www.thalesgroup.com

Model checking temporisé, application à l'avionique

Eric JENN – *Thales Avionics*
Pierre-Alain BOURDIL – *Thales Avionics / LAAS*

THALES

www.thalesgroup.com

Model checking temporisé, application à l'avionique

Eric JENN – *Thales Avionics*
Pierre-Alain BOURDIL – *Thales Avionics / LAAS*

une modeste

un sous^{+}*-système*

THALES

D'où vient-il?

Thales

Thales Avionics

Centre de compétences Missions et Fonctions

Service Méthodes et Outils

10^4

10^0

THALES

D'où vient-il?

« B »

SPARK

Frama-C

FIACRE
TINA

Altarica

10^4

10^0

Thales

Thales Avionics

Centre de compétences Missions et Fonctions

Service Méthodes et Outils

THALES

D'où vient-il?

Thales

Thales Avionics

Centre de compétences Missions et Fonctions

Service Méthodes et Outils

THALES

D'où vient-il?

« B »

IN ACTION

Thales

Thales Avionics

SPARK

Frama-C

FIACRE

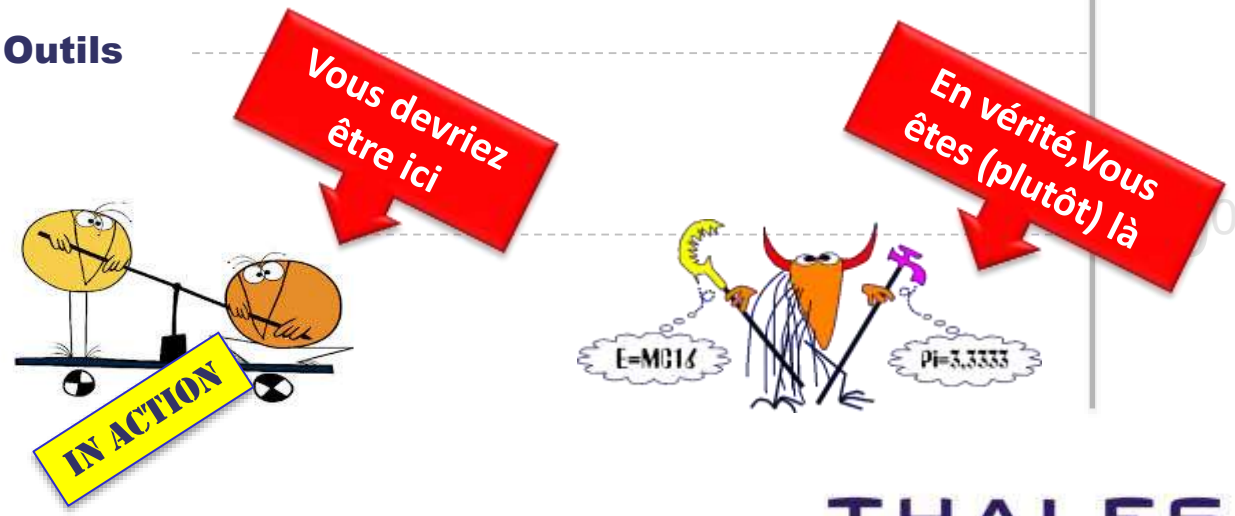
TINA

Altarica

10^4

Centre de compétences Missions et Fonctions

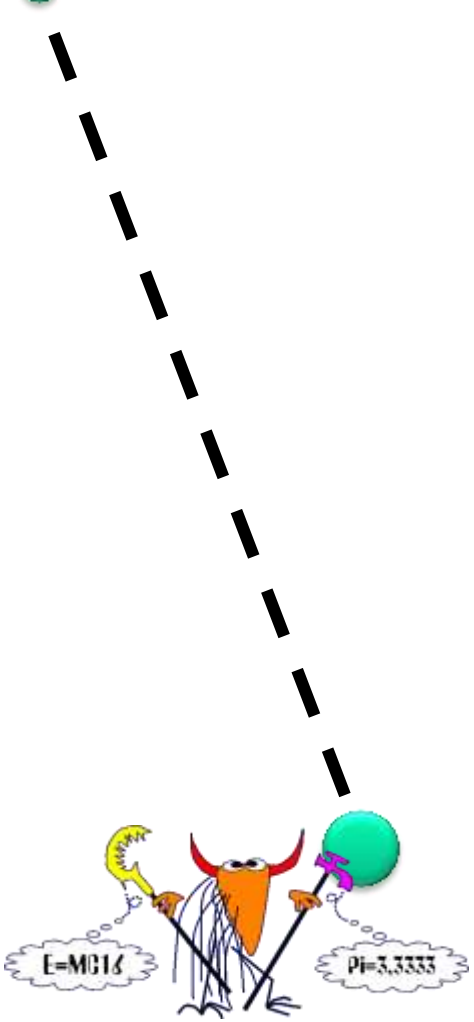
Service Méthodes et Outils



THALES

D'où vient-il?

FIACRE, TINA

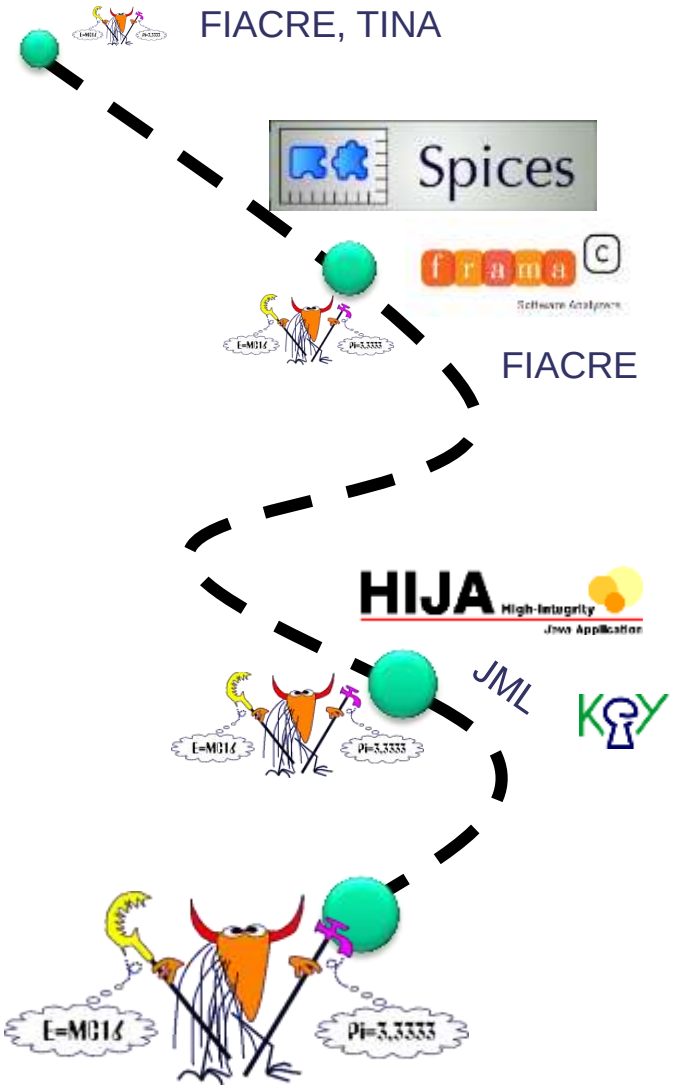


THALES

D'où vient-il?

THALES

Pourquoi les méthodes formelles?



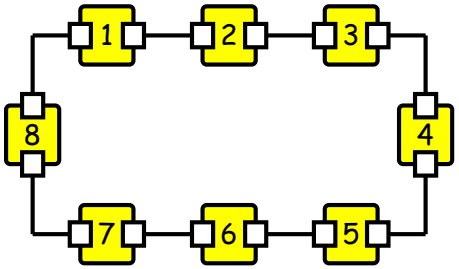
THALES

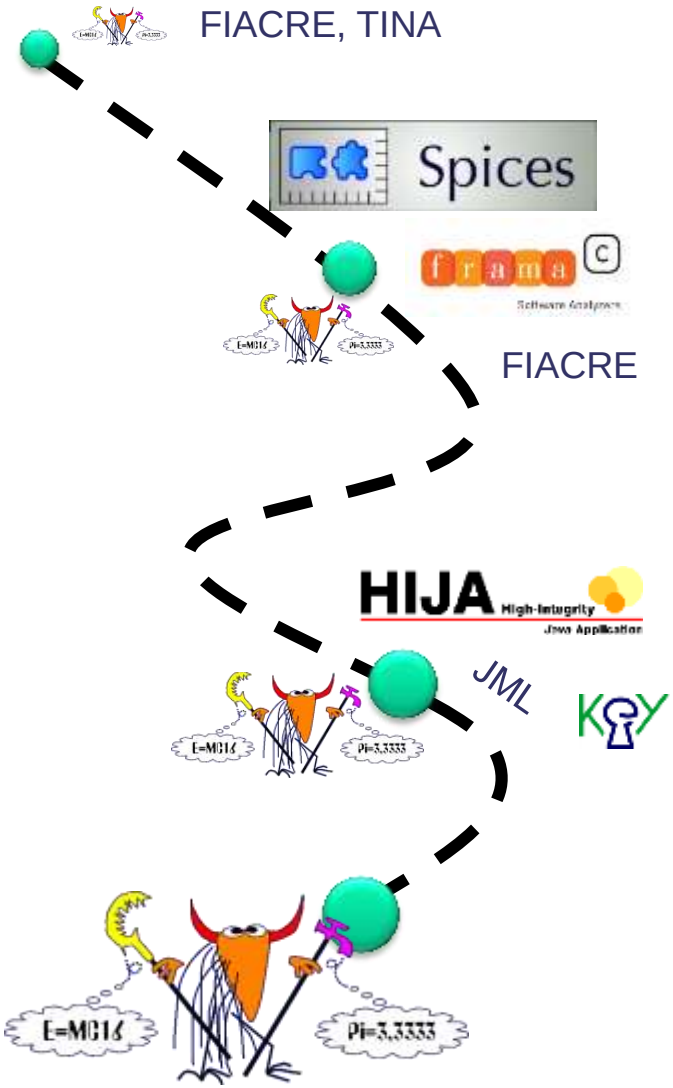
Pourquoi les méthodes formelles?

Thèse CIFRE THAV/LAAS-VERTICS

Pierre-Alain BOURDIL : « Contribution au développement de méthodes et outils de modélisation et de vérification par model-checking appliqués à la vérification formelle d'un protocole de communication avionique. »

Travaux centrés sur l'expression et l'exploitation des symétries structurelles





THALES

Pourquoi le *model checking* temporisé ?

Problèmes temporels

FIACRE, TINA

Opportunités « contextuelles »

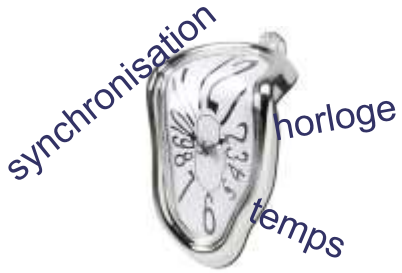
Model-checking

THALES

Pourquoi le *model checking* temporisé ?

Problèmes temporels

- Difficiles à appréhender…
- Difficiles à observer, traiter…
- Souvent découverts et traités tardivement…



FIACRE, TINA

Opportunités « contextuelles »

Technique model-checking

THALES

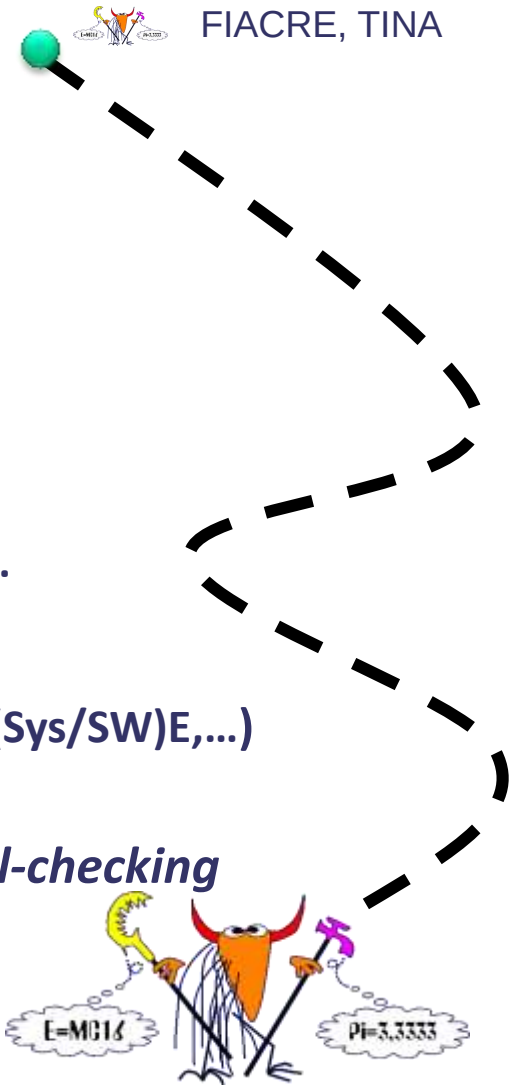
Pourquoi le *model checking* temporisé ?

Problèmes temporels

- Difficiles à appréhender…
- Difficiles à observer, traiter…
- Souvent découverts et traités tardivement…

Opportunités « contextuelles »

- Maturité des méthodes et outils…
- Maturité des parties prenantes…
- « Tendance à l'abstraction » (MD(Sys/SW)E,…)

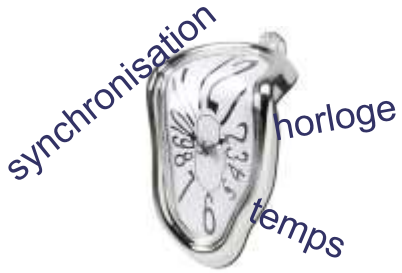


Technique model-checking

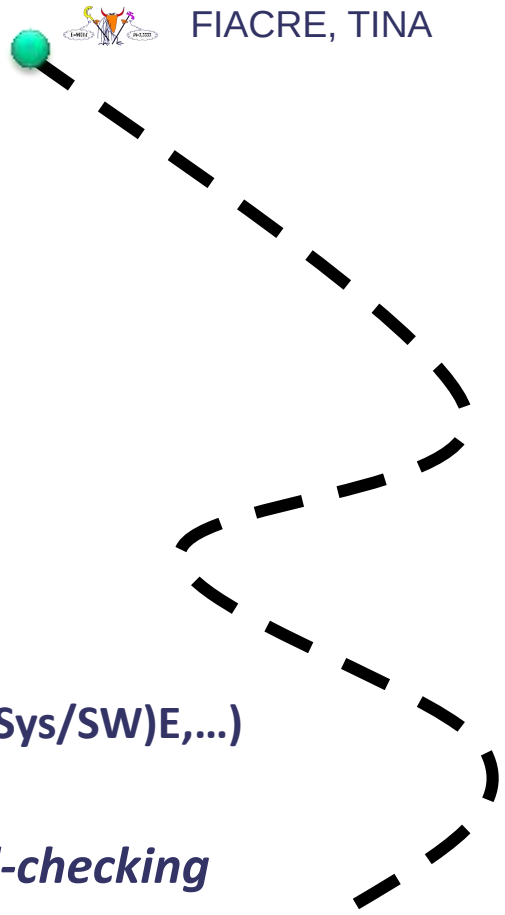
THALES

Pourquoi le *model checking* temporisé ?

Problèmes temporels



- Difficiles à appréhender…
- Difficiles à observer, traiter…
- Souvent découverts et traités tardivement…



Opportunités « contextuelles »

- Maturité des méthodes et outils…
- Maturité des parties prenantes…
- « Tendance à l'abstraction » (MD(Sys/SW)E,…)

Technique model-checking

- Une technologie (assez) automatique
- Utilisant des formalismes (assez) naturels

THALES

Automatic Flight & Control System (AFCS)

Fonctions principales

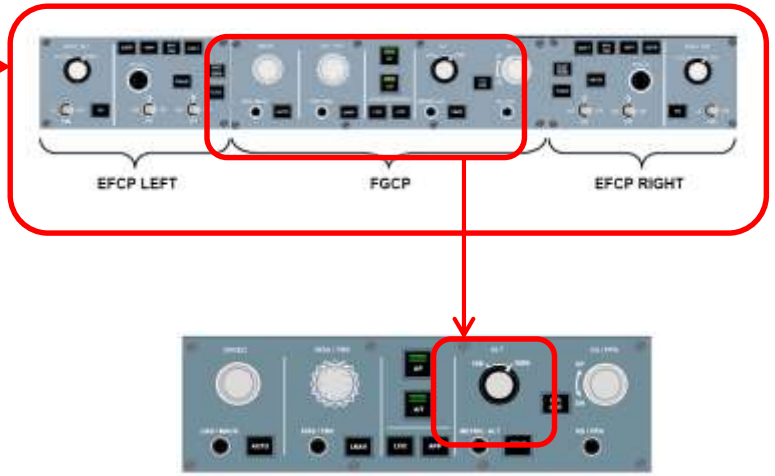
- Elaboration d'informations de guidage à destination du pilote
- Elaboration des commandes de la manette de contrôle de poussée
- Gestion des consignes et des modes
- Elaboration des consignes à destination du système de commande de vol / actionneurs, en lieu et place du pilote

THALES

Automatic Flight & Control System (AFCS)

Fonctions principales

- Elaboration d'informations de guidage à destination du pilote
- Elaboration des commandes de la manette de contrôle de poussée
- Gestion des consignes et des modes
- Elaboration des consignes à destination du système de commande de vol / actionneurs, en lieu et place du pilote



La fonction cible

La fonction cible

Elaboration de la consigne d'altitude

ALT_TGT = 10000 ft

THALES

La fonction cible

ALT_TGT = 10000 ft

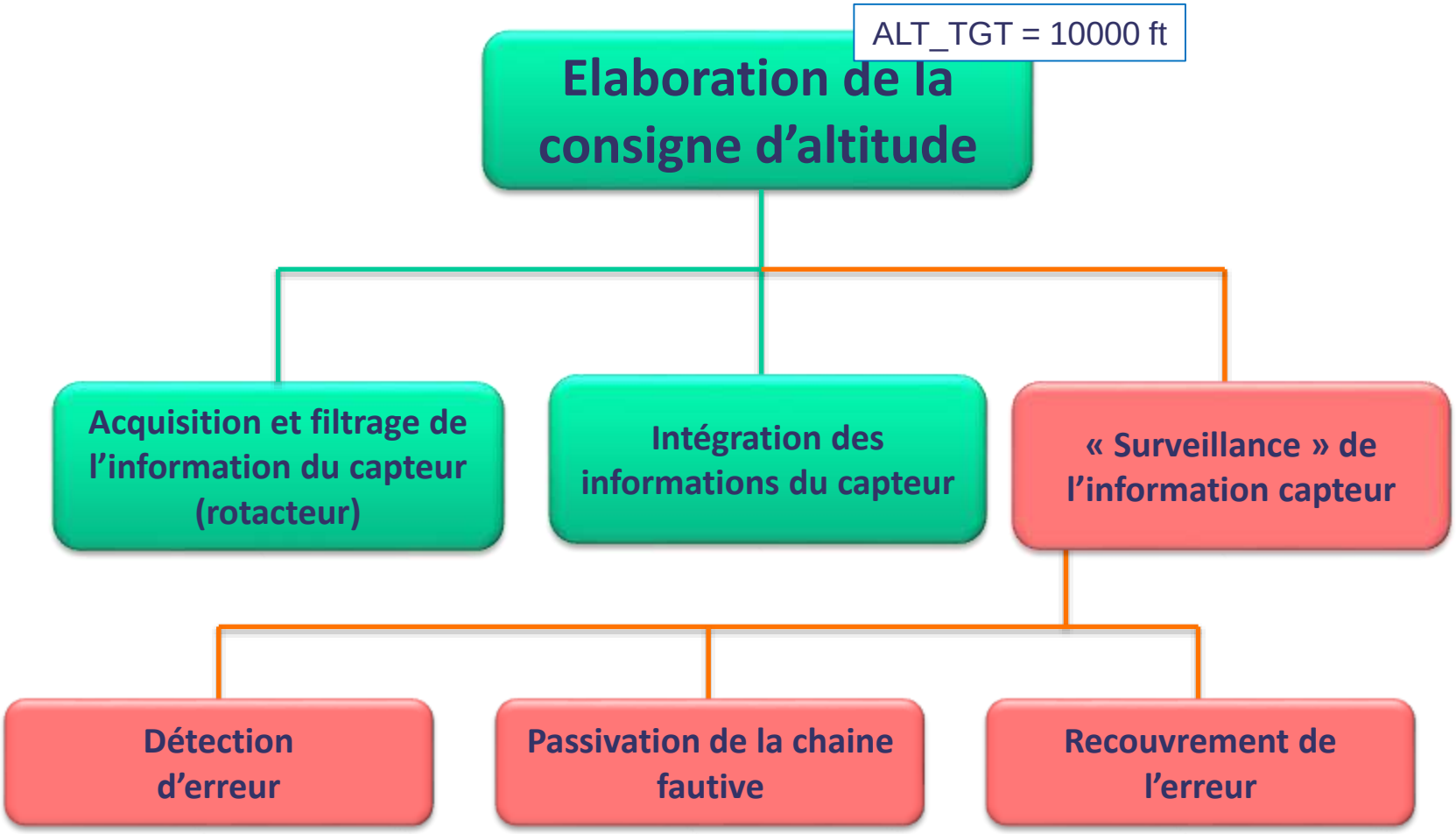
Elaboration de la consigne d'altitude

Acquisition et filtrage de l'information du capteur (rotacteur)

Intégration des informations du capteur

THALES

La fonction cible



THALES

Le problème

Etant attendu que

« La surveillance doit traiter toute modification de consigne non accompagnée d'une information de détection de mouvement… »

« La surveillance ne doit pas se déclencher de façon intempestive… »

« Surveillance » de l'information capteur

Sachant que

« Les éléments de traitement et de communication sont **asynchrones**… »

Alors

« **Déterminez les durées de maintien des signaux…** »

THALES

Mais est-ce un « vrai » problème?

Est-ce un problème ?

Désespérante absence de problème

Fig. 1

« **Déterminez les durées de maintien des signaux… »**

THALES

Mais est-ce un « vrai » problème?

Est-ce un problème ?

Est-ce un vrai problème ?

Faux problème réjouissant…

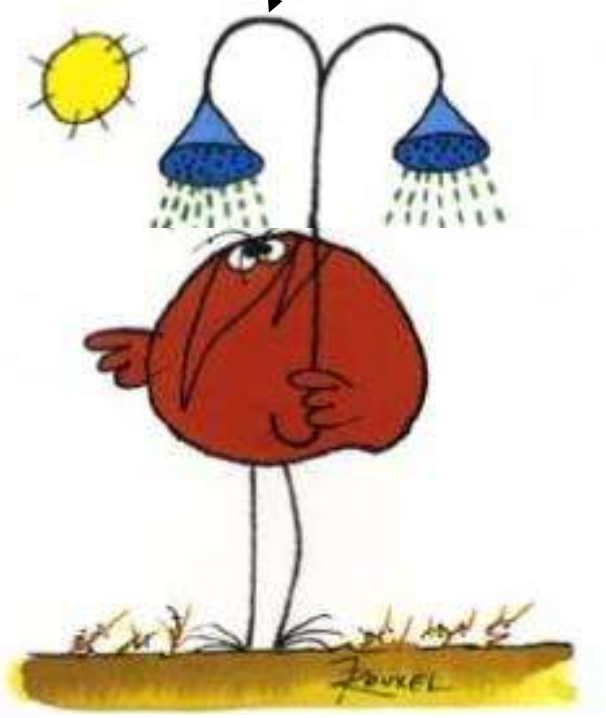


Fig. 1 bis

« **Déterminez les durées de maintien des signaux… »**

THALES

Mais est-ce un « vrai » problème?

Est-ce un problème ?

Est-ce un vrai problème ?

Excellente solution
à un faux problème

Fig. 1 ter

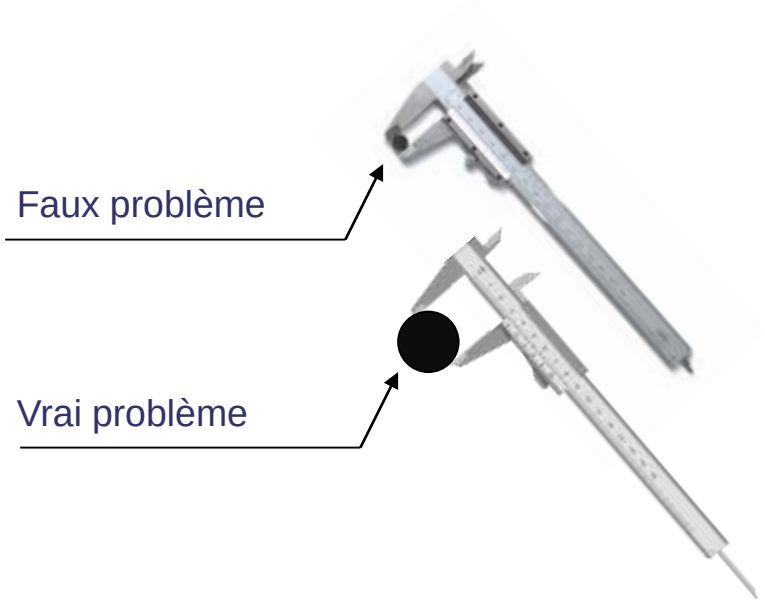
« **Déterminez les durées de maintien des signaux… »**

THALES

Mais est-ce un « vrai » problème?

Est-ce un problème ?

Est-ce un vrai problème ?



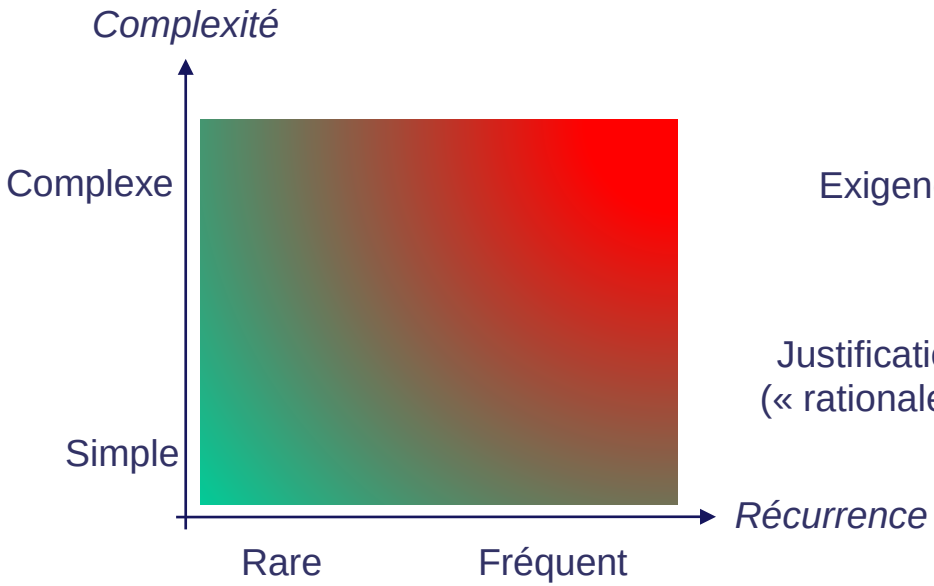
« Déterminez les durées de maintien des signaux… »

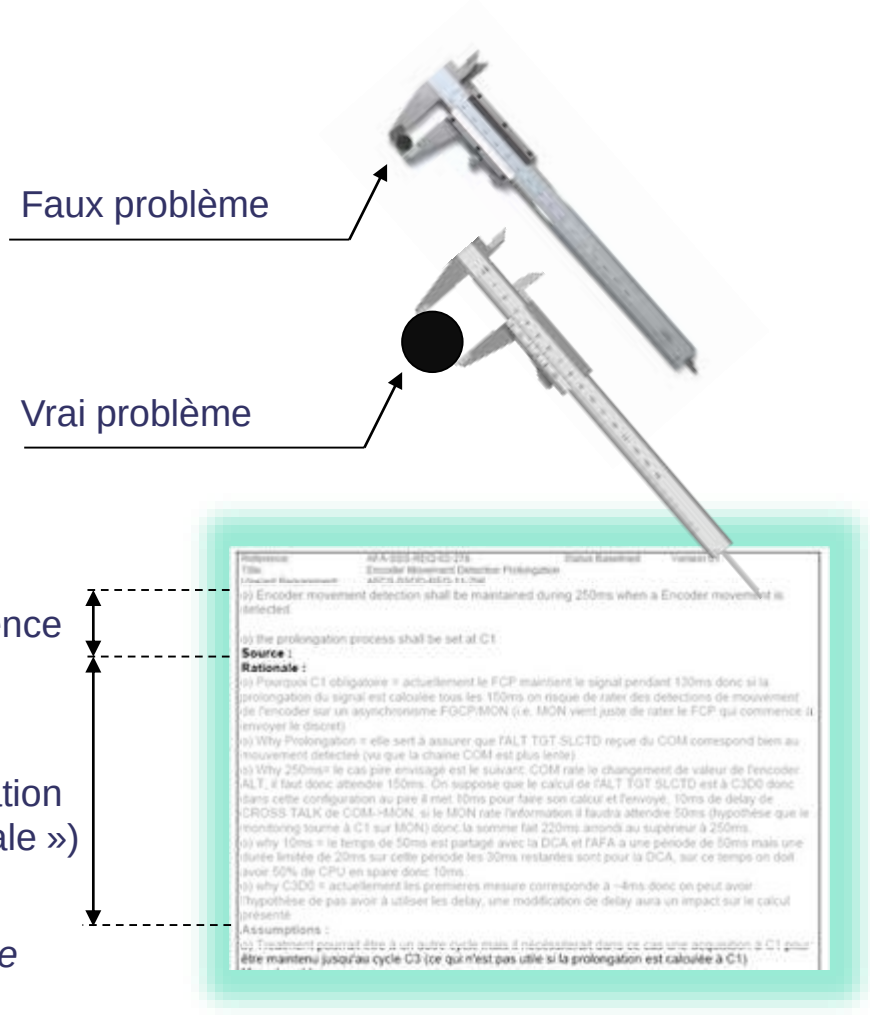
THALES

Mais est-ce un « vrai » problème?

Est-ce un problème ?

Est-ce un vrai problème ?





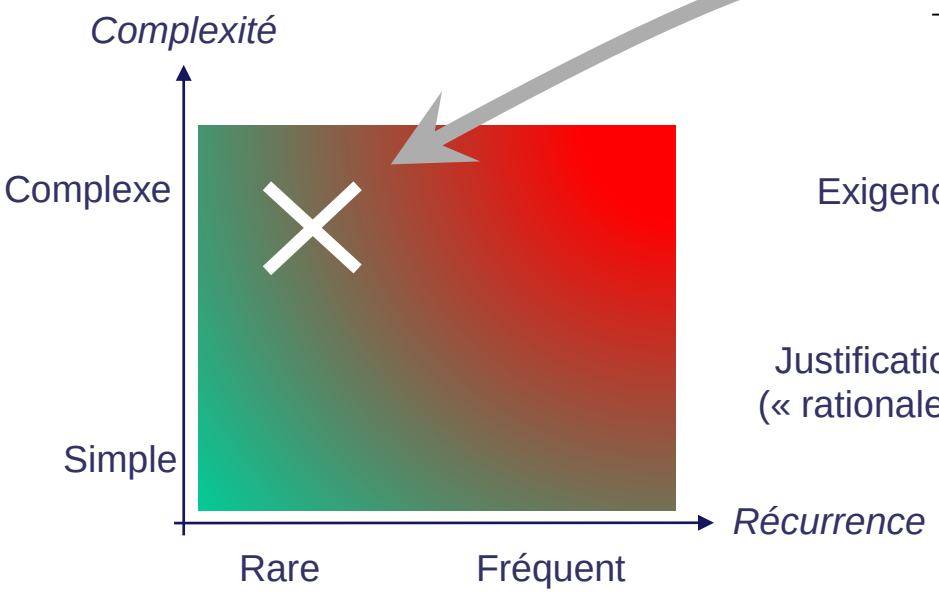
« **Déterminez les durées de maintien des signaux… »**

THALES

Mais est-ce un « vrai » problème?

Est-ce un problème ?

Est-ce un vrai problème ?



Faux problème

Vrai problème

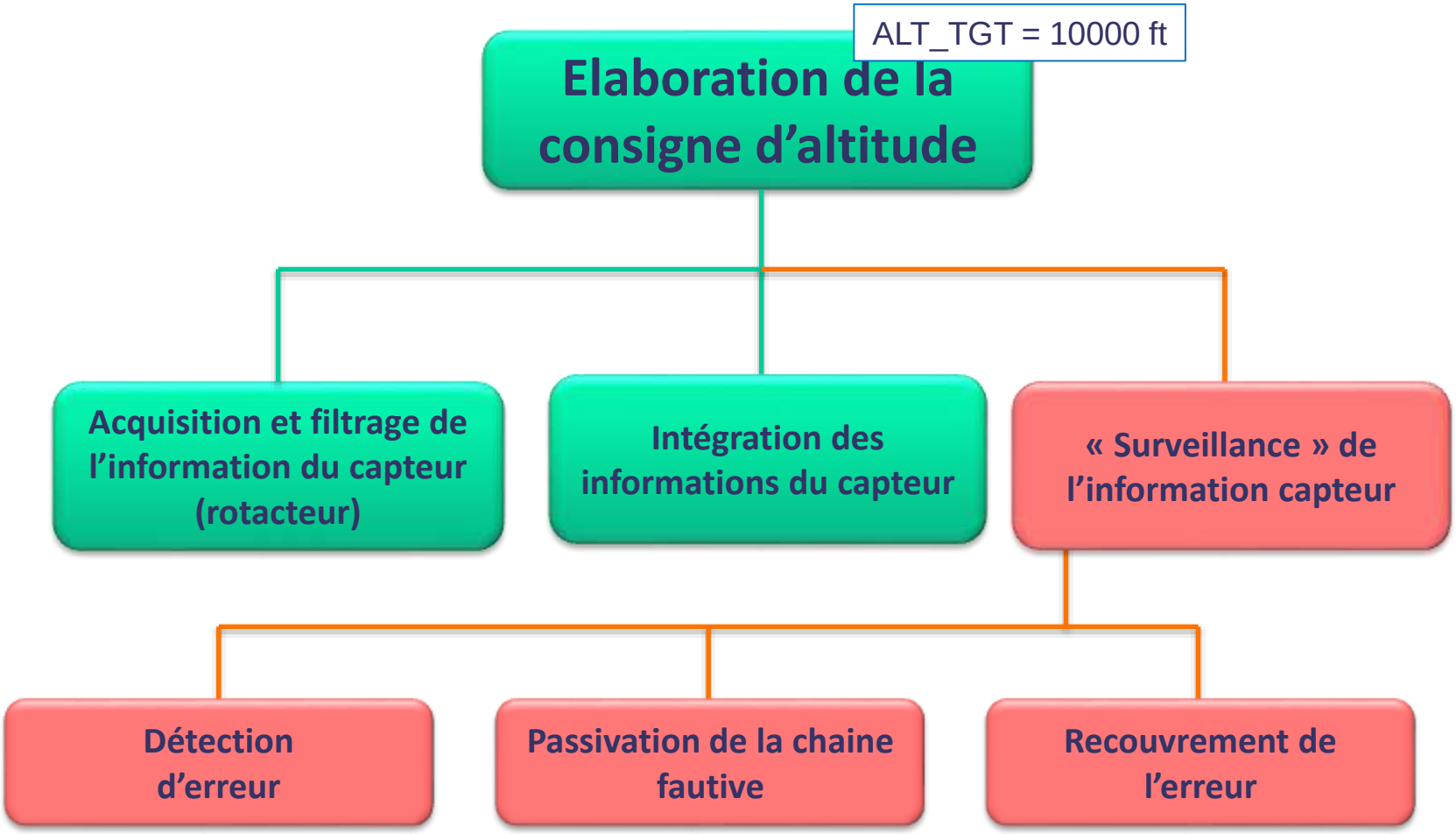
Exigence

Justification
(« rationale »)

« Déterminez les durées de maintien des signaux… »

THALES

La fonction cible



THALES

Du système… au modèle

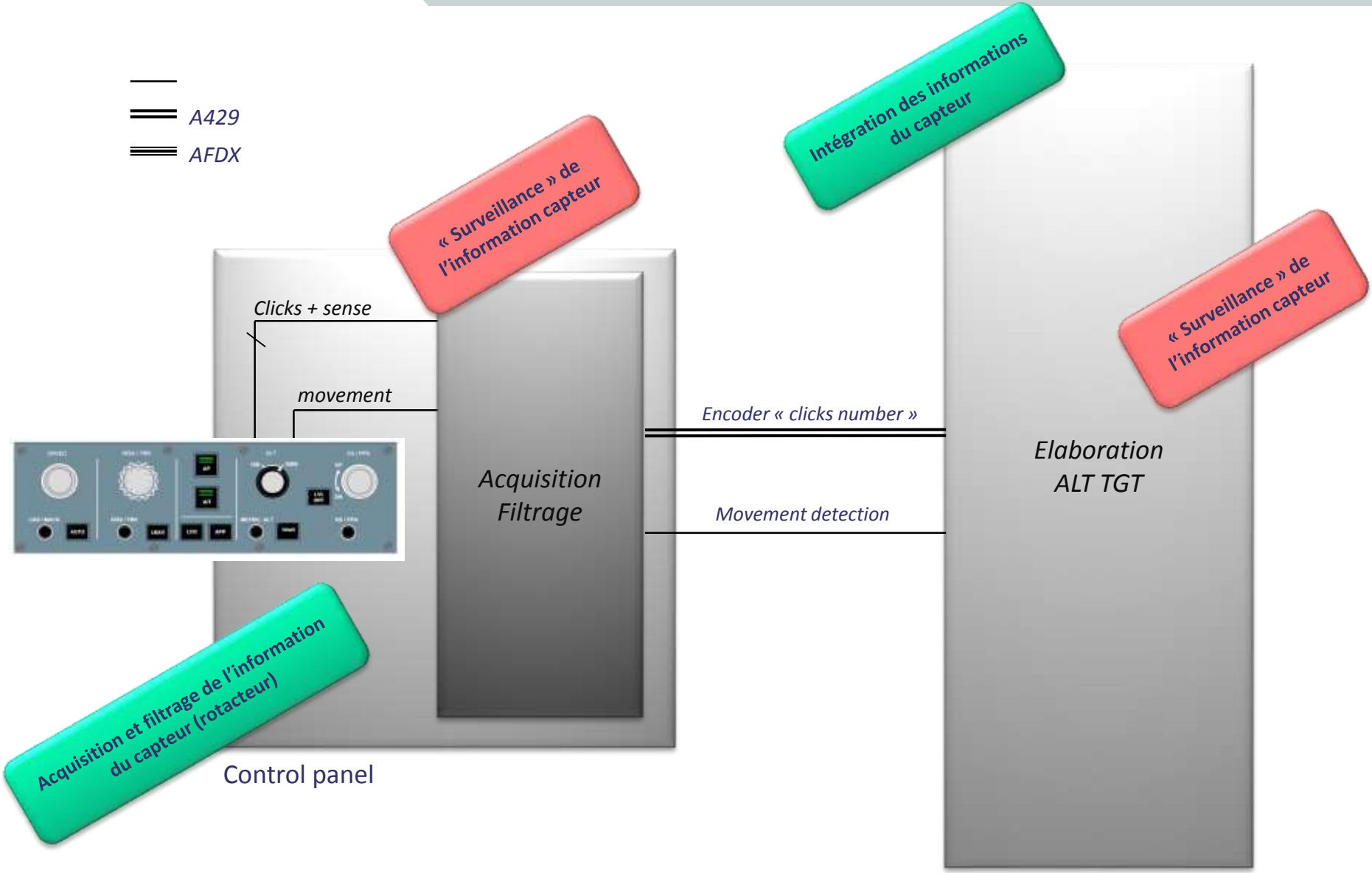
« Surveillance » de l'information capteur

Intégration des informations du capteur

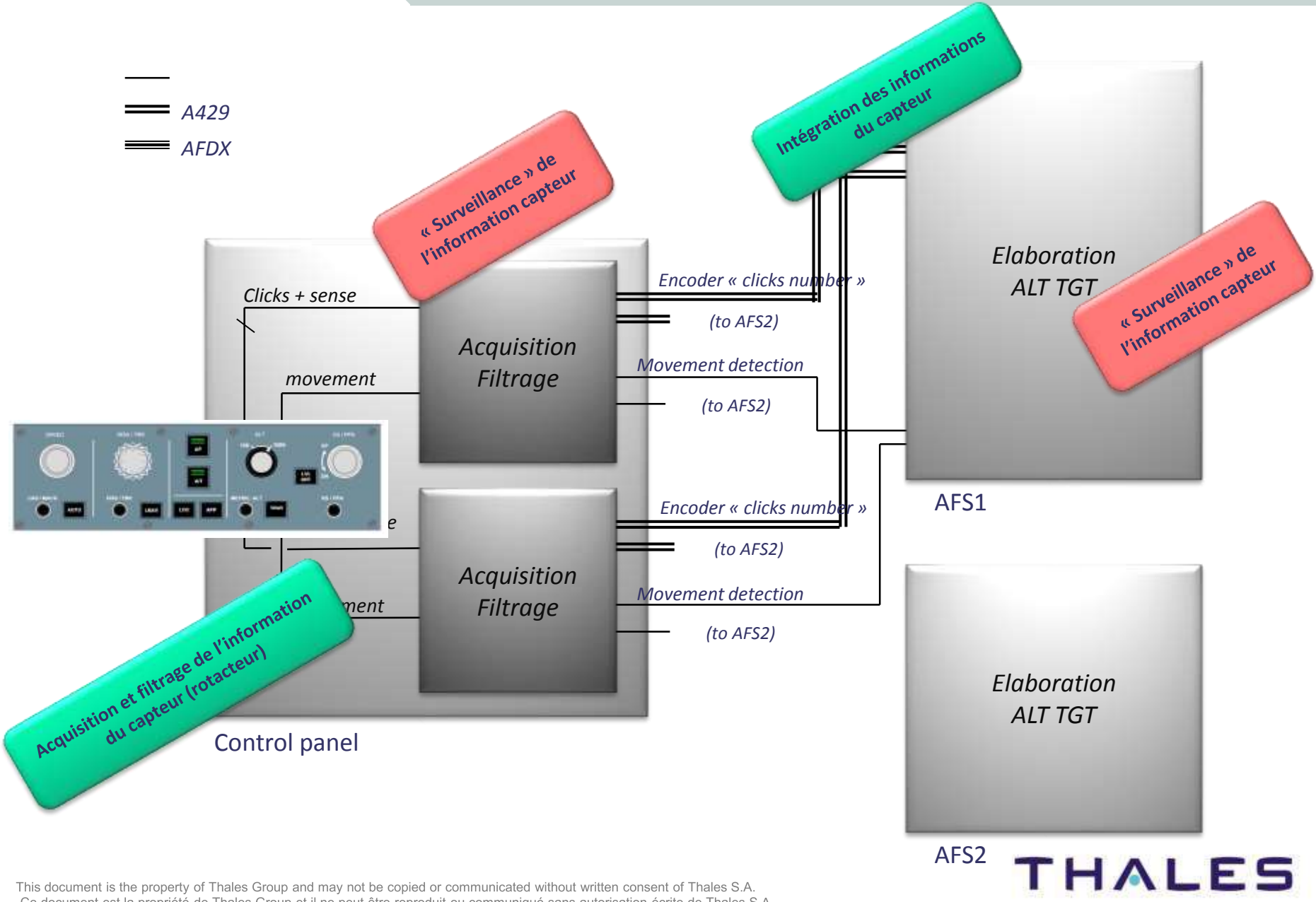
« Surveillance » de l'information capteur

Acquisition et filtrage de l'information du capteur (rotacteur)

Du système… au modèle

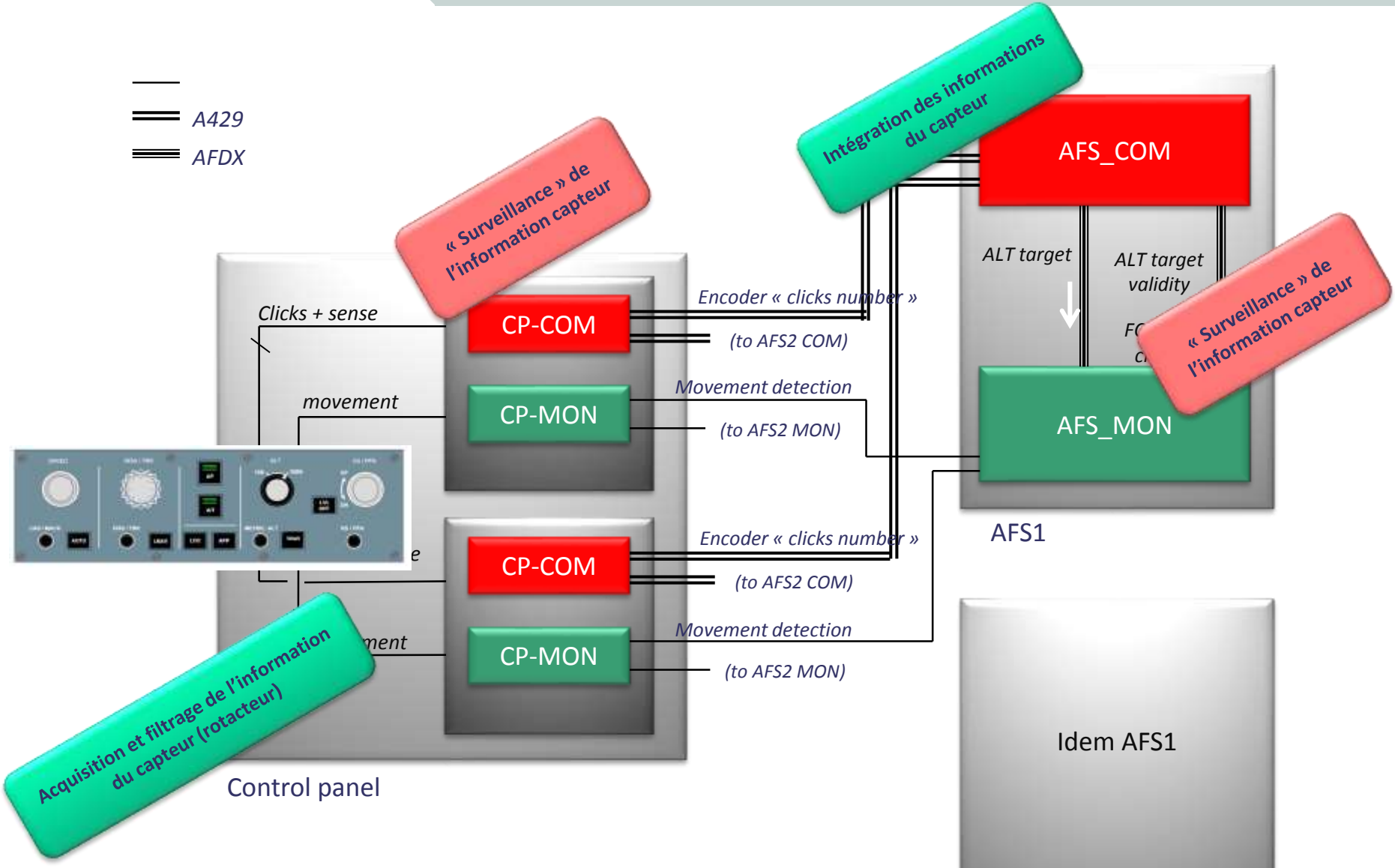


Du système… au modèle



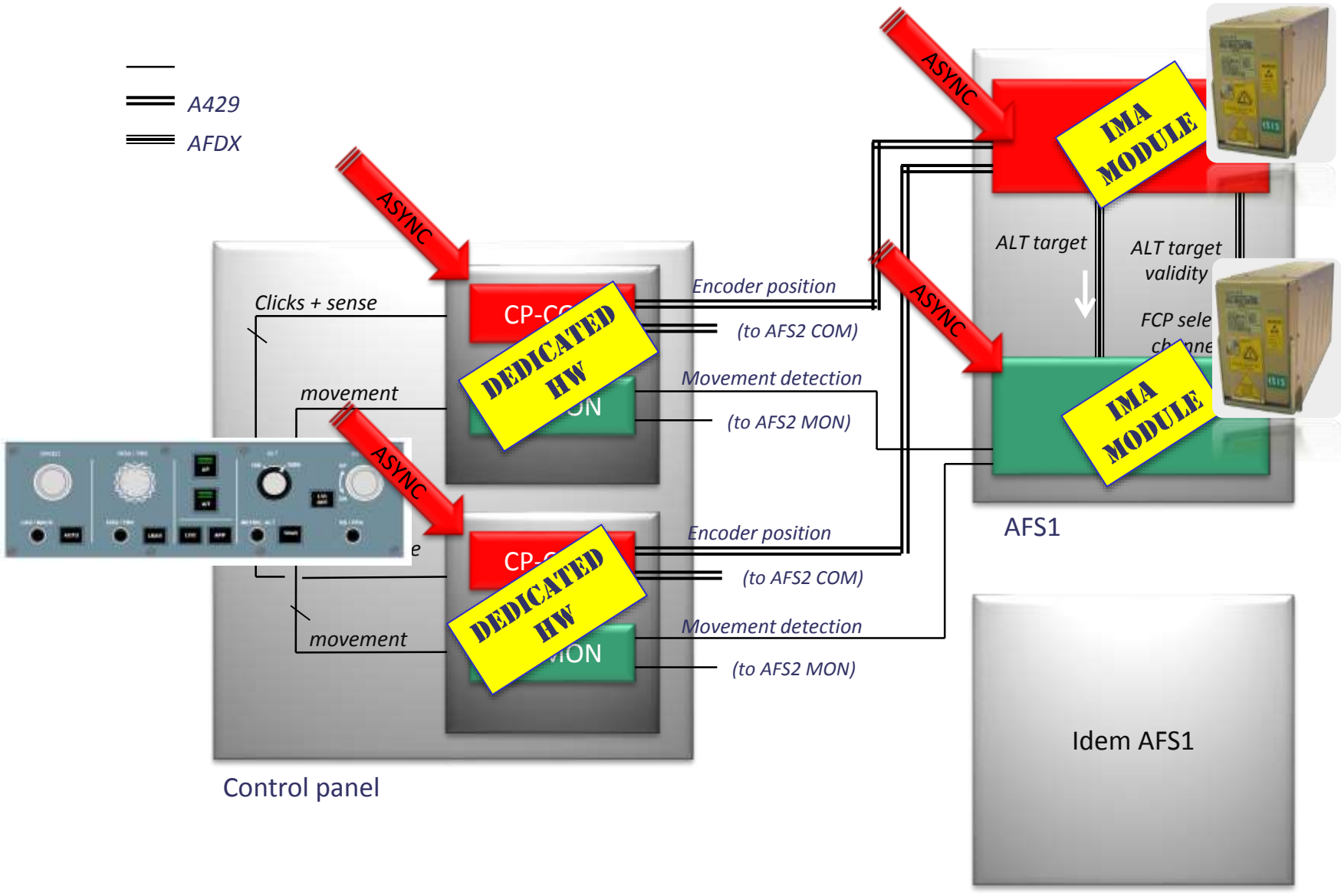
THALES

Du système… au modèle



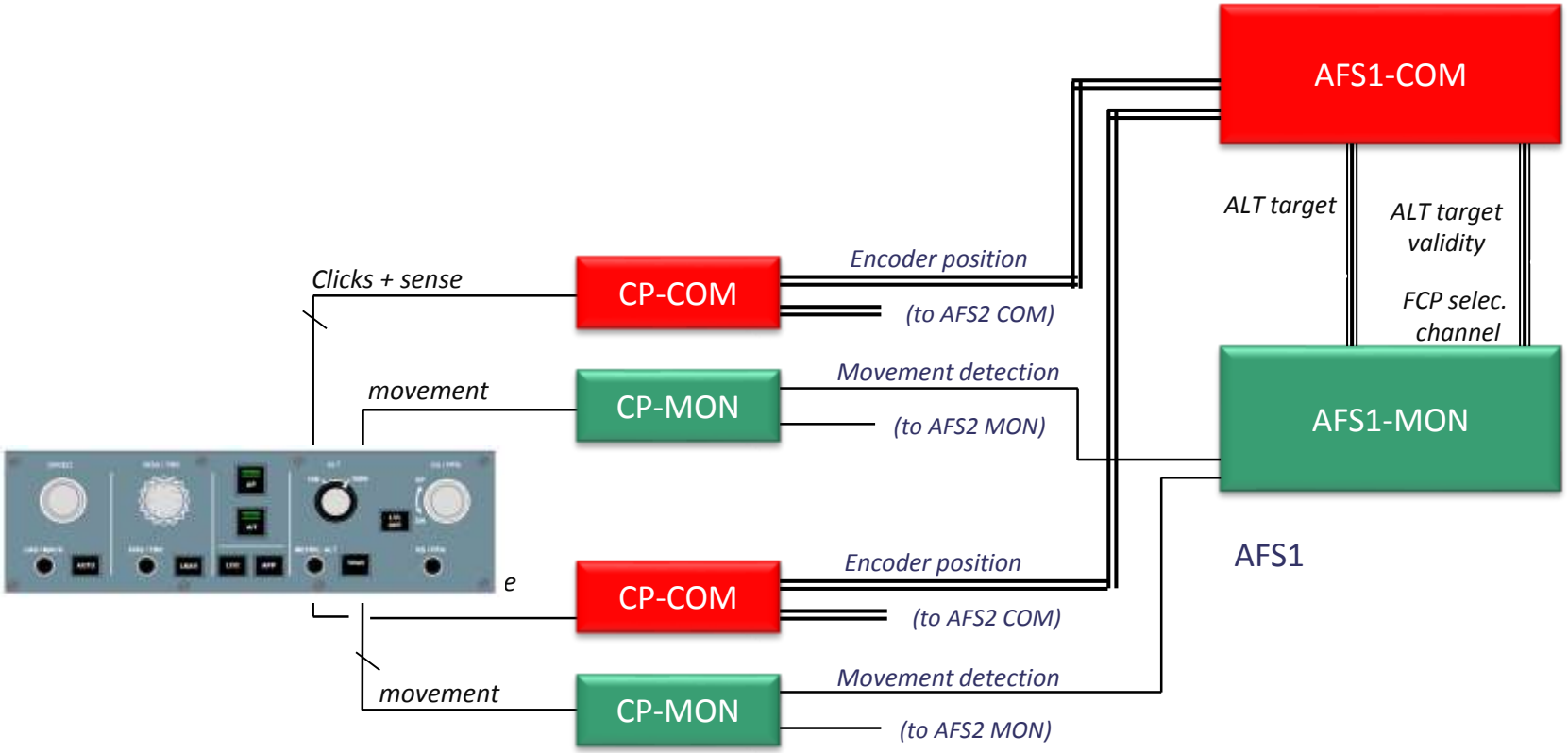
THALES

Du système… au modèle

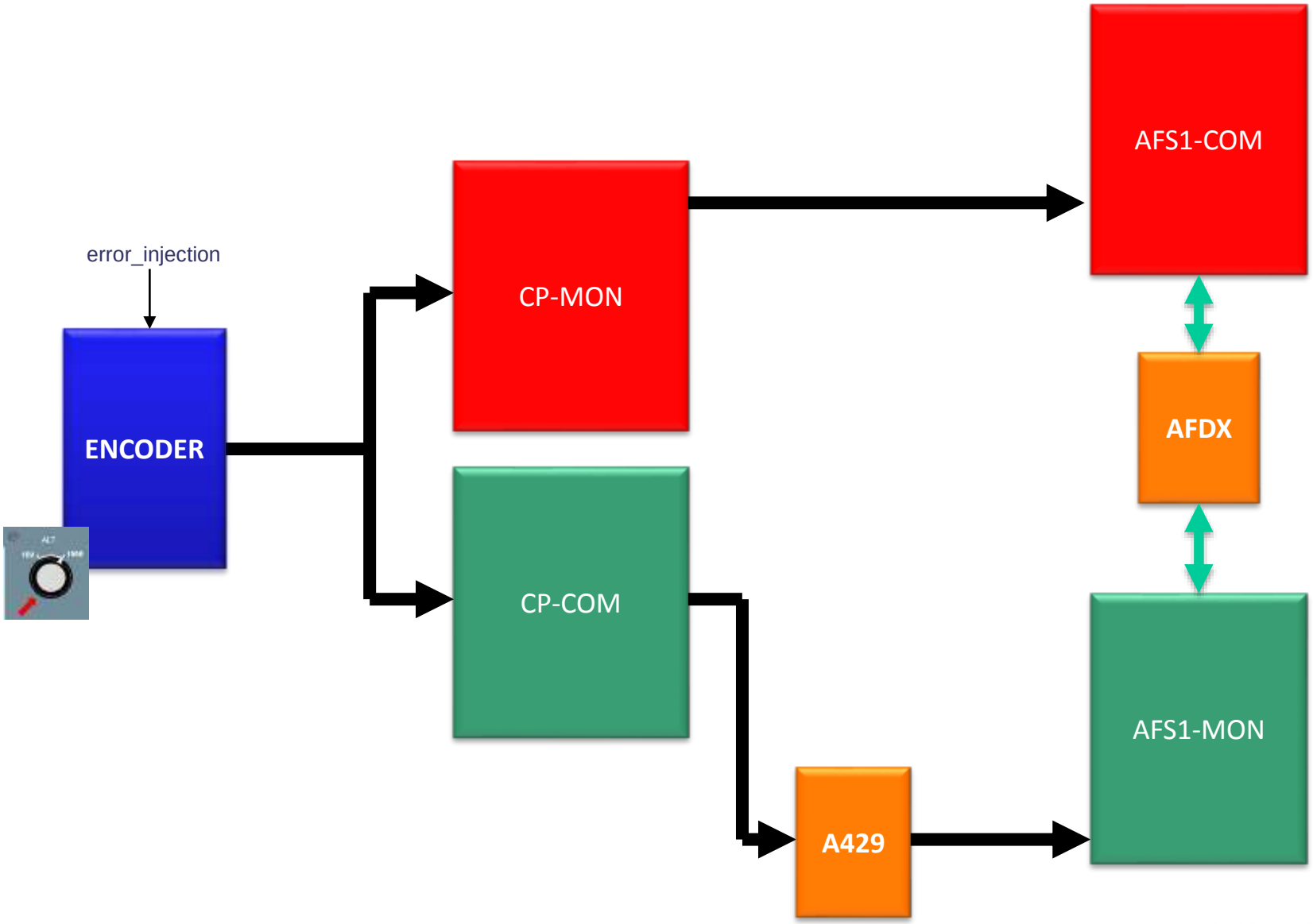


THALES

Du système… au modèle

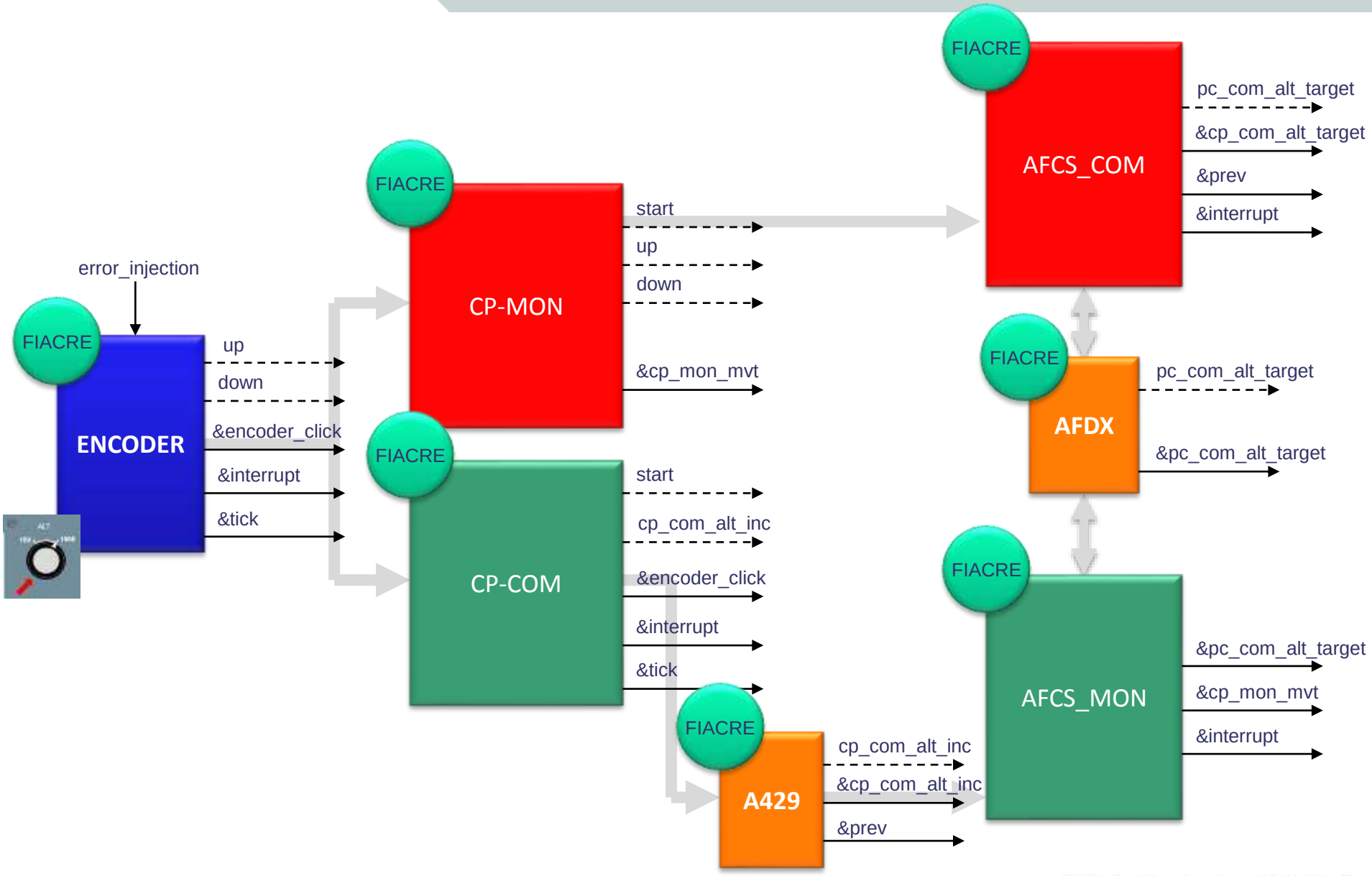


Du système… au modèle



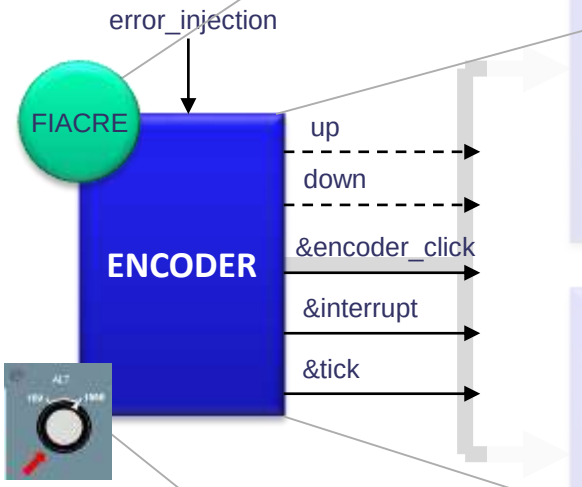
THALES

Du système… au modèle



THALES

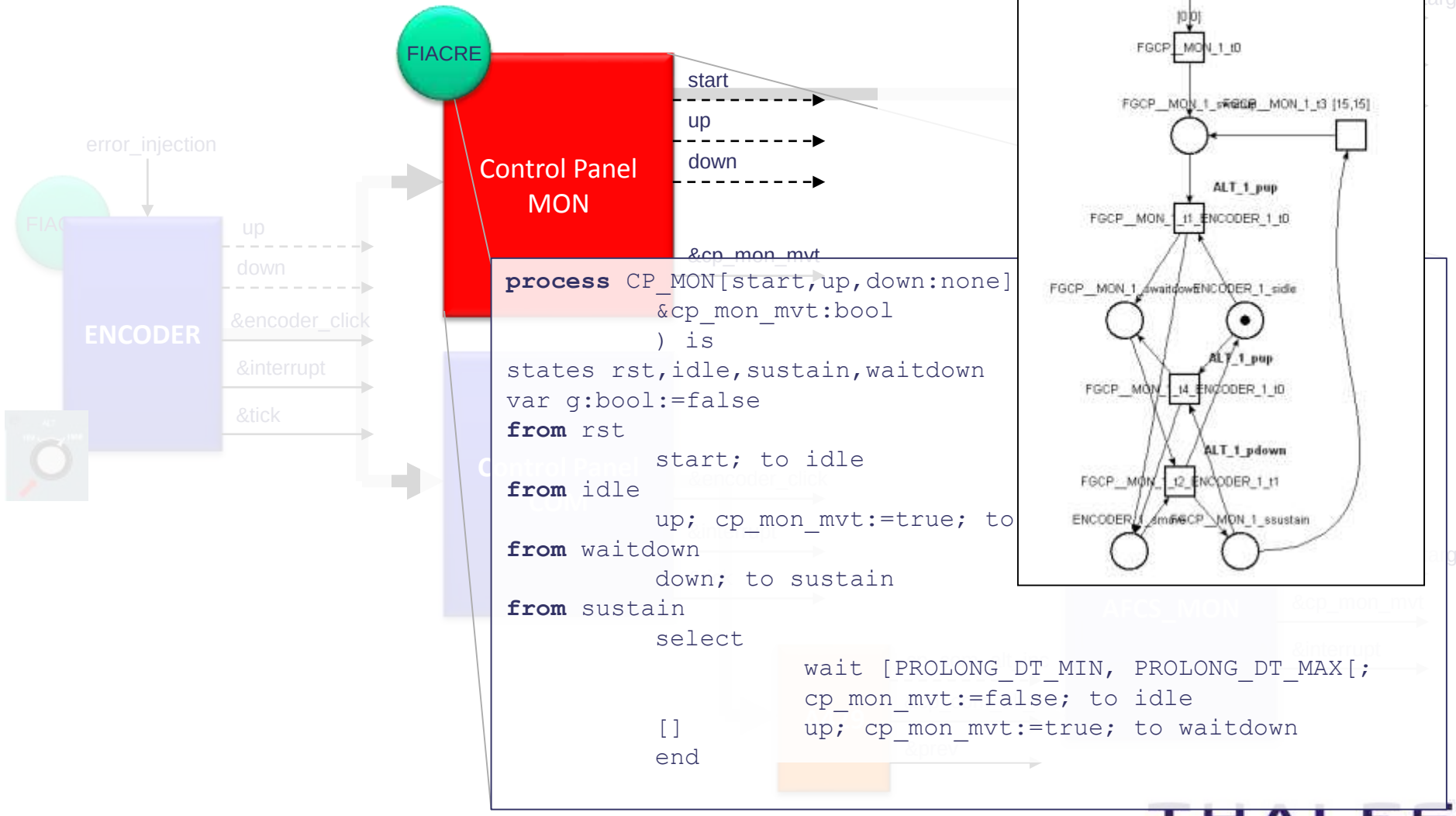
Du système… au modèle




```
process ENCODER[up,down:none](
          &encoder_click:EncoderClick,
          &interrupt:bool,
          errorInjection:bool,
          &tick:bool
          ) is
states idle,move,permanent_failure
var cpt_transient_failure:bool:=false
from idle
     on not interrupt;
     select
        encoder_click:=ChangeAltYes;
        fiacre_tag(MOVEMENT);
                    up;
                    to move
     [] on errorInjection;
                    fiacre_tag(PERM_FAIL);
                    encoder_click:=ChangeAltYes;
                    to permanent_failure
     end
from move
     on not interrupt;
#if (SAMPLING_ENCODER==1)
     tick:=true;
#endif
     encoder_click:=ChangeAltNo;
     down;
     to idle
```

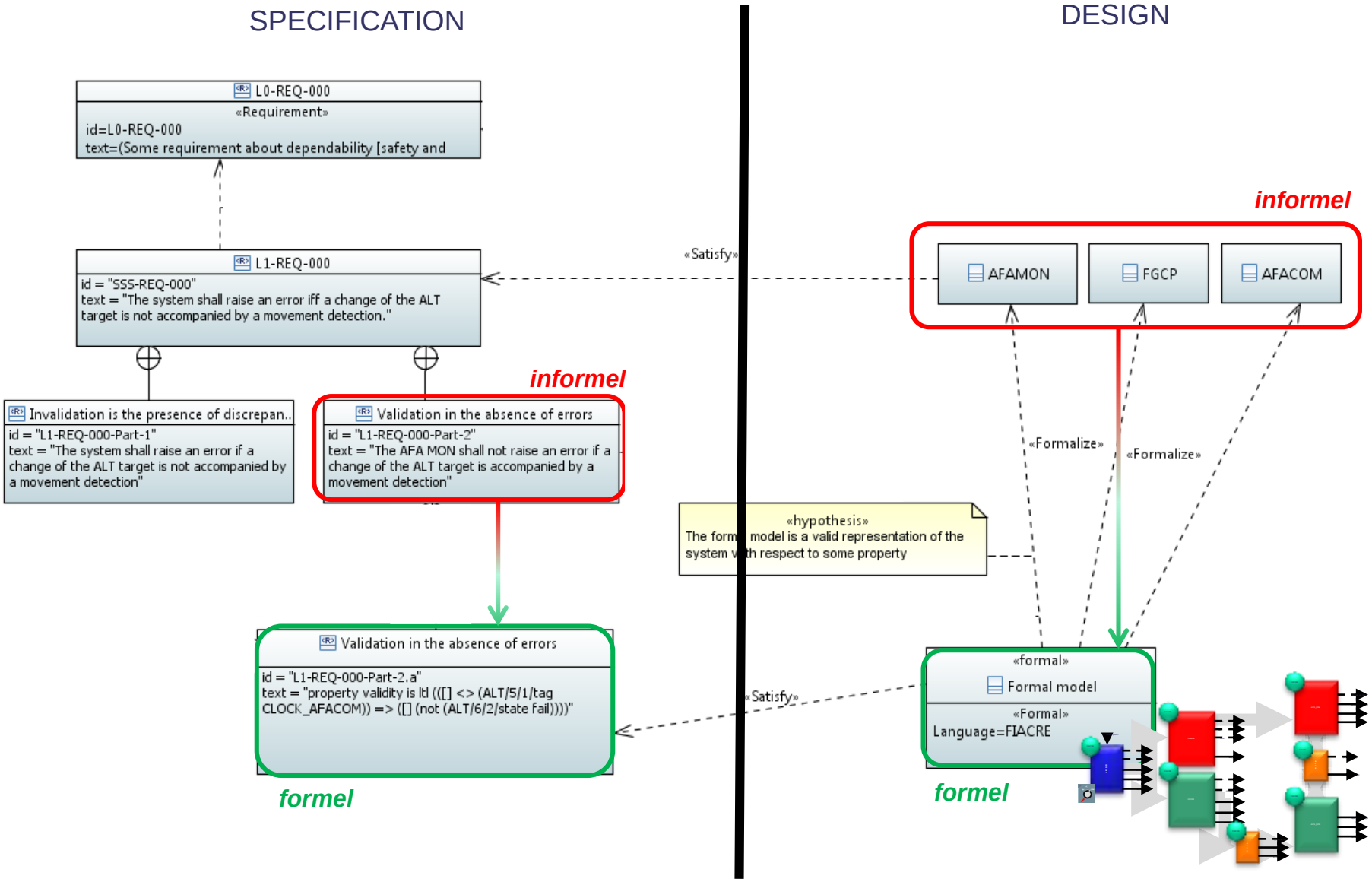

THALES

Du système… au modèle



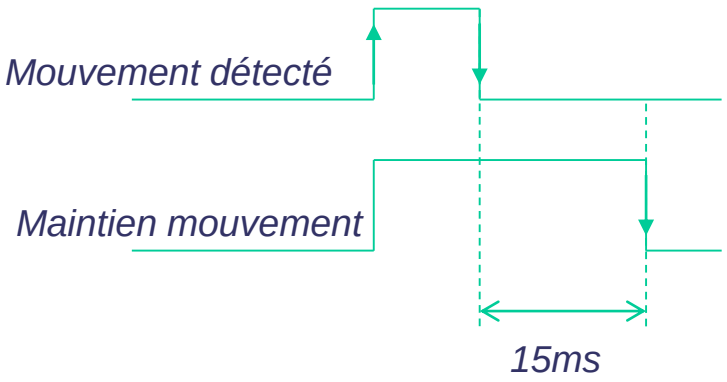
THALES

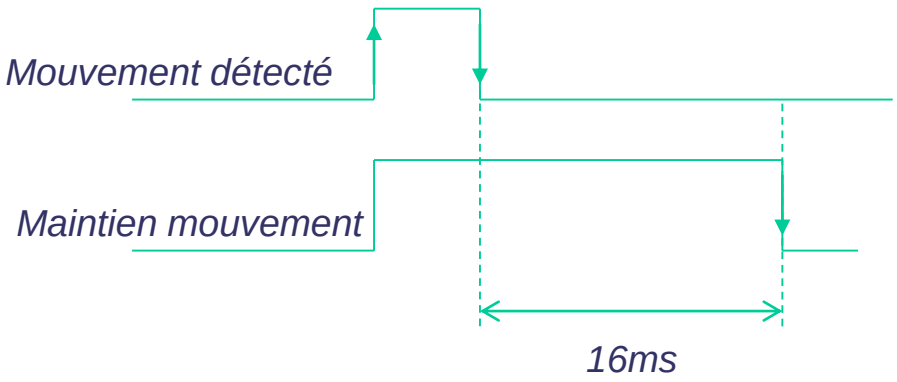
De l'exigence informelle… à l'exigence formelle



THALES

Finalement…






```
process
FGCP_MON[up,down:none](&extendedMvt:bool) is
(…)
wait [15,15];
(…)
```

```
process
FGCP_MON[up,down:none](&extendedMvt:bool) is
(…)
wait [16,16];
(…)
```

KO! + contre exemple

THALES

Quels résultats?

Les erreurs identifiées par *model-checking* « correspondent » à des erreurs observées dans le cycle de développement.

Pas « d'explosion » de l'espace d'état

- **Simplifications**
  - Pas de dérive d'horloge
- **Abstractions**
  - Pas de contrainte de délai entre deux mouvements
  - Abstraction des données échangées…
- **1 modèle par ordre d'initialisation, phase variable**
- **[Problème (très) simple]**

Temps de vérification acceptables, temps de familiarisation avec le formalisme FIACRE acceptable

L'analyse du ROI reste à faire…

THALES

Quelles suites?

Concernant le cas d'étude AFCS

- **Application de FIACRE / TINA à la vérification de la logique MASTER / SLAVE**

Et au-delà?

- **Travaux en cours dans le cadre du projet collaboratif INGEQUIP (IRT St-Exupéry)**
  - « Remontée des contre-exemples »
  - Finalisation des travaux sur la prise en compte des symétries?

- **Journées THALES, J2: « *Critical software development and formal methods* »**

THALES

Ce qui suit n’a pas été présenté.
Mais peut éventuellement être utile.

THALES

Quelles leçons?

Quelques *difficultés*

- **Techniques**
  - **Bien comprendre / cerner le problème**
  - Bien poser le problème
  - Bien choisir le formalisme, l'outil,…
  - Composer avec des problèmes « réels »
  - Disposer d'un outillage fiable
  - Assurer (?) la correction du modèle de vérification
  - Pouvoir exploiter les informations de diagnostic
  - Assurer le « passage à l'échelle »
  - Assurer la « réutilisabilité » des modèles

Quelle est la nature du problème ?
Quel rôle joue le temps dans le système?

THALES

Quelles leçons?

Quelques *difficultés*

- **Techniques**
  - Bien comprendre / cerner le problème
  - **Bien poser le problème**
  - Bien choisir le formalisme, l'outil,…
  - Composer avec des problèmes « réels »
  - Disposer d'un outillage fiable
  - Assurer (?) la correction du modèle de vérification
  - Pouvoir exploiter les informations de diagnostic
  - Assurer le « passage à l'échelle »
  - Assurer la « réutilisabilité » des modèles

Quelles propriétés attend-on?
Quelles abstractions peut-on faire?
Quelles simplifications peut-on faire? Avec quelles conséquences?

THALES

Quelles leçons?

Quelques *difficultés*

- **Techniques**
  - Bien comprendre / cerner le problème
  - Bien poser le problème
  - **Bien choisir le formalisme, l'outil,…**
  - Composer avec des problèmes « réels »
  - Disposer d'un outillage fiable
  - Assurer (?) la correction du modèle de vérification
  - Pouvoir exploiter les informations de diagnostic
  - Assurer le « passage à l'échelle »
  - Assurer la « réutilisabilité » des modèles

Comment choisir le « bon » formalisme / propriété?
Comment éviter de multiplier les formalismes?
Comment exploiter efficacement le modèle de conception?

THALES

Quelques *difficultés*

- **Techniques**
  - Bien comprendre / cerner le problème
  - Bien poser le problème
  - Bien choisir le formalisme, l'outil,…
  - **Composer avec des problèmes « réels »**
  - Disposer d'un outillage fiable
  - Assurer (?) la correction du modèle de vérification
  - Pouvoir exploiter les informations de diagnostic
  - Assurer le « passage à l'échelle »
  - Assurer la « réutilisabilité » des modèles

Quelles leçons?

Quelques *difficultés*

- **Techniques**
  - Bien comprendre / cerner le problème
  - Bien poser le problème
  - Bien choisir le formalisme, l'outil,…
  - Composer avec des problèmes « réels »
  - **Disposer d'un outillage fiable**
  - Assurer (?) la correction du modèle de vérification
  - Pouvoir exploiter les informations de diagnostic
  - Assurer le « passage à l'échelle »
  - Assurer la « réutilisabilité » des modèles

Quand on cherche à planter un clou, on ne cherche pas à tester le marteau.

THALES

Quelles leçons?

Quelques *difficultés*

- **Techniques**
  - Bien comprendre / cerner le problème
  - Bien poser le problème
  - Bien choisir le formalisme, l'outil,…
  - Composer avec des problèmes « réels »
  - Disposer d'un outillage fiable
  - **Assurer (?) la correction du modèle de vérification**
  - Pouvoir exploiter les informations de diagnostic
  - Assurer le « passage à l'échelle »
  - Assurer la « réutilisabilité » des modèles

Avoir (au moins) autant confiance dans le modèle de vérification que dans le modèle de conception…

Pouvoir dériver le modèle de vérification du modèle de conception

Pouvoir tirer profit du caractère formel du modèle pour vérifier certaines bonnes propriétés (*sanity checks*)?

Pouvoir exécuter le modèle…

THALES

Quelles leçons?

Quelques *difficultés*

- **Techniques**
  - Bien comprendre / cerner le problème
  - Bien poser le problème
  - Bien choisir le formalisme, l'outil,…
  - Composer avec des problèmes « réels »
  - Disposer d'un outillage fiable
  - Assurer (?) la correction du modèle de vérification
  - **Pouvoir exploiter les informations de diagnostic**
  - Assurer le « passage à l'échelle »
  - Assurer la « réutilisabilité » des modèles

« Remonter » les contre-exemples au niveau du modèle de vérification. *(problème général du MDE…)*

THALES

Quelles leçons?

Améliorer les outils… et, surtout :

Quelques *difficultés*

- **Techniques**
  - Bien comprendre / cerner le problème
  - Bien poser le problème
  - Bien choisir le formalisme, l'outil,…
  - Composer avec des problèmes « réels »
  - Disposer d'un outillage fiable
  - Assurer (?) la correction du modèle de vérification
  - Pouvoir exploiter les informations de diagnostic
  - **Assurer le « passage à l'échelle »**
  - Assurer la « réutilisabilité » des modèles

THALES

Quelles leçons?

Quelques *difficultés*

- **Non techniques**
  - Faire adhérer à la démarche
    - formel =/= ludique, réminiscences douloureuses…
  - Gérer la multiplicité des formalismes informels et formels
- **Estimer le gain…**

On ne vise pas *nécessairement* la suppression d'activités de vérification « au sens de la DO ». Les méthodes formelles si elles sont suffisamment automatisées permettent avant tout (i) d'éviter des erreurs et (ii) d'éviter la détection tardives des erreurs…

Quelles leçons?

Quelques *difficultés*

- **Non techniques**
  - Faire adhérer à la démarche
    - formel =/= ludique, réminiscences douloureuses…
  - Gérer la multiplicité des formalismes informels et formels
- **Estimer le gain…**

Les formalismes « mathématiques » sont familiers aux automaticiens, aux aérodynamiciens,…
Quid des informaticiens? (Ô paradoxe…)

THALES

Quelles leçons?

Quelques *difficultés*

- **Non techniques**
  - Faire adhérer à la démarche
    - formel =/= ludique, réminiscences douloureuses…
  - Gérer la multiplicité des formalismes informels et formels
- **Estimer le gain…**

« Overdose » de formalismes, de langages, de technologies,…

THALES

THALES

Références

[1] Fabien Kuntz et al, « Model-based diagnosis for avionics systems using minimal cuts », 22nd International workshop on Principles of Diagnosis

[2] Peter Schmitt *et al, «* A case study of specification and verification using JML in an avionics application », JTRES'06 Proceedings of the 4th international workshop on Java Technologies for real-time embedded systems

[3] Pierre-Alain Bourdil *et al, « Model-Checking Real-Time Properties of an AutoFlight Control System Function », ISSRE 2014, nov. 3-6, 214, Naples (à paraître)*

THALES