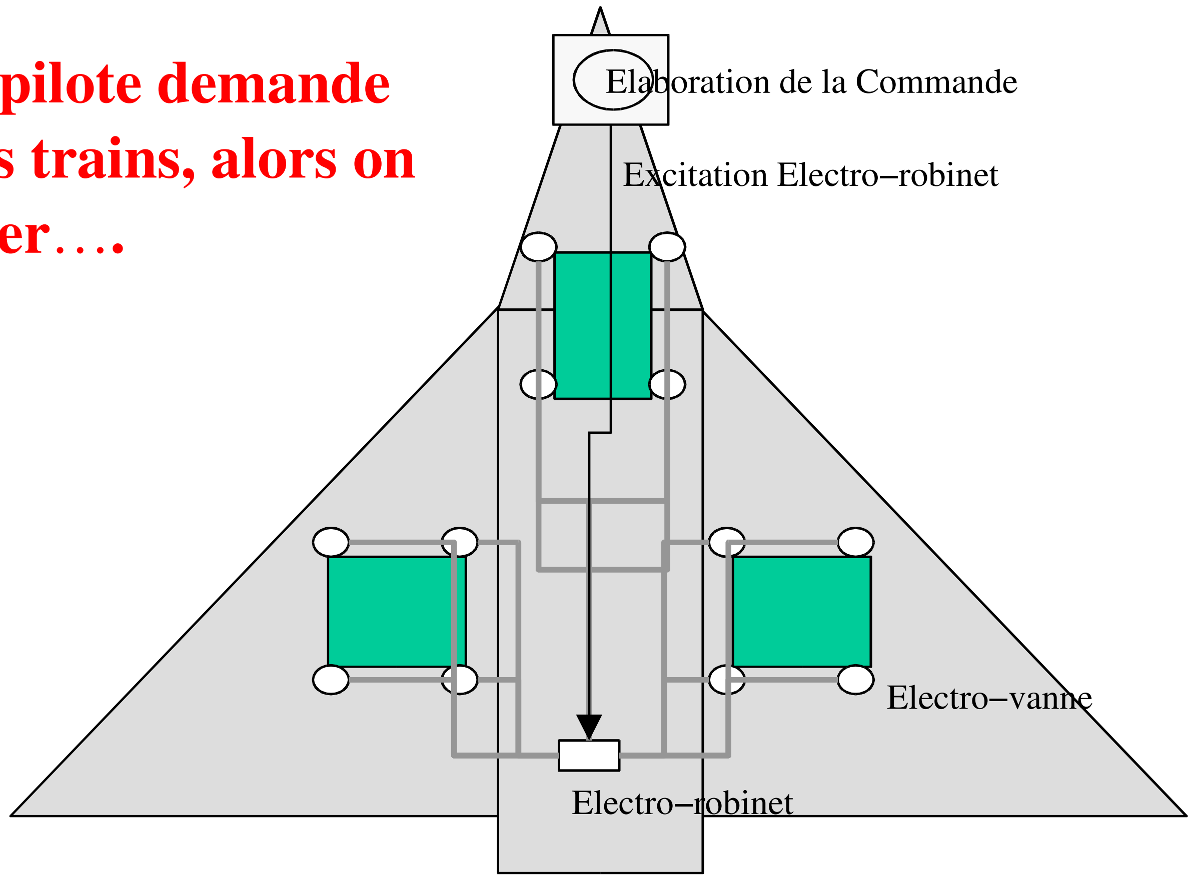
1. Excitation Electro–robinet
2. Attente disponibilité de la puissance hydraulique
3. Excitation de toutes les Electro vannes d'ouverture des trappes
4. Attente de l'ouverture de toutes les trappes
5. Excitation de toutes les Electro vannes de descente des trains
6. Attente de la descente de tous les trains
7. Excitation de toutes les Electro–vannes de fermeture des trappes
8. Attente de la fermeture de toutes les trappes
9. Désexcitation de l'Electro–robinet

=> séquence qui doit pouvoir être interrompue à tout instant par un ordre inverse

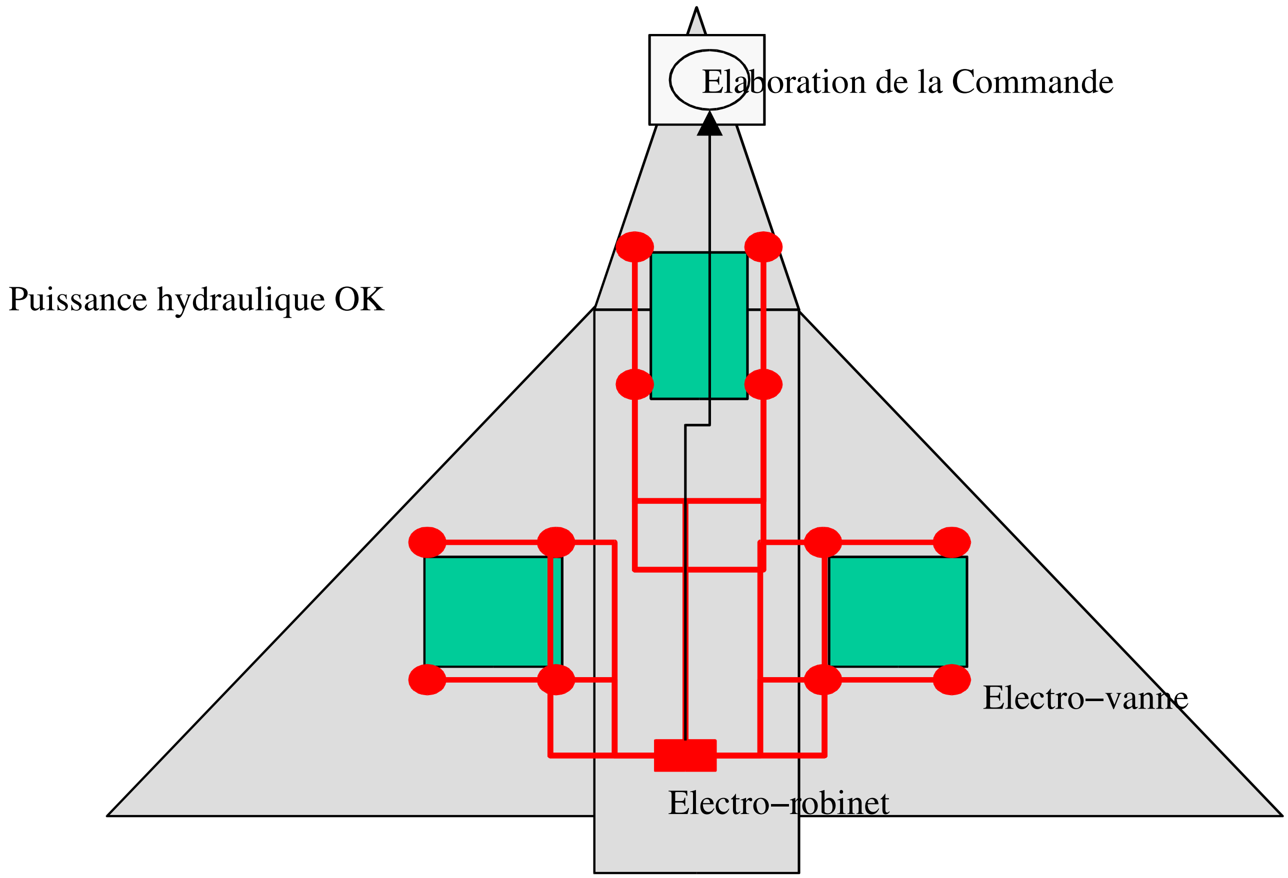
=> séquence qui doit pouvoir être reprise en n'importe quel point...

L'étude de cas… en image

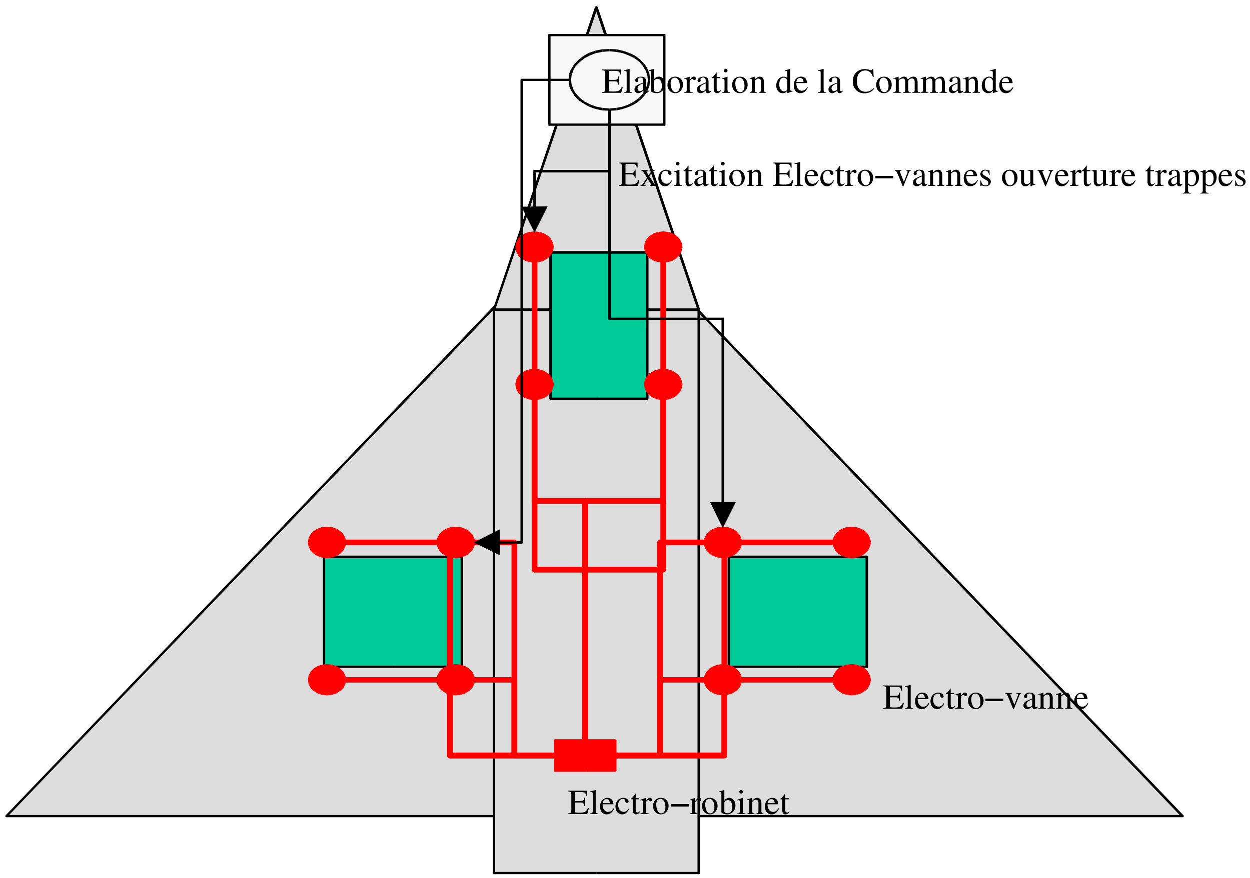
Lorsque le pilote demande la sortie des trains, alors on doit observer….



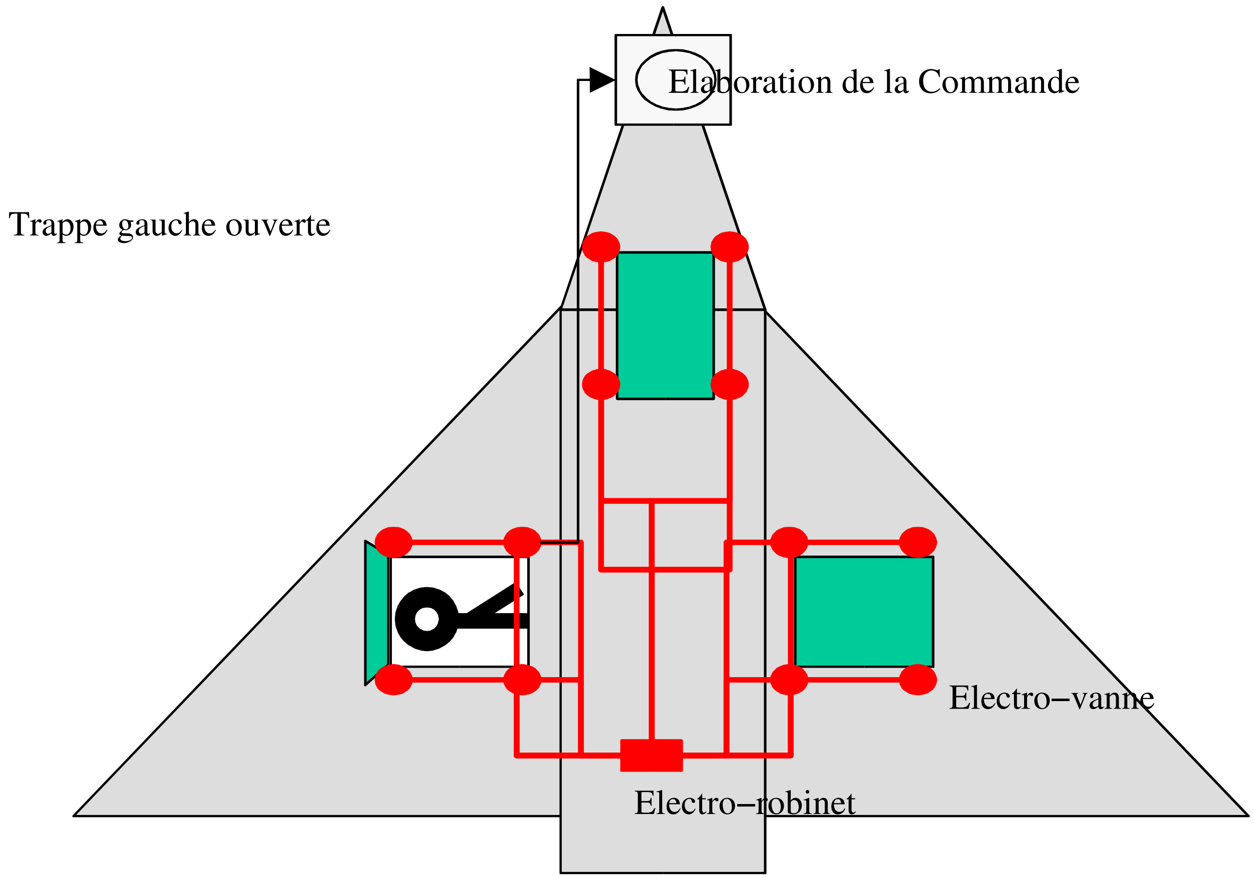
L'étude de cas… en image



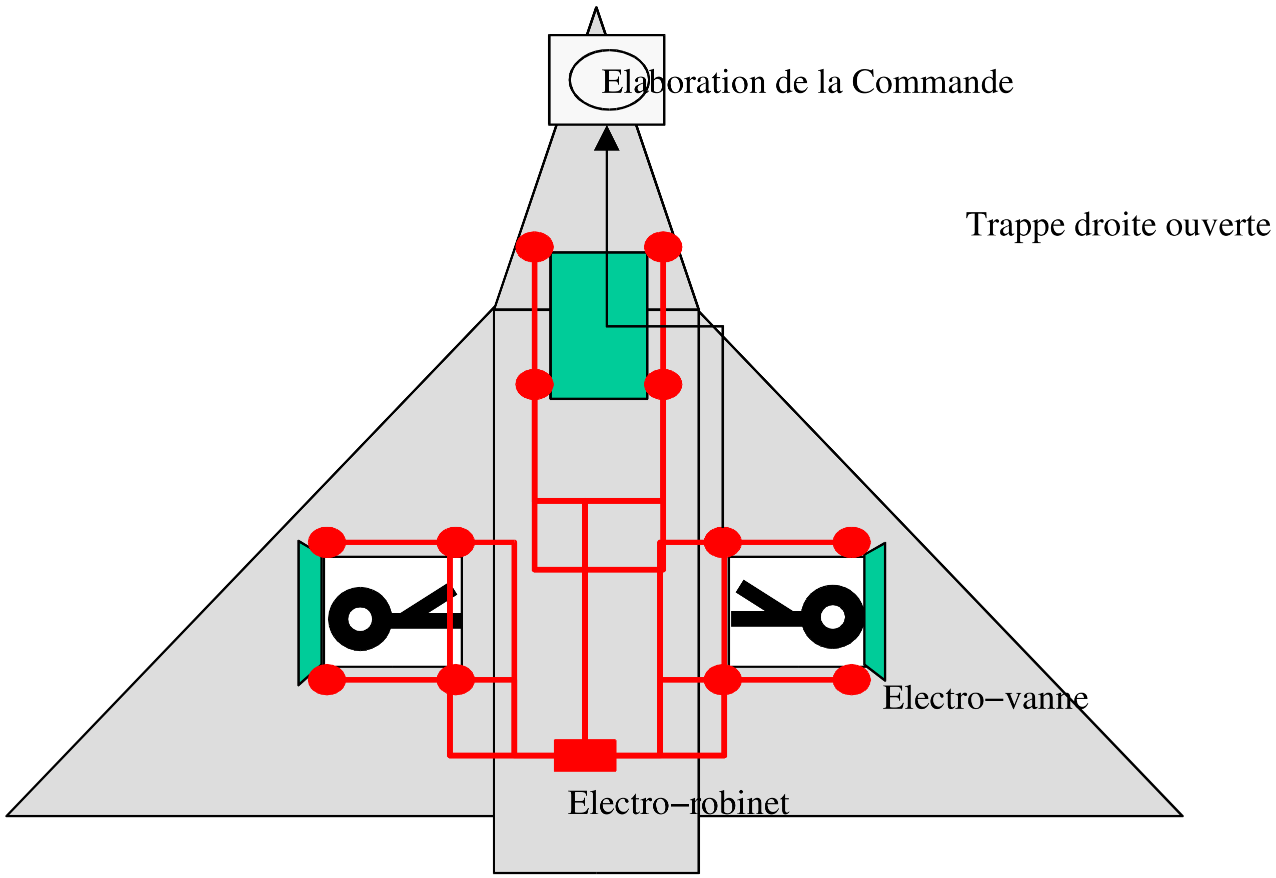
L'étude de cas… en image



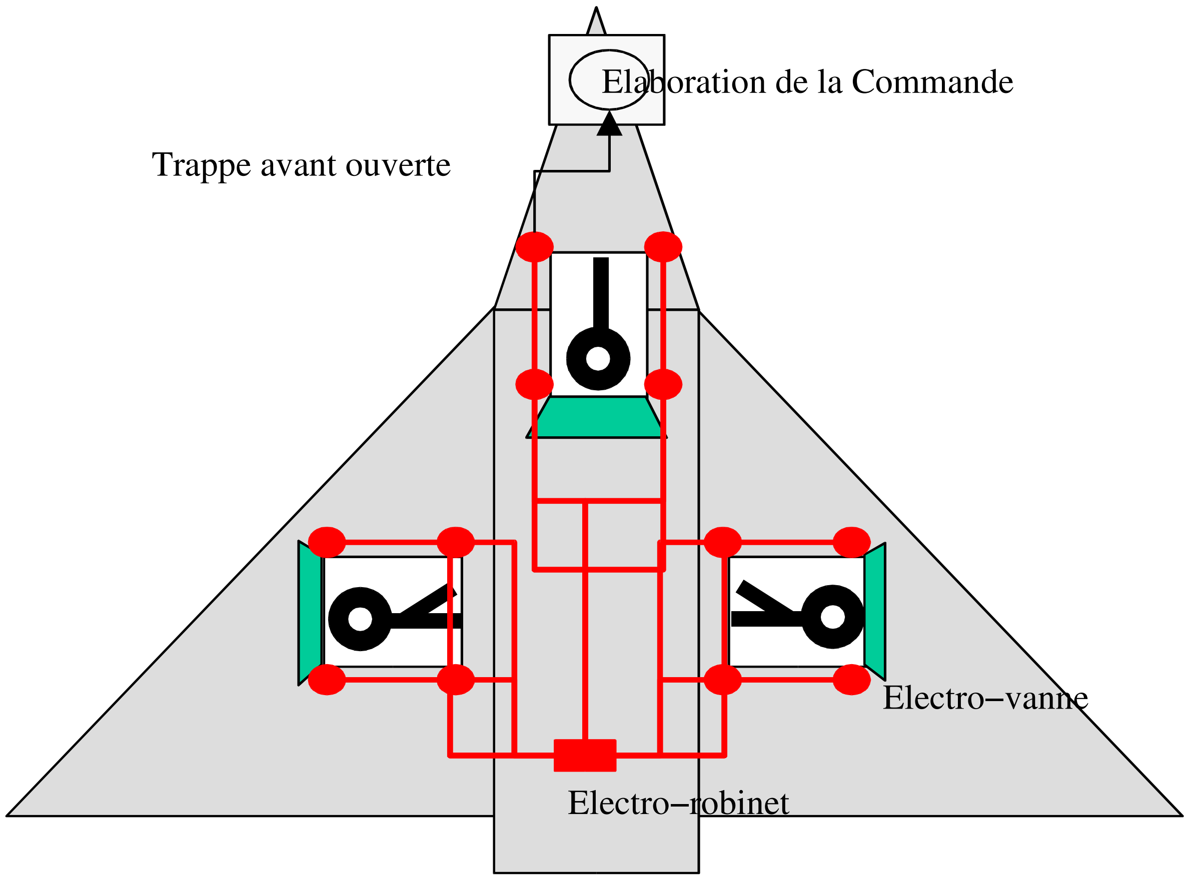
L’étude de cas… en image



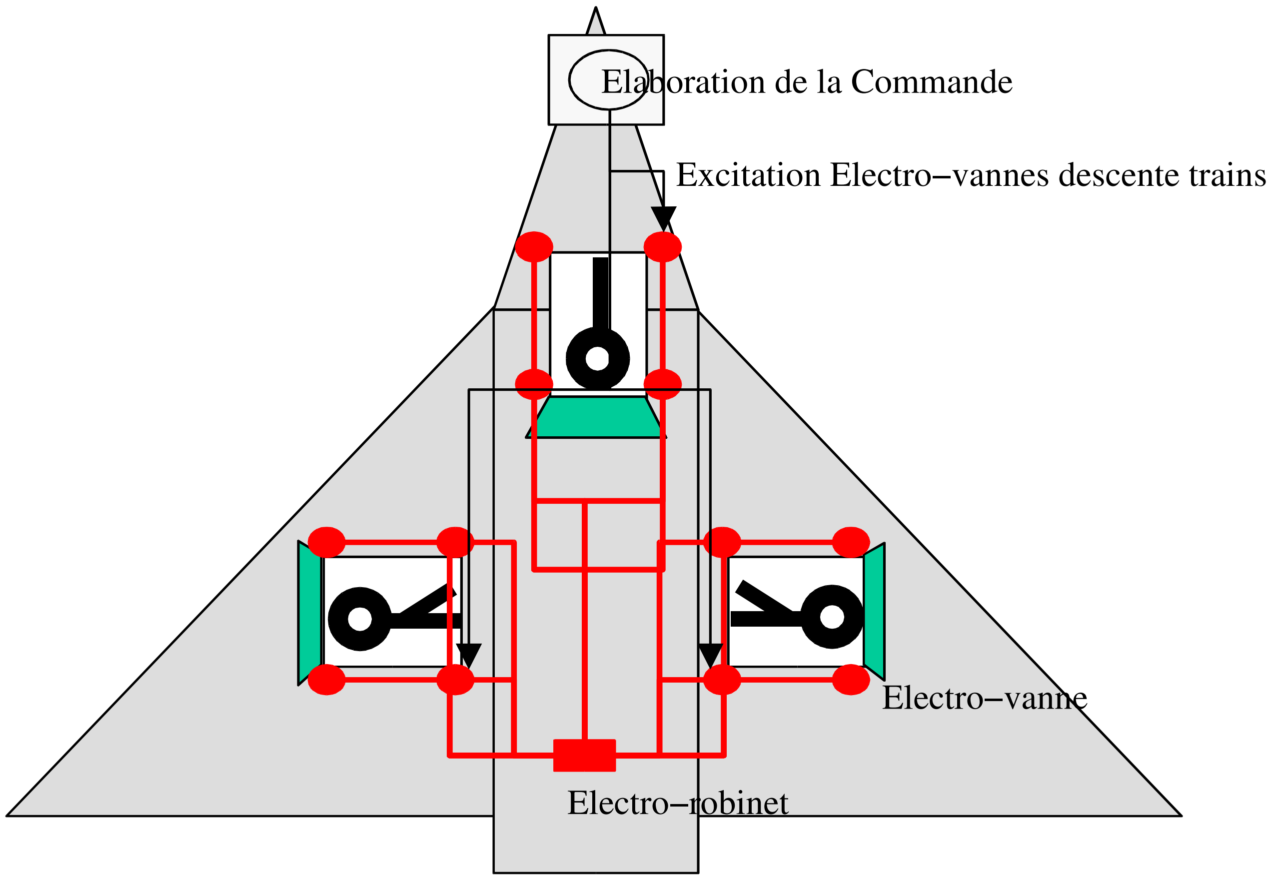
L’étude de cas… en image



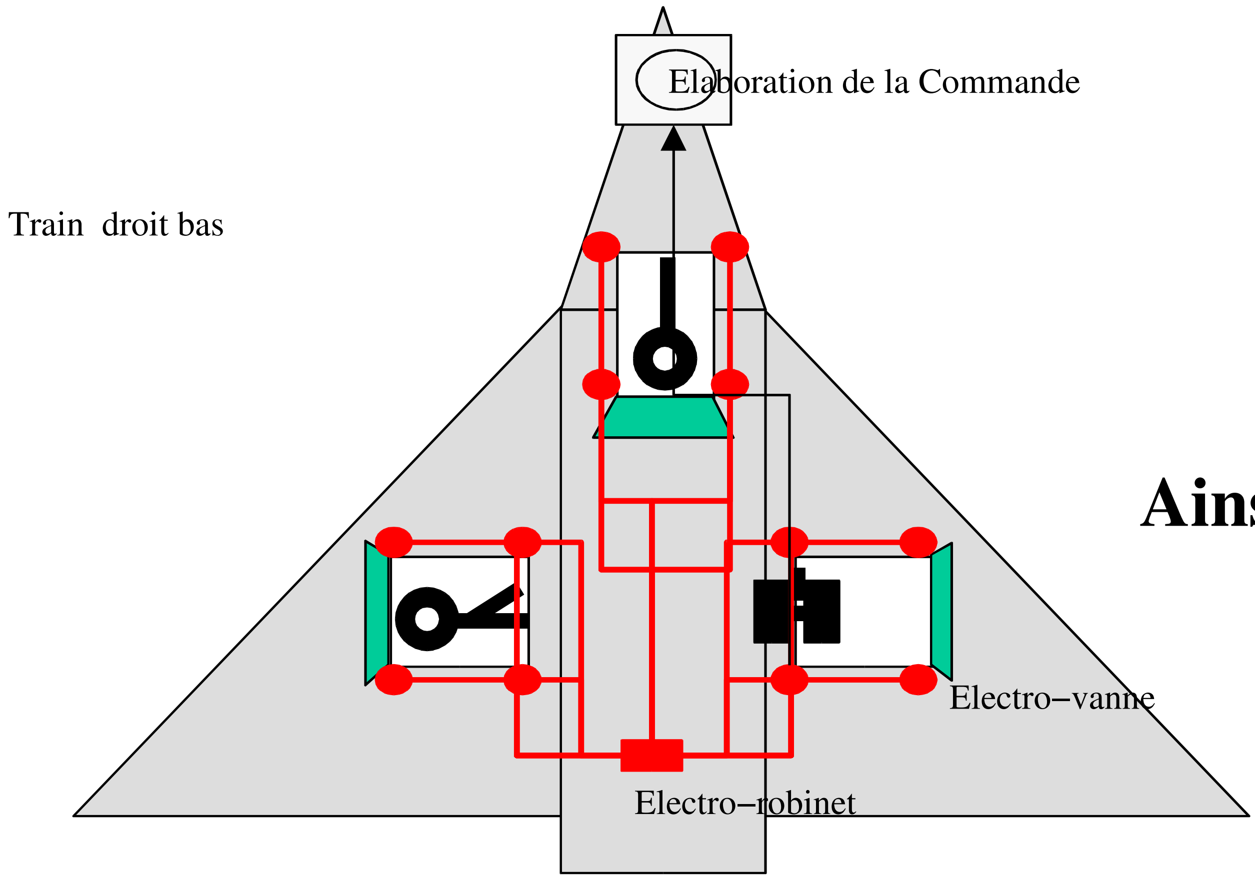
L'étude de cas… en image



L'étude de cas… en image



L'étude de cas… en image



Ainsi de suite…

L'étude de cas… : description plus détaillée

Ce que le système doit faire et ne doit pas faire :

=> nombreuses exigences fonctionnelles et temporelles

- non rentrée du train alors que l'avion est au sol
- non sortie intempestive du train
- non entrée intempestive du train
- …

- ***en mode nominal, tout ordre de descente des trains doit être satisfait en moins de 14 secondes***
- ***en mode nominal, tout ordre de montée des trains doit être satisfait en moins de 15 secondes***

=> propriétés retenues dans le cas d'étude.

2. Démonstration de la propriété

"en mode nominal, une commande de sortie des trains est satisfaite en au plus 14 secondes"

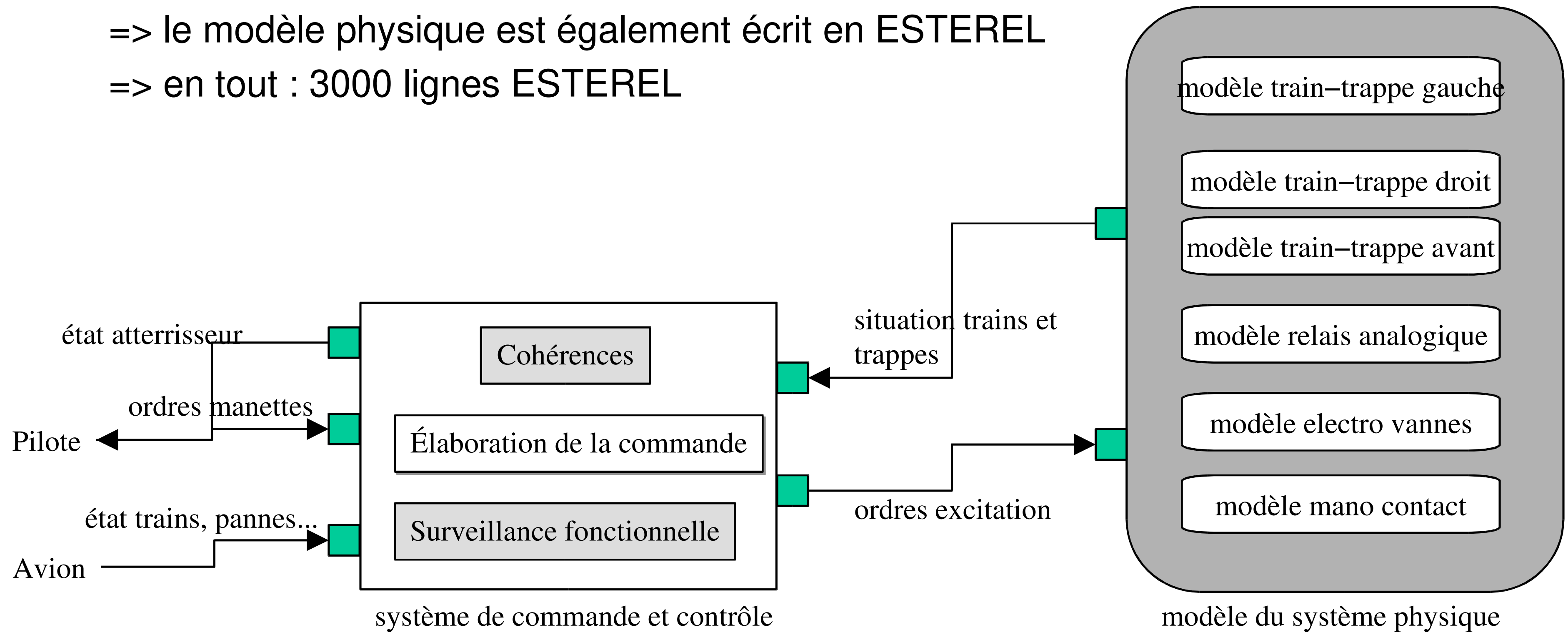
Démonstration de la propriété de descente nominale...

Système décrit en ESTEREL par Dassault Aviation

Mais... nécessite un modèle des mécanismes physiques pour la vérification

=> le modèle physique est également écrit en ESTEREL

=> en tout : 3000 lignes ESTEREL



Démonstration de la propriété de descente nominale...

Contrainte (Dassault Aviation)

- démonstration par utilisation de techniques automatiques (model checking…)

=> Tentative avec plusieurs outils

- le model checker de ESTEREL (**échec** en 1996)
- les outils autour de LUSTRE : LESAR et NP–tools (**échec**)
- le model checker SMV : **réussite**

- autres techniques ?
  - Automates temporisés avec UPPAAL (en cours)
  - vérification compositionnelle ?
  - … ?

Démonstration de la propriété de descente nominale...

Avec les outils ESTEREL...

– expérience réalisée en 1996 par l'INRIA et Dassault Aviation, pendant le projet GENIE

=> model checker ESTEREL = TiGER

=> **échec** (saturation de la mémoire au bout de deux jours)

Démonstration de la propriété de descente nominale...

Avec les outils LUSTRE… : LESAR et NP–tools

=> traduction du code ESTEREL en LUSTRE, pour vérification avec LESAR et NP–tools

=> **échec** sur l'Atterrisseur simplifié complet

=> essai par décomposition du système : démonstration de la propriété sur un Atterrisseur

- ne comportant qu'un seul dispositif "train/trappe" : **réussite**
- ne comportant que deux dispositifs "train/trappe" : **réussite**

=> démonstration de la propriété sur le système par ***composition*** des preuves sur chaque "train/trappe" ?

Démonstration de la propriété de descente nominale...

Avec les outils LUSTRE… : dans le cas d'un seul train–trappe

=> suppression de tout ce qui concerne T_G e T_D dans le programme

=> codage de la propriété

```
apres_attente =
if await_n_x(QUATORZE_SECONDES, true,
(true-> pre(PALETTE_POSITION_UP)) and not PALETTE_POSITION_UP,
PALETTE_POSITION_UP)
then true
else if PALETTE_POSITION_UP then false
else (false ->pre(apres_attente));
prop = (not apres_attente) or (T_A_POSITION_TRAIN_BAS and
T_A_POSITION_TRAPPE_FERMEE);
```

Avec **QUATORZE_SECONDES=350**

Démonstration de la propriété de descente nominale...

…. LUSTRE… : dans le cas d'un seul train–trappe (suite)

=> vérification avec **LESAR** sur une station de travail SPARC 10 à 440 MHz et 1 Go de Mémoire en 3 mn

```
Debut 1 trains avec delai = 350
lundi, 17 décembre 2001, 11:24:04 MET
start normalisation ... done
start minimal network generation
    ........................................................................
    ........................................................................
    ........................................................................
    ........................................................................
    ........................................................................
    ........................................................................
    .................................. done (3655 -> 2226 nodes)
building bdds ... 495 (on 495)
computing relevant statevars ... done (475 on 477)
DONE => 24720 states 65589 transitions
```

TRUE PROPERTY

```
lundi, 17 décembre 2001, 11:27:08 MET
Fin 1 trains avec delai = 350
```

Démonstration de la propriété de descente nominale...

…. LUSTRE… : dans le cas d'un seul train–trappe (suite)

Si vérification d'une propriété plus forte : par remplacement de **QUATORZE_SECONDES** par 28 (1,12 seconde)

=> vérification avec **LESAR** sur une station de travail SPARC 10 à 440 MHz et 1 Go de Mémoire en 1 mn et 30 secondes

```
Debut 1 trains avec delai = 28
lundi, 17 décembre 2001, 11:19:11 MET
Pollux Version 1.34
start normalisation ... done
start minimal network generation
   ............................................................................
   ........ done (1401 -> 938 nodes)
building bdds ... 173 (on 173)
computing relevant statevars ... done (153 on 155)
DONE => 23532 states 63213 transitions

TRUE PROPERTY
lundi, 17 décembre 2001, 11:20:41 MET
Fin 1 trains avec delai = 28
```

Démonstration de la propriété de descente nominale...

…. LUSTRE… : dans le cas de deux train–trappes

=> suppression de tout ce qui concerne T_A dans le programme

=> codage de la propriété

```
apres_attente = …

prop = (not apres_attente) or (T_G_POSITION_TRAIN_BAS and
T_G_POSITION_TRAPPE_FERMEE and
T_D_POSITION_TRAIN_BAS and
T_D_POSITION_TRAPPE_FERMEE );
```

=> vérification d'une propriété plus forte par remplacement de **`QUATORZE_SECONDES`** par 36 (1,44 seconde)

Démonstration de la propriété de descente nominale...

…. LUSTRE… : dans le cas de deux train–trappes (suite)

=> vérification avec **LESAR** sur une station de travail SPARC 10 à 440 MHz et 1 Go de Mémoire en 10 heures et 20 minutes

```
Debut 2 trains avec delai = 36
jeudi, 13 décembre 2001, 19:33:53 MET
Pollux Version 1.34
start normalisation ... done
start minimal network generation
   ...........................................................................
   ............................... done (2089 -> 1433 nodes)
building bdds ... 252 (on 252)
computing relevant statevars ... done (216 on 218)
DONE => 98061 states 274693 transitions
```

TRUE PROPERTY

```
vendredi, 14 décembre 2001, 05:53:25 MET
Fin 2 trains avec delai = 36
```

Démonstration de la propriété de descente nominale...

…. LUSTRE… : dans le cas de deux train–trappes (suite)

=> tentative de vérification d'une propriété plus forte par remplacement de **`QUATORZE_SECONDES`** par 36 (1,44 seconde)

=> vérification avec **LESAR** interrompue après **16 jours** de calcul
(note : il n'y a pas eu de saturation de la mémoire)

=> échec !

Démonstration de la propriété de descente nominale...

Note :

– **échec** de NP–tools dans tous les cas

– NP–tools traduit un programme LUSTRE (car nécessite le déploiement du système en autant d'instance que de "pre" emboîtés)

=> explosion combinatoire !

Alors que :

– **réussite** de SMV sur l'atterrisseur à 3 trains / trappes, en moins de 20 minutes !

3. Les pistes…

Les pistes...

Utiliser des langages et outils manipulant le temps

par exemple :

- automates temporisés et UPPAAL...

Utiliser des techniques de vérification compositionnelle

– les quelles ?
– Comment ?

=> Appel à idées

Note :

le code ESTEREL ou LUSTRE du système et le code ESTEREL ou LUSTRE modélisant les organes physiques est disponible…