

Propagation des pannes dans les systèmes complexes

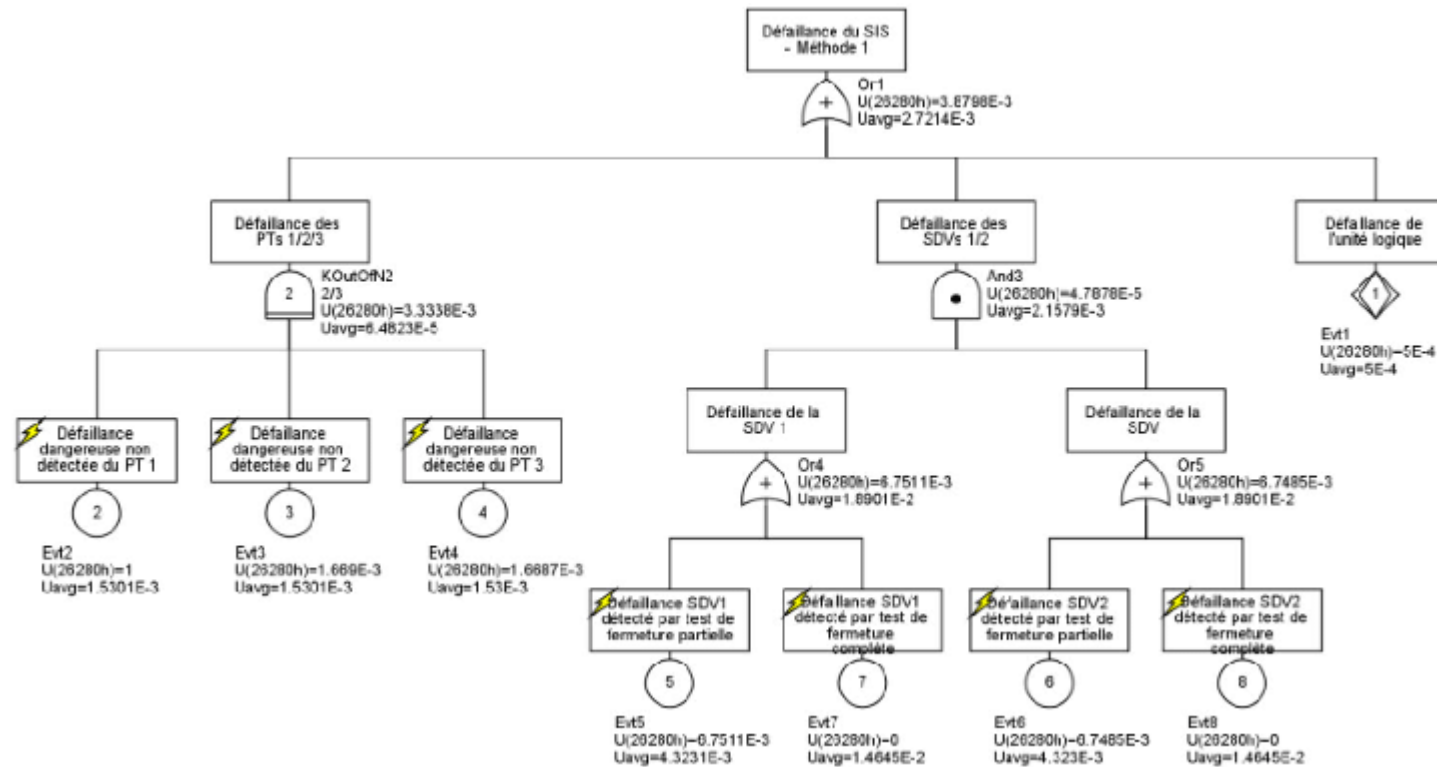
arbres de défaillances et dépendances causales

Analyse de sûreté de fonctionnement- FHA -PSSA -SSA

- ▶ **Functional Hazard Analysis**
 - ▶ Que peut-il arriver ?
 - ▶ Identification des dangers fonctionnels
 - ▶ A quel point cela est-il mauvais ?
 - ▶ Evaluation des conséquences des dangers dans le pire cas.
 - ▶ A quelle fréquence est-ce acceptable ?
 - ▶ Détermination des objectifs de safety
 - ▶ fréquence acceptable pour évènements ayant une certaine sévérité. (fh = flight hour)
 - ▶ catastrophique $< 10^{-9}/\text{fh}$
 - ▶ hasardeux $< 10^{-7}/\text{fh}$
 - ▶ majeur $< 10^{-5}/\text{fh}$
- ▶ **Preliminary System Safety Assessment**
 - ▶ Projection des évènements redoutés identifiés en FHA sur les sous-systèmes
 - ▶ Identification d'évènements de plus bas niveaux
- ▶ **System Safety Assessment**
 - ▶ Projections sur les composants des sous-systèmes
 - ▶ arbres de défaillance
 - ▶ Quantification des probabilités

Arbres de défaillance

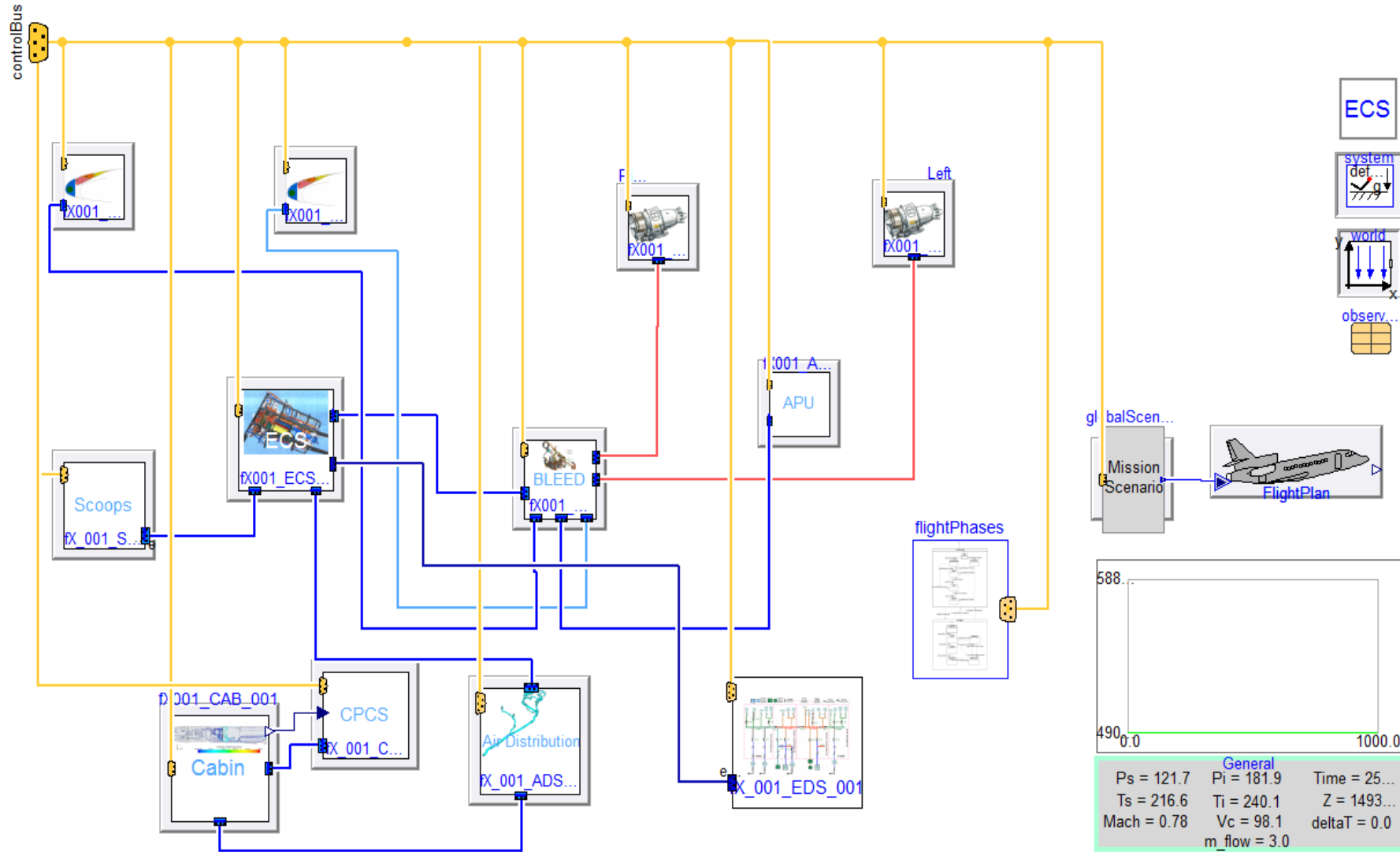
- ▶ Lourdeur des schémas
- ▶ Difficultés de relecture
- ▶ Activité très chronophage



Recherche d'une approche formelle

- ▶ Assurer la cohérence entre FHA-PSSA-SSA
- ▶ Modèles réutilisables
- ▶ Simulation plutôt que relecture
- ▶ Construction d'un modèle global complexe à partir d'une décomposition hiérarchique
- ▶ Travail collaboratif
- ▶ Objectif : faire évoluer les normes de certification dans l'aéronautique (ARP4754 et ARP4761)

Avion=Systeme de systemes



Modèles statiques/dynamiques

- ▶ Décomposition en sous-systèmes interconnectés = modèle statique
 - ▶ Définition des interfaces
- ▶ Comportement = modèle dynamique
 - ▶ Plusieurs comportements associés à un même sous-système selon l'objectif d'analyse, ou le niveau de maturité du modèle
- ➔ Modèle statique polymorphe
 - ▶ Interfaces adaptées à
 - ▶ Niveau de maturité du modèle
 - ▶ objectif d'analyse
- ▶ Objectifs d'analyse :
 - ▶ Performance
 - ▶ Range
 - ▶ Analyse de sûreté de fonctionnement
 - ▶ Cout
 - ▶ Impact environnemental

Outil de modélisation dans la plate-forme 3DExperience de Dassault-System

- ▶ Langage de Modélisation : Modelica
 - ▶ langage orienté objet destiné à la modélisation de systèmes complexes
 - ▶ systèmes comportant des composantes mécaniques, électriques, hydrauliques ou thermiques.
- ▶ Environnement de développement : Dymola
 - ▶ (Dynamic Modeling Laboratory) de [Dassault Systèmes](#)
- ▶ Modèle physique et modèle de Safety 2 modèles de comportement associés à un même modèle statique
- ▶ Exemple de mise en œuvre sur un sous-système d'un Falcon : Le system de conditionnement d'air

Analyse de sûreté de fonctionnement

- ▶ Dimensionnant pour la conception d'un avion
 - ▶ Objectifs vérifiés à tous les niveaux de décomposition du système et de chaque sous-système
- ▶ Définition des objectifs fonctionnels (FHA)
 - ▶ Projection sur la décomposition en sous-systèmes (modèle statique)
- ▶ Propagation des pannes au travers des interfaces
 - ▶ Exigences de safety de chaque sous-système
 - ▶ Choix d'architecture : redondances

Modélisation du comportement sur occurrence de pannes

- ▶ 2 types de modèles
 - ▶ Les modèles de sûreté de fonctionnement (safety)
 - ▶ Comportements simplifiés : propagation des pannes par des équations booléennes
 - ▶ Abstraction du temps
 - ▶ Les modèles dysfonctionnels
 - ▶ Modèles physiques complexes
 - ▶ Equations différentielles (modélisation du temps)
 - ▶ Modèles de Safety utilisés dès l'amont de la définition du système/sous-système
 - ▶ Modèles dysfonctionnels utilisés dans un range limité couplés à des modèles physiques complexes
 - ▶ Exemples : charbonnage d'un contact, dérive d'un capteur ...

Modèles formels pour les études de Safety

- ▶ Obtenir un système d'équations booléennes qui décrit la propagation des pannes
 - ▶ Pour chaque système de la décomposition
 - ▶ Relier les interfaces d'entrée/sortie par une équation qui traduit la conséquence d'une entrée défaillante et des pannes internes de ce système sur les sorties
- ▶ Visualiser cette propagation dans un simulateur
- ▶ Générer un arbre de défaillance
- ▶ Calculer les coupes minimales
- ▶ Quantifier la probabilité d'occurrence de l'évènement redouté

Problème de la propagation dans un système complexe : boucle de causalité

- ▶ Exemple de causalité :
 - ▶ Système électrique
 - ▶ Fournit de l'électricité par transformation d'énergie mécanique prélevée sur le moteur
 - ▶ Système carburant
 - ▶ Injecte le carburant dans le moteur par des pompes électriques
 - ▶ Moteur
 - ▶ fournit de l'énergie mécanique lorsqu'il est alimenté en carburant
- ▶ **Le moteur est en panne** lorsqu'il n'a plus de carburant
- ▶ le système carburant n'injecte plus de carburant si les pompes sont en pannes
- ▶ les pompes sont en pannes s'il n'y a plus d'électricité
- ▶ le système électrique ne fournit plus d'électricité s'il ne reçoit plus d'énergie mécanique
- ▶ il n'y a plus d'énergie mécanique **si le moteur est en panne**

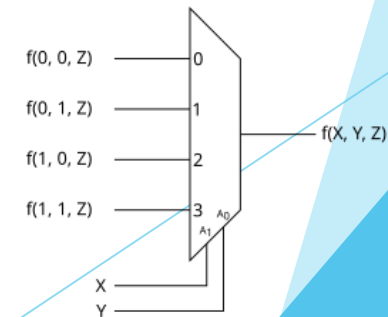
Résolution des boucles de causalité

► Expansion de Shannon

- décomposition d'une équation booléenne selon une ou plusieurs variables principales.
 - quelle que soit la fonction F : $F = x.F_x + \bar{x}.F_{\bar{x}}$ où F est une formule booléenne, x est une variable, $\bar{x}$ est la négation de x et les formules F_x et $F_{\bar{x}}$ sont obtenus à partir de F en affectant x et $\bar{x}$ à 1 et 0 respectivement.

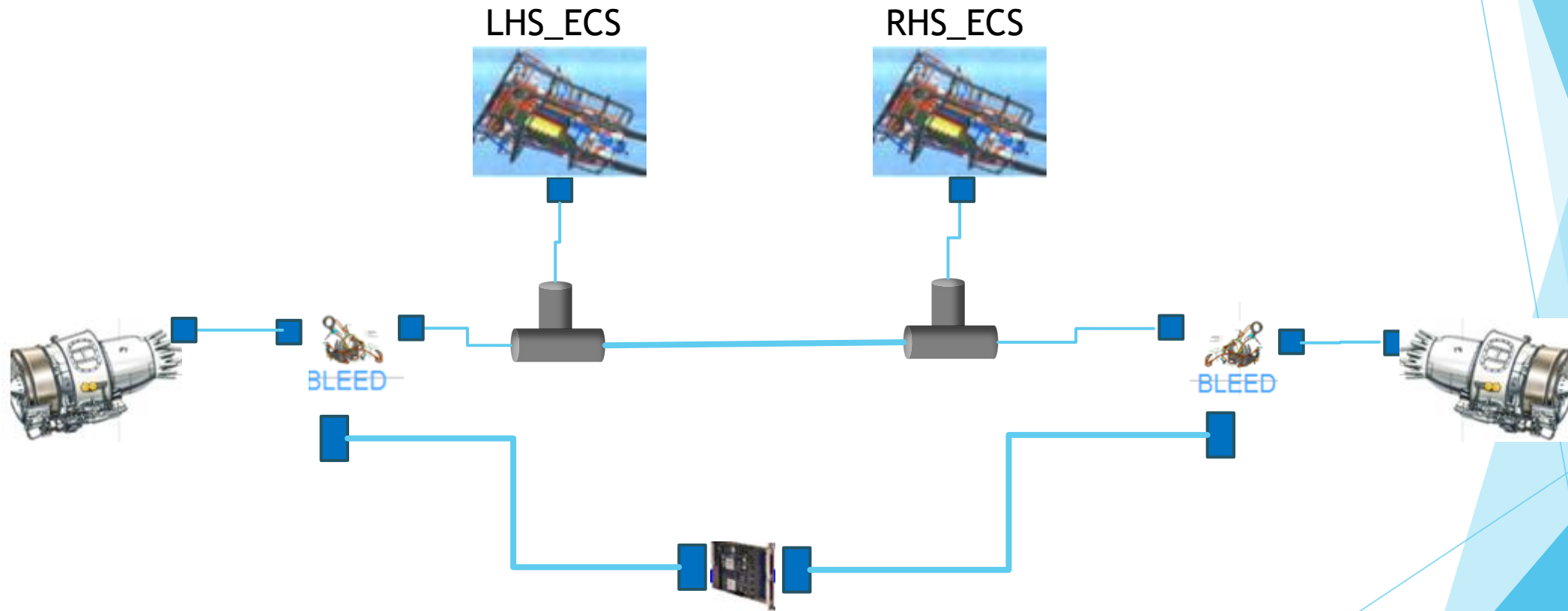
► Boucle de causalité = une variable dépend d'elle-même

- On casse la boucle en décomposant l'équation selon Shannon en prenant la variable de boucle comme variable principale
 - $v = v.F_1 + \bar{v}.F_0$
- On vérifie la stabilité de la boucle
- On choisit la partie négative ou positive de la décomposition de Shannon en fonction de la valeur de la variable à l'instant initial (lorsqu'aucune panne n'est présente)
- Les boucles peuvent être complexes car portant sur plusieurs variables

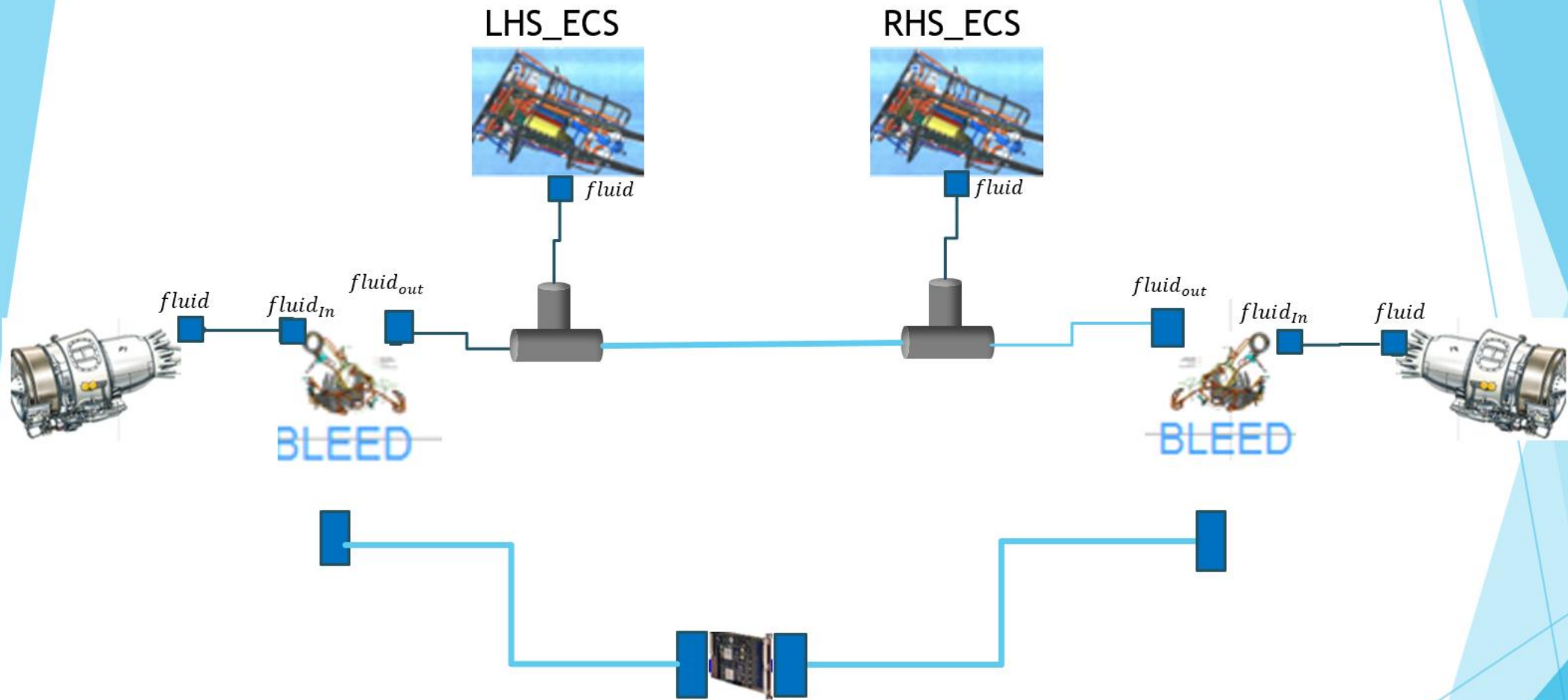


Etude d'un sous-système : le BLEED

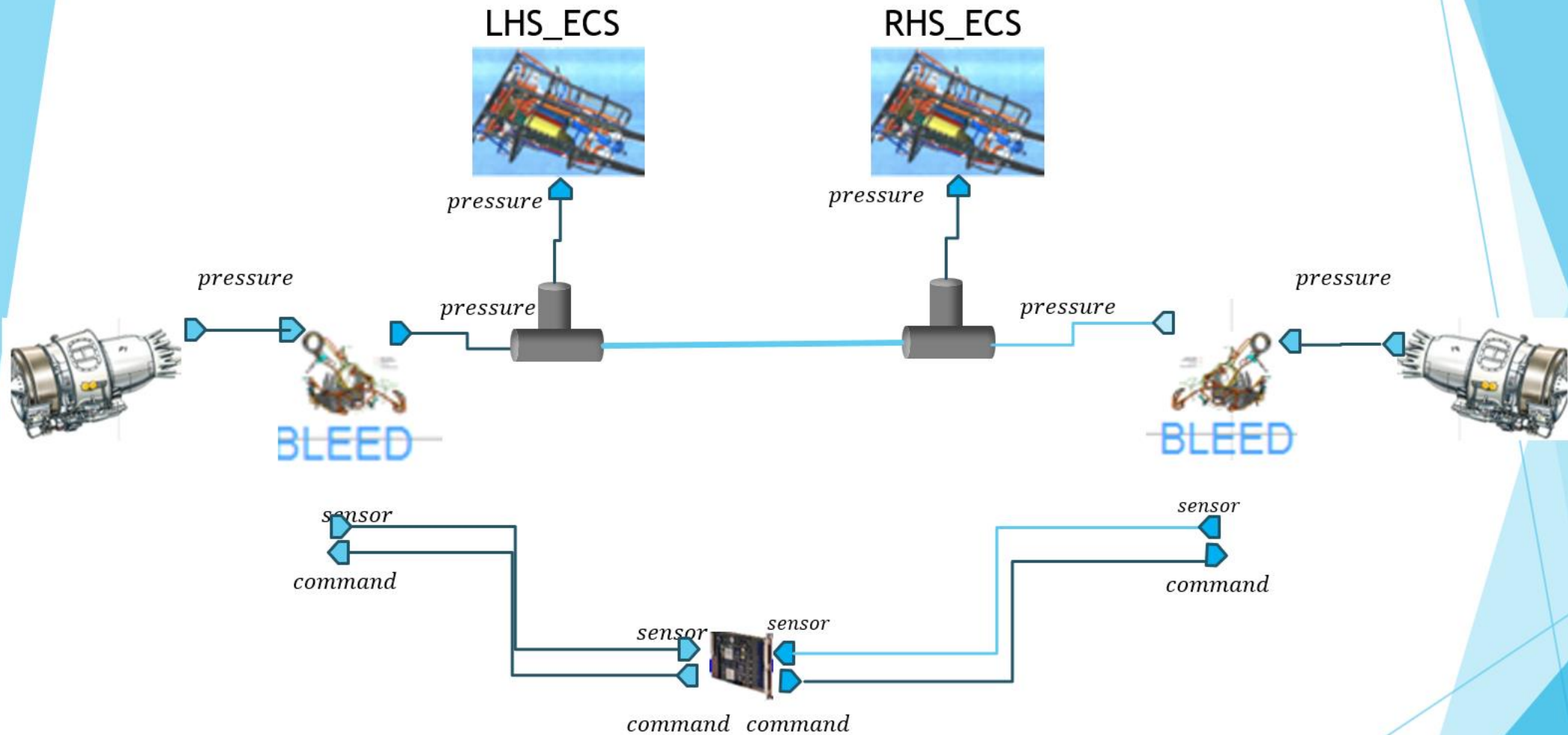
exemple simplifié



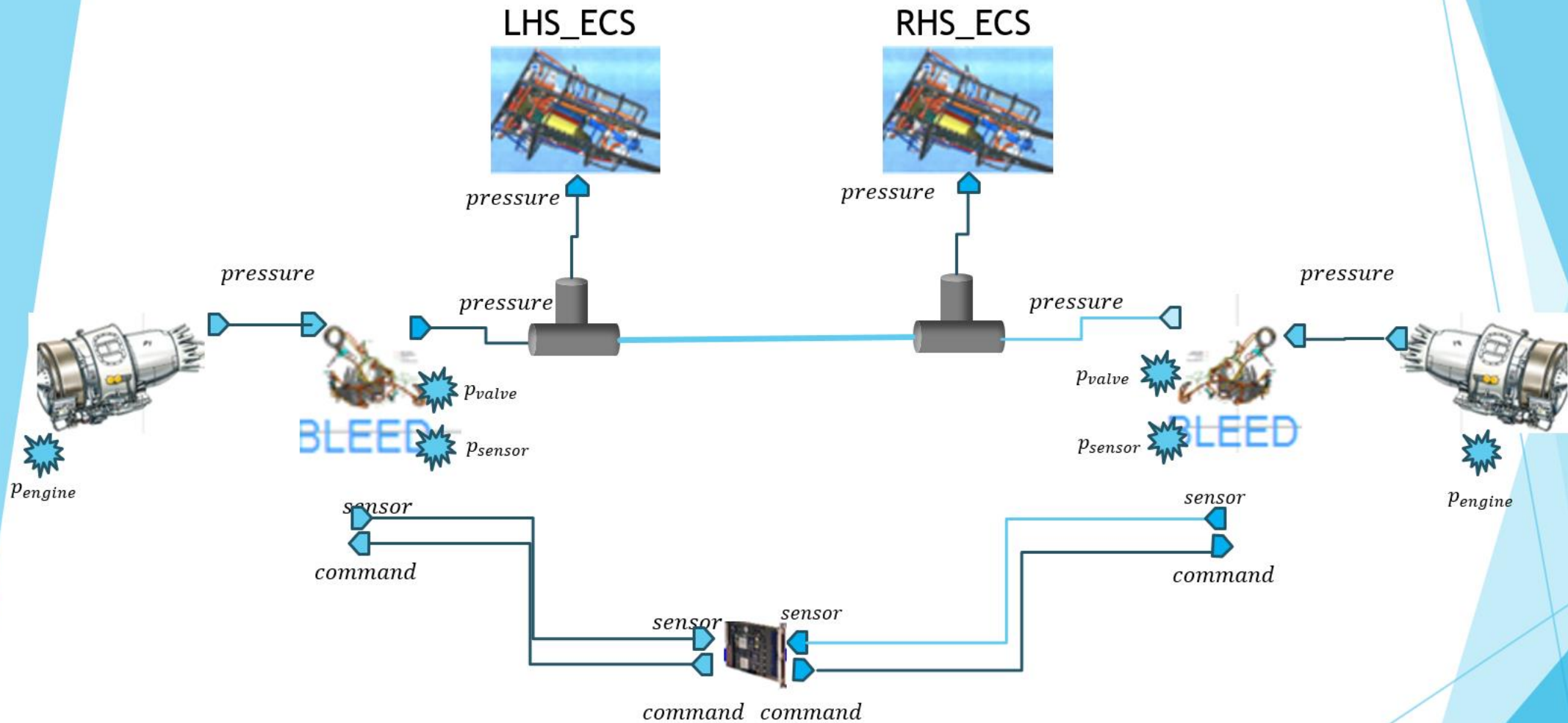
Animation-1



Animation-2 les interfaces s'adaptent au problème étudié



Animation-2 on identifie les pannes du système



Modélisation des objets du système

▶ Moteur

▶ Interface : $fluid$

▶ Panne : p_{engine}

▶ BLEED

moteur : $fluid_{in}$

▶ Interface : tuyau : $fluid_{out}$

contrôleur : $\begin{cases} sensor \\ command \end{cases}$

▶ Panne : p_{sensor}, p_{valve}

▶ Contrôleur

▶ Interface : $sensor$

$command : close$

▶ Tuyau

▶ Interface : $fluid_L, fluid_R, fluid_{out}$

• Moteur

$$pressure = \overline{p_{engine}}$$

• BLEED

$$\begin{cases} no_{pressure_out} = close \vee p_{pressure_in} \\ over_{pressure_out} = \overline{close} \wedge \overline{no_{pressure_in}} \wedge (p_{sensor} \wedge p_{valve}) \end{cases}$$

$$sensor = \overline{no_{pressure_out}} \wedge \overline{over_{pressure_out}}$$

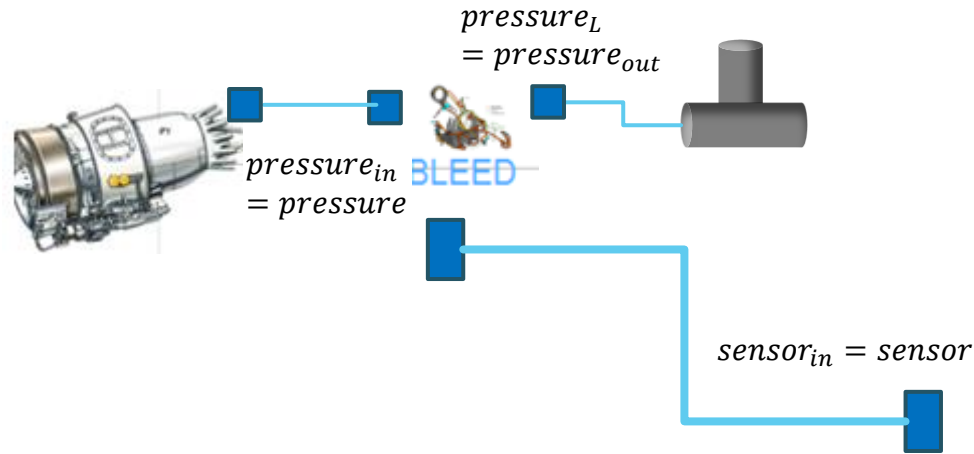
• Contrôleur

$$close = \overline{sensor_{in}}$$

• Tuyau

$$pressure_{out} = pressure_L \wedge pressure_G$$

Compilation du modèle



Résolution du système $\Rightarrow$ boucle de causalité sur la variable command

$$close = \overline{no_{pressure}} \wedge (p_{sensor} \vee \overline{over_{pressure}}) = no_{pressure} \vee \overline{p_{sensor}} \wedge over_{pressure}$$

$$close = close \vee p_{engine} \vee \overline{p_{sensor}} \wedge (\overline{close} \wedge p_{valve} \wedge \overline{p_{engine}})$$

$$close = close \wedge \overline{close} \wedge (p_{engine} \vee \overline{p_{sensor}} \wedge p_{valve})$$

A l'état initial $close = false$; on vérifie que la boucle est stable; l'équation de *command* est donnée par la partie négative de la décomposition de shannon

$$close = p_{engine} \vee \overline{p_{sensor}} \wedge p_{valve}$$

On obtient les équations en sortie du BLEED :
$$\begin{cases} no_{pressure} = p_{engine} \\ over_{pressure} = \overline{p_{engine}} \wedge p_{sensor} \wedge p_{valve} \end{cases}$$

Système d'équations résultant

$$pressure_{in} = pressure$$

$$sensor_{in} = sensor$$

$$pressure_L = pressure_{out}$$

$$pressure = \overline{p_{engine}}$$

$$\begin{cases} no_{pressure} = close \vee p_{engine} \\ over_{pressure} = \overline{close} \wedge p_{valve} \end{cases}$$

$$sensor$$

$$= \overline{no_{pressure}} \wedge (over_{pressure} \wedge p_{sensor} \vee \overline{over_{pressure}})$$

$$= \overline{no_{pressure}} \wedge (p_{sensor} \vee \overline{over_{pressure}})$$

$$close = \overline{sensor_{in}}$$

Simulation

LHS_ECS



pressure 

pressure

p_{valve}

 p_{sensor}

sensor

command

sensor

$$\textit{command} \quad \textit{command}$$

RHS_ECS



pressure

pressure

 p_{valve} p_{sensor}

sensor

command

sensor

sensor

$$\textit{command} \quad \textit{command}$$

pressure

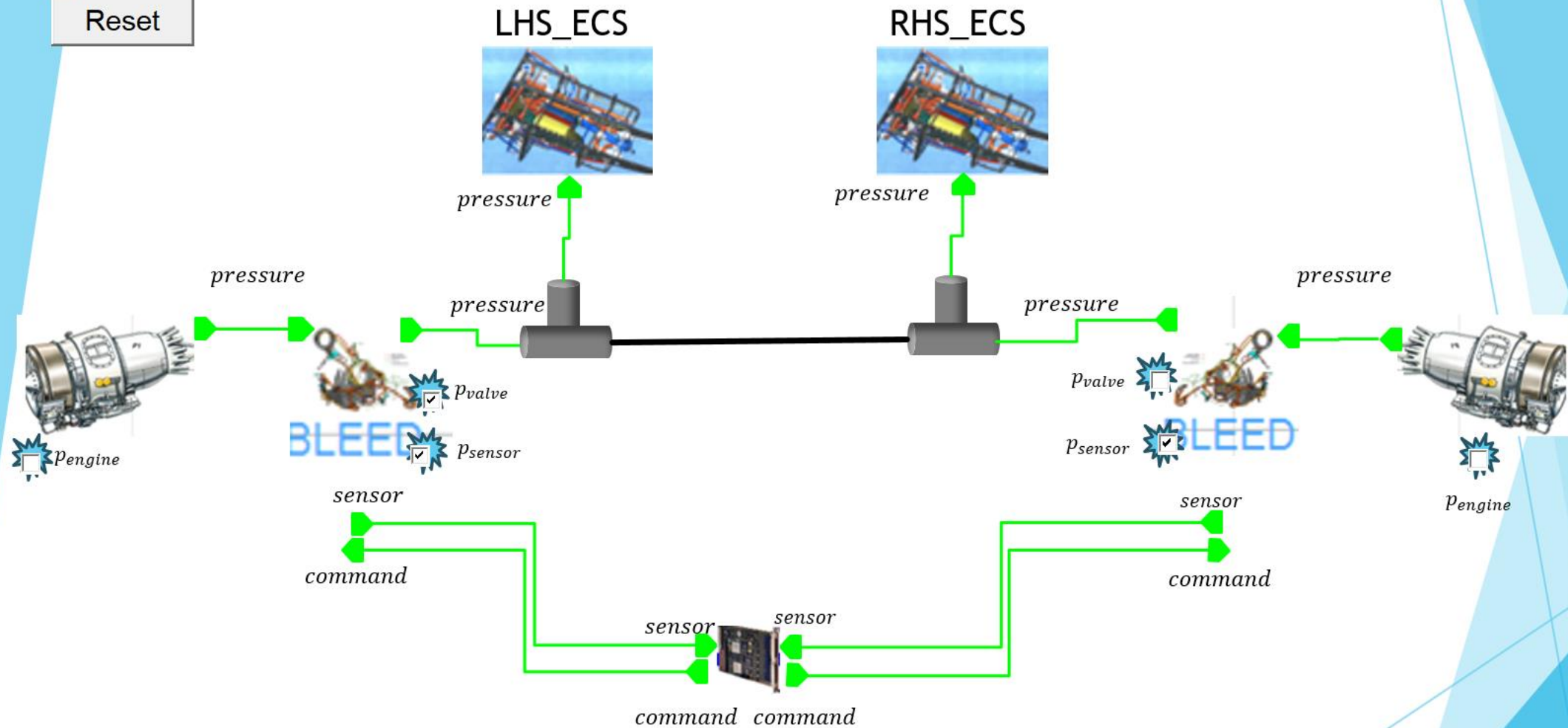


pengine

Simulation

1 - il n'y a aucune panne

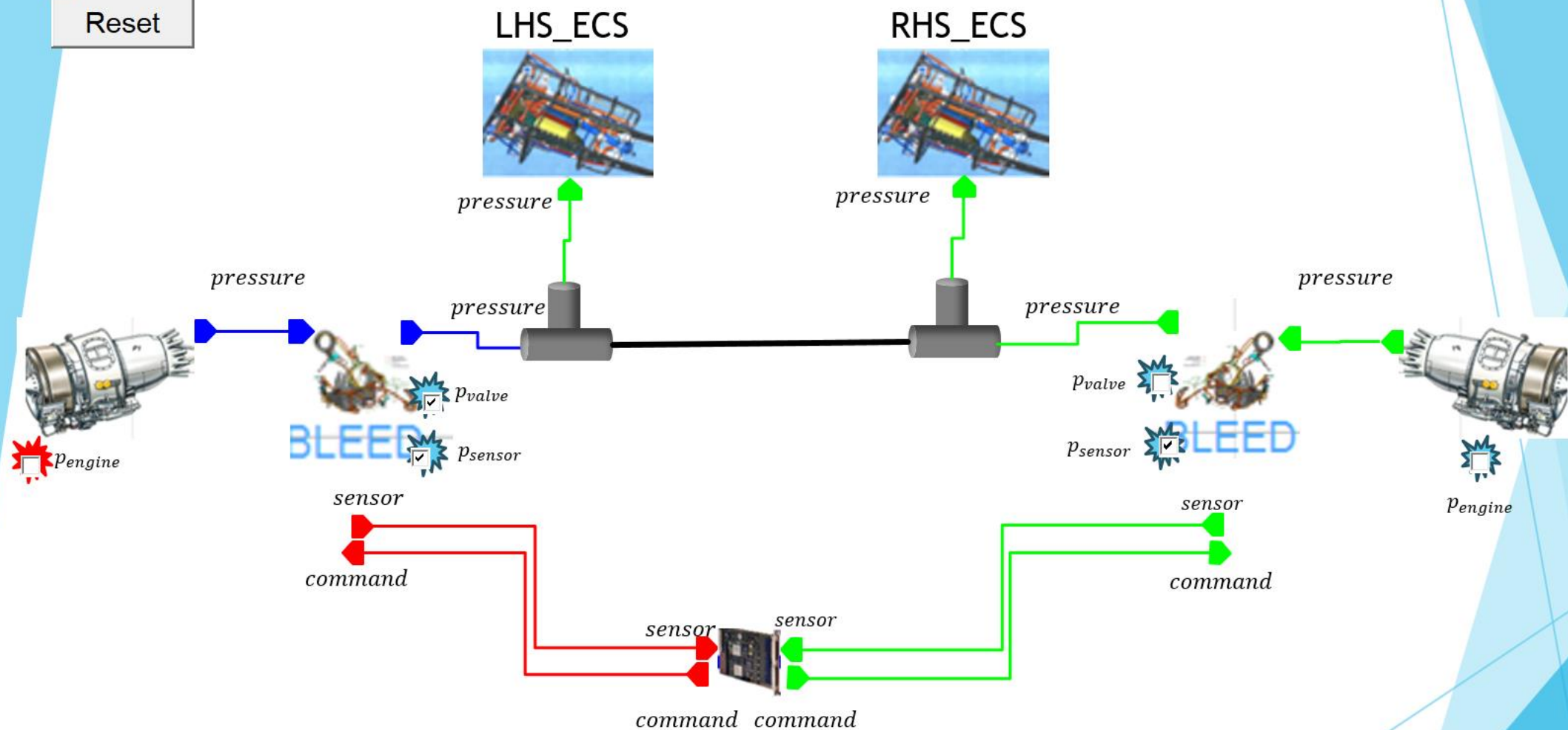
Reset



Simulation

Reset

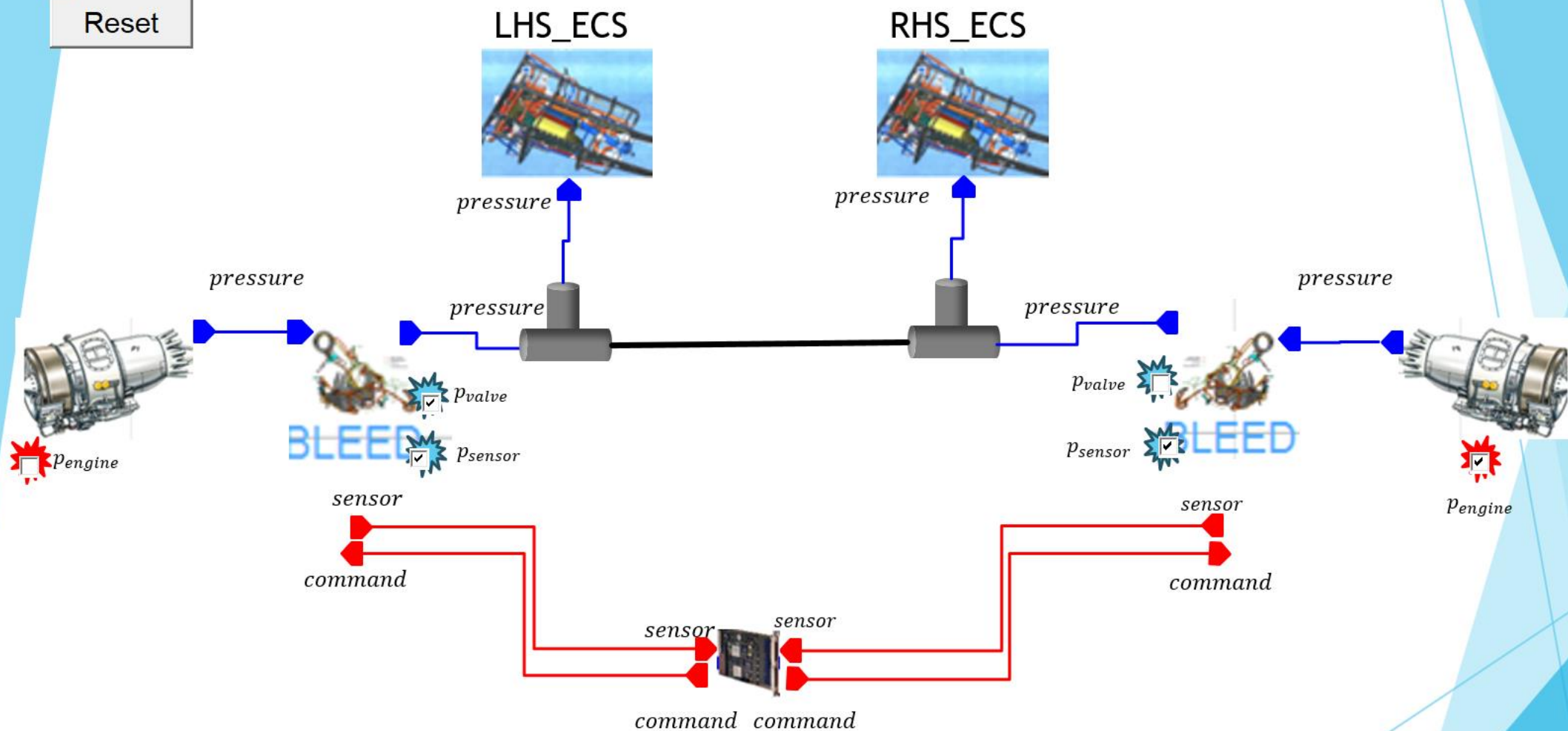
2 - panne du moteur gauche : la pression est correcte en entrée des ECS droite et gauche



Simulation

Reset

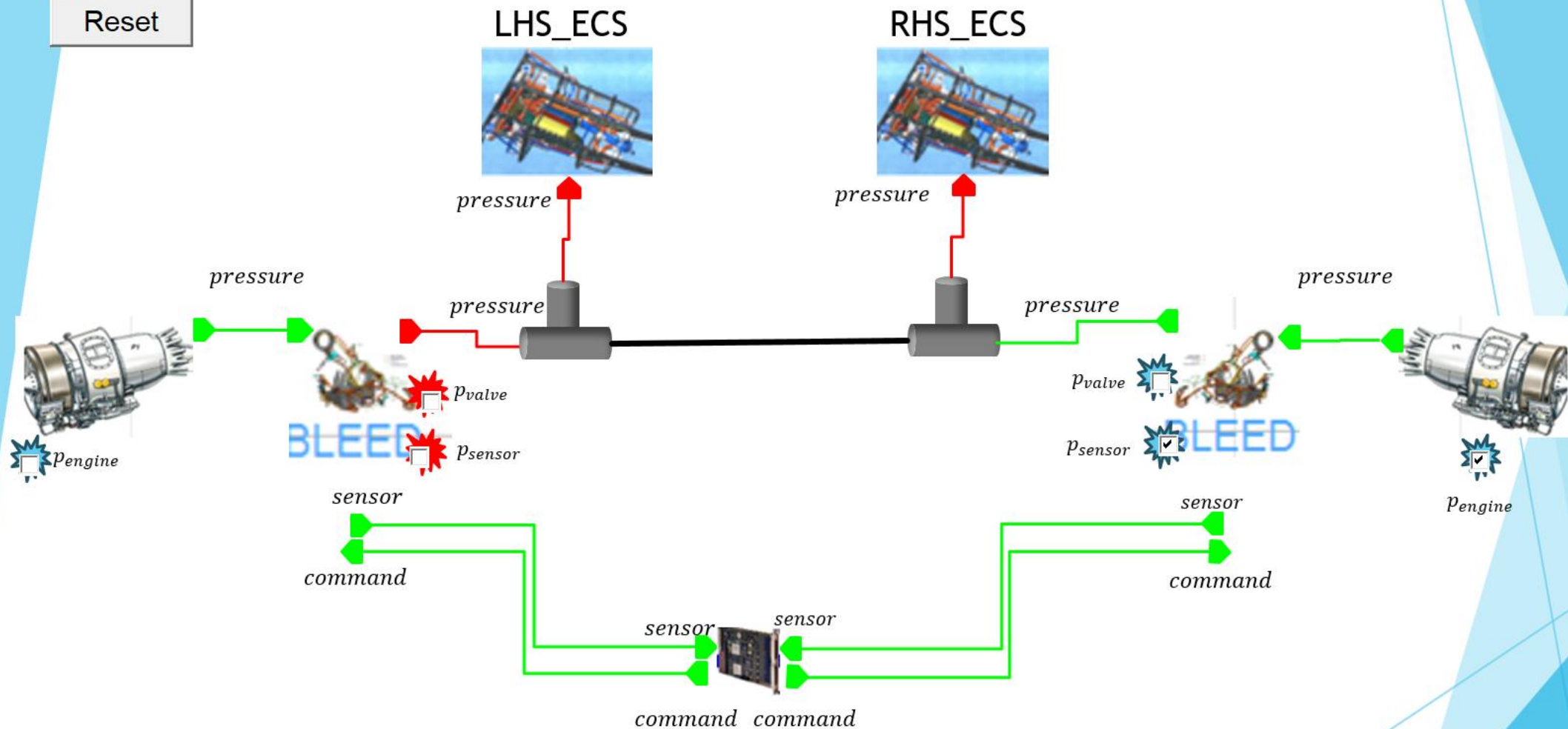
3 - panne des moteurs gauche et droite : pas de pression en entrée des ECS droite et gauche



Simulation

Reset

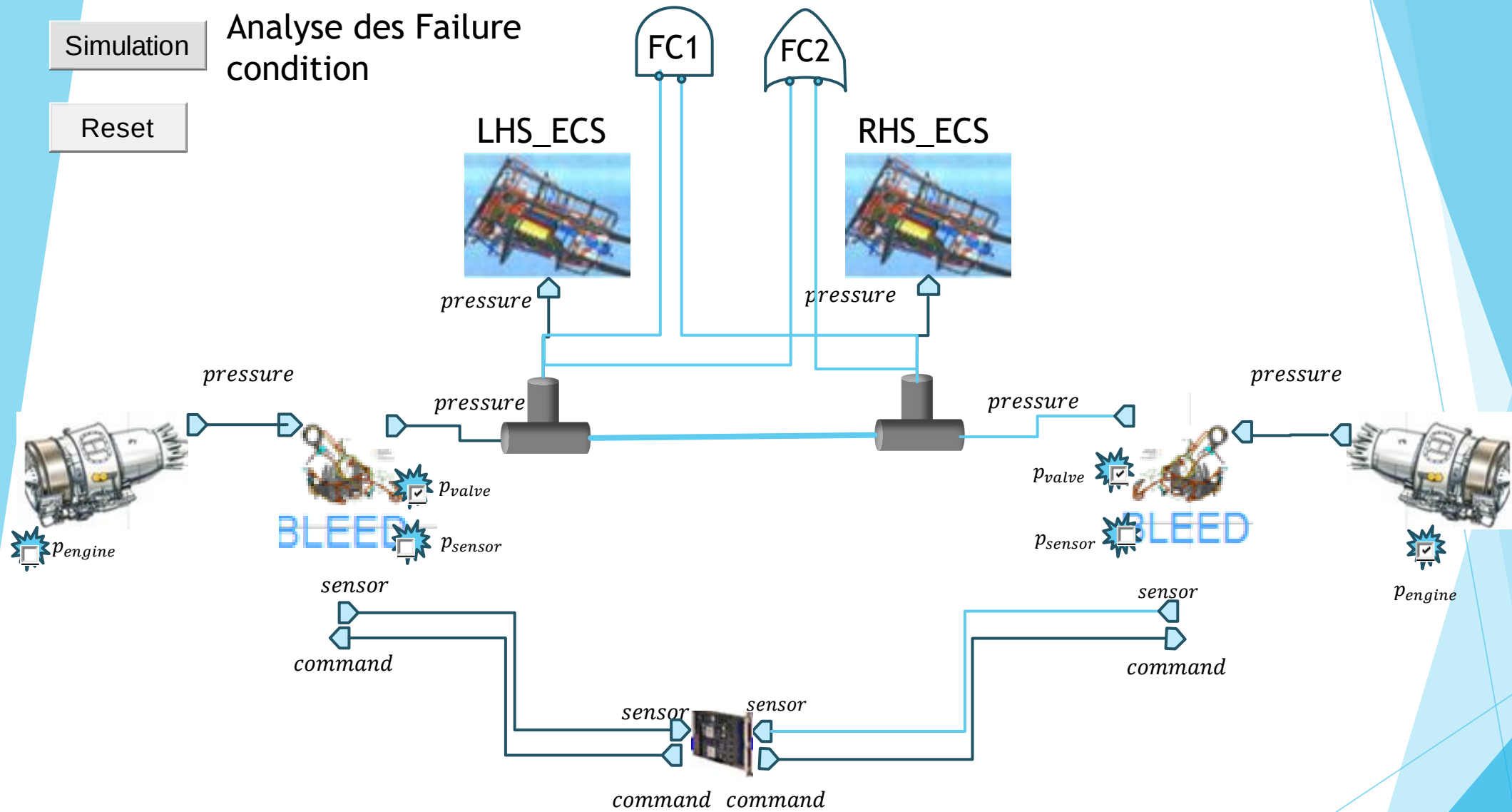
4 - panne du capteur et de la vanne du BLEED droit: surpression en entrée des ECS droite et gauche



Simulation

Analyse des Failure
condition

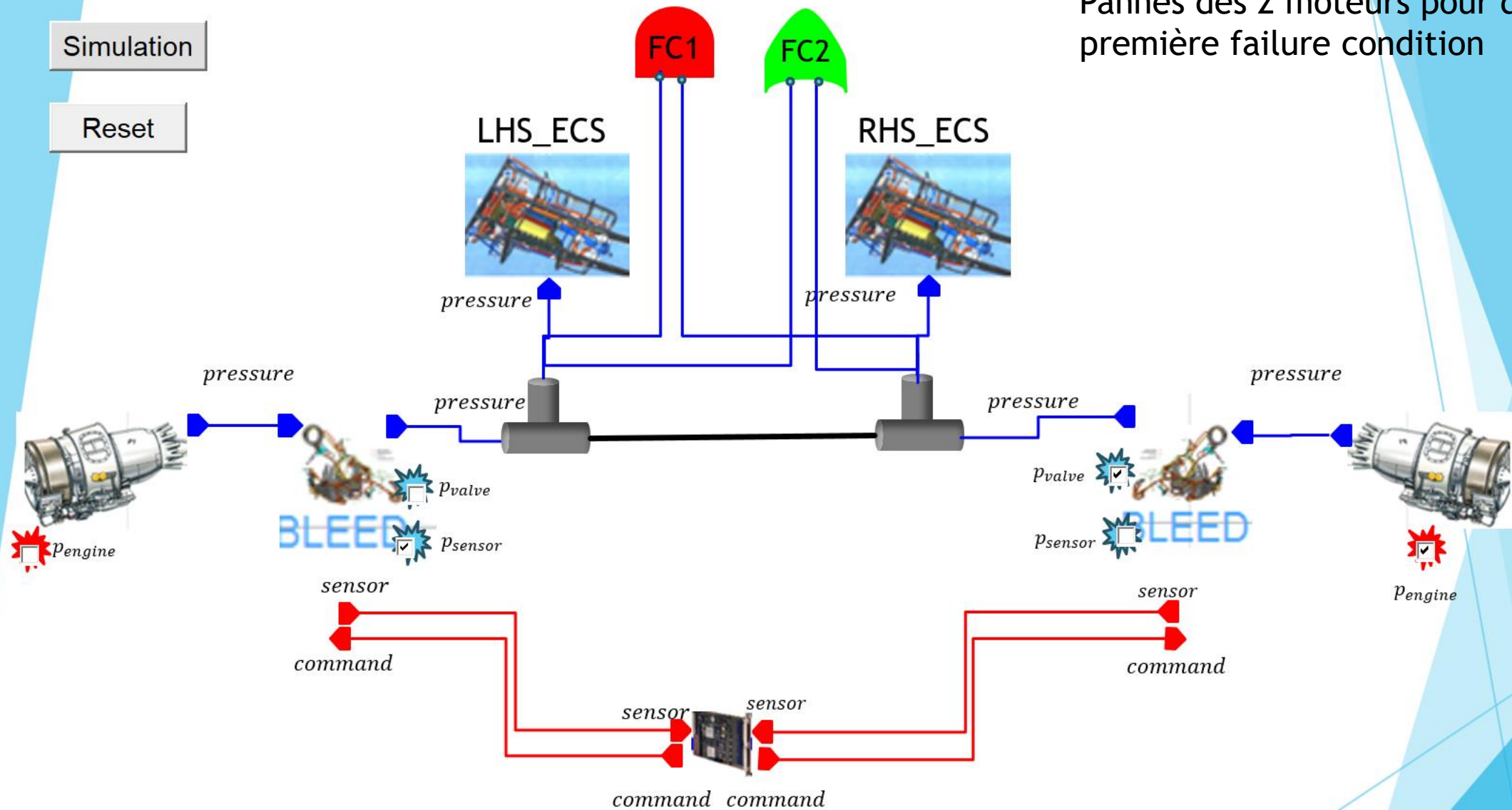
Reset



Simulation

Reset

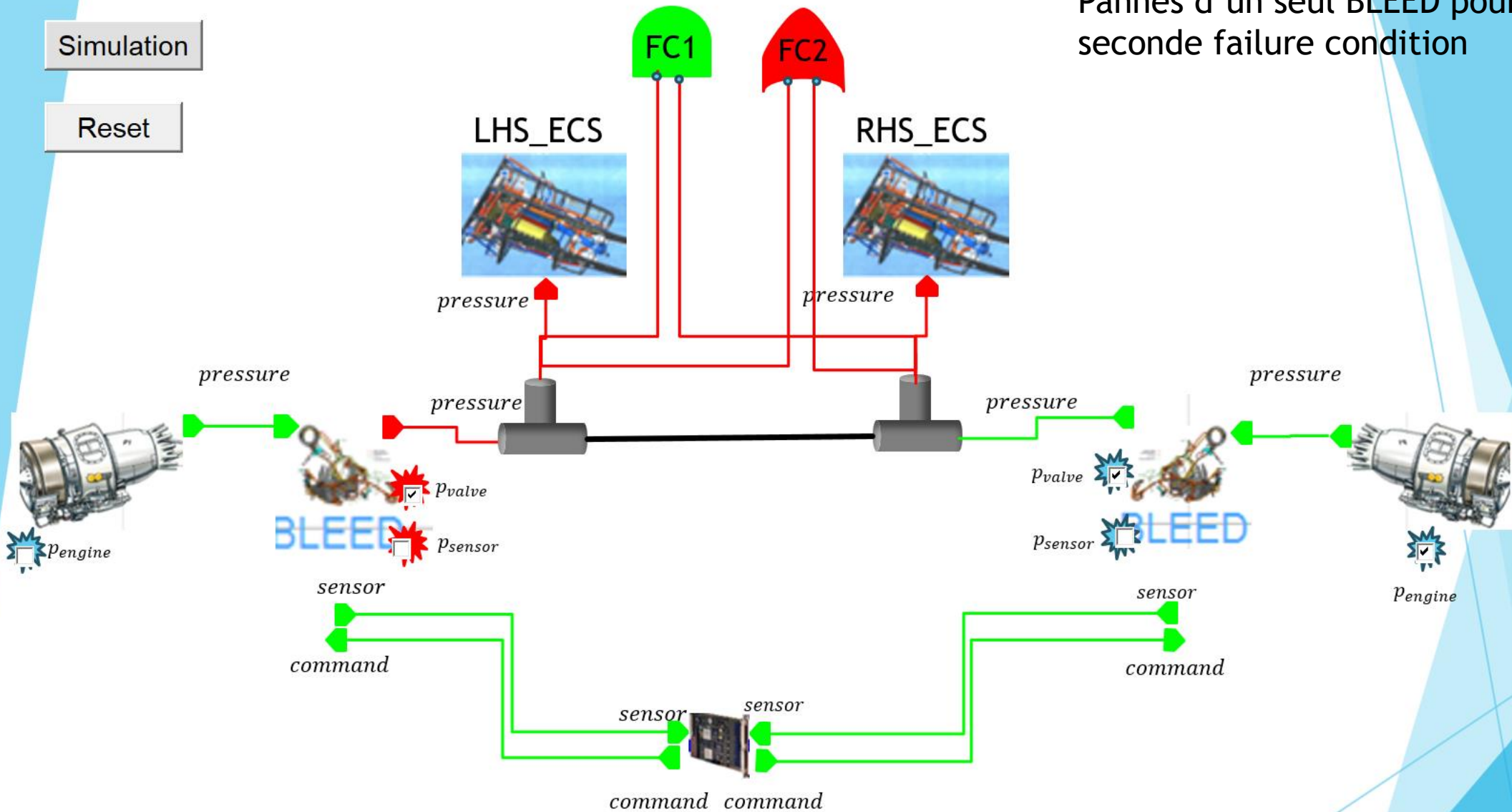
Pannes des 2 moteurs pour déclencher la première failure condition



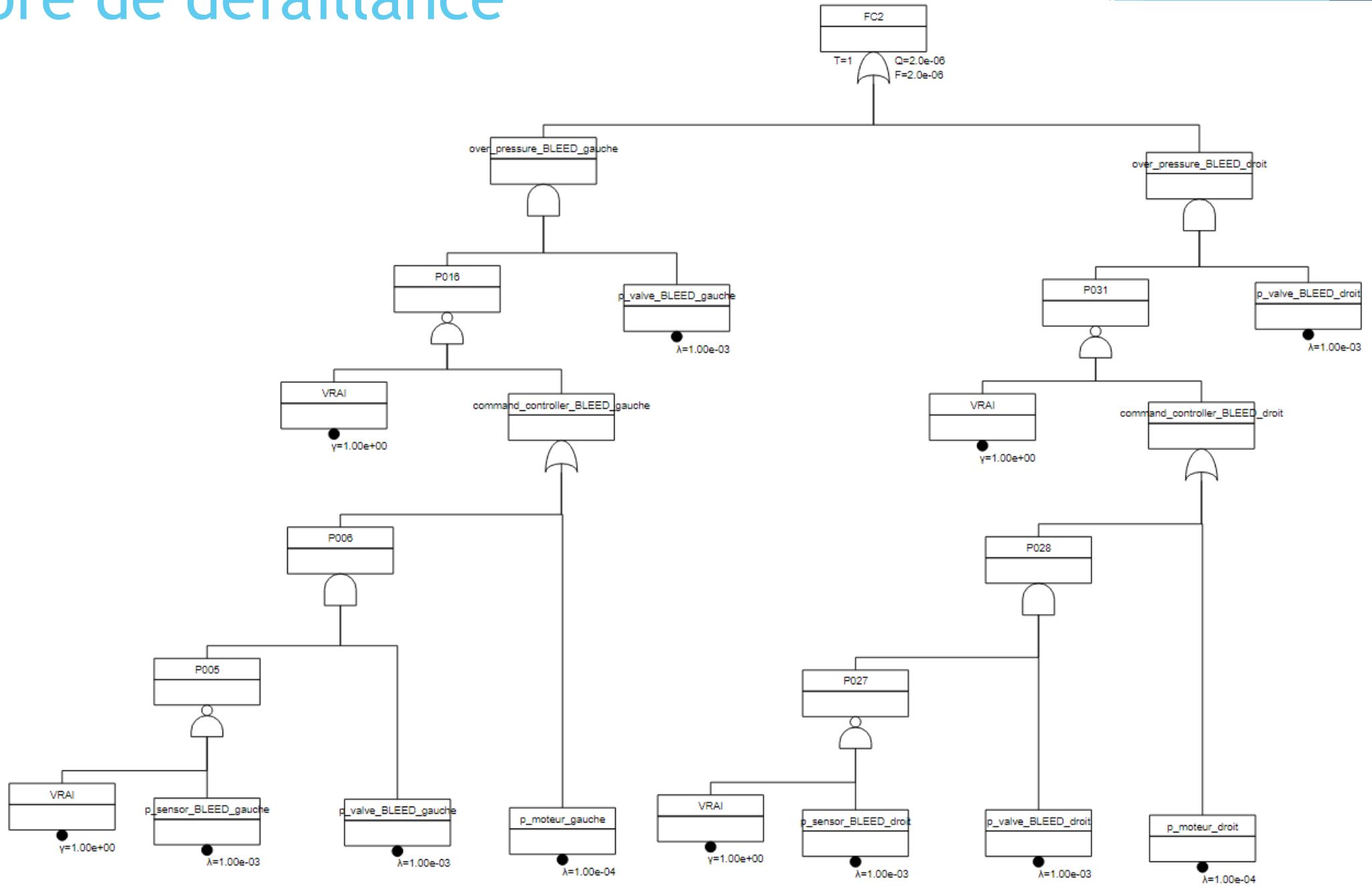
Simulation

Reset

Pannes d'un seul BLEED pour déclencher la seconde failure condition



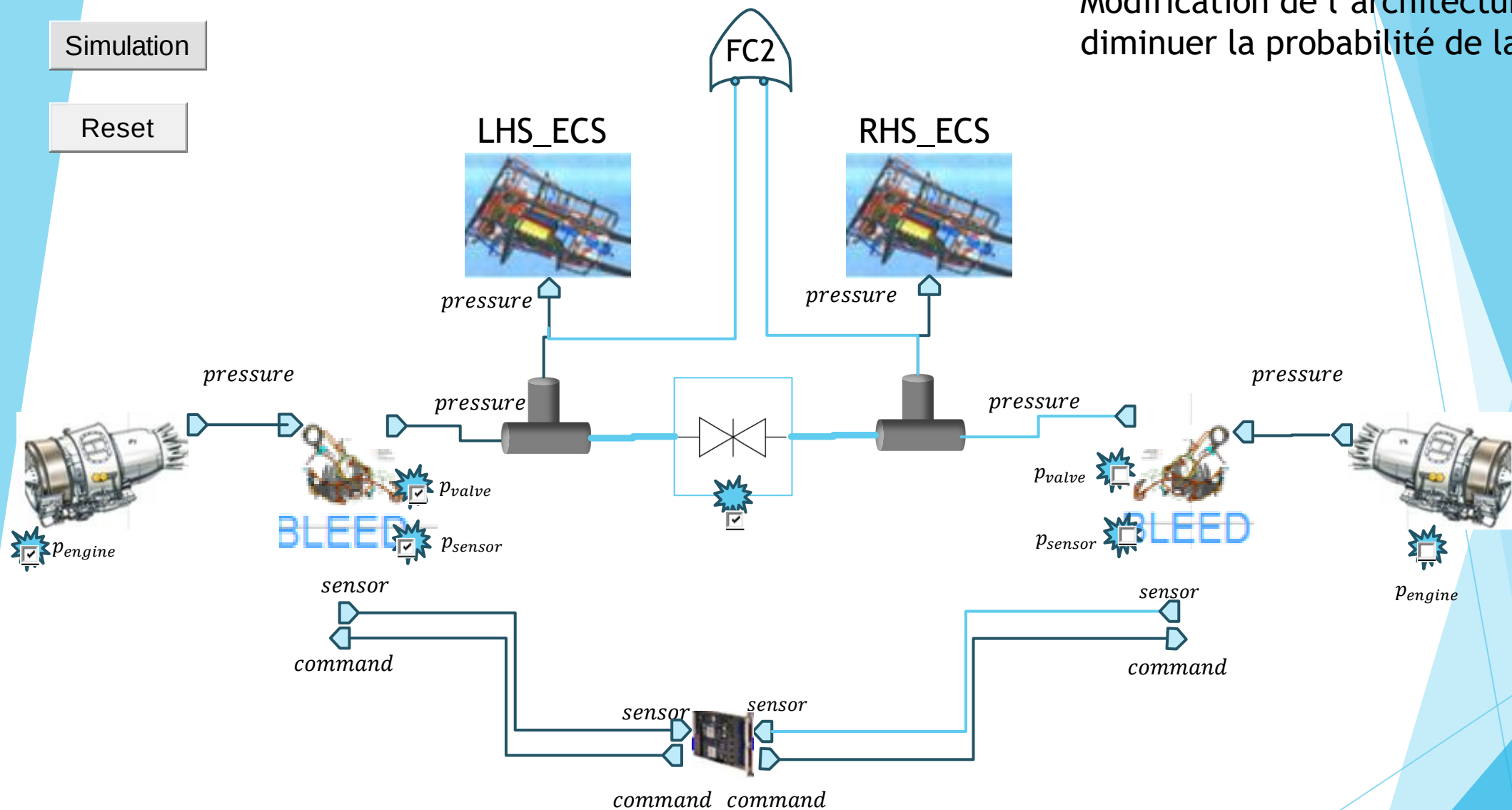
Arbre de défaillance



Simulation

Reset

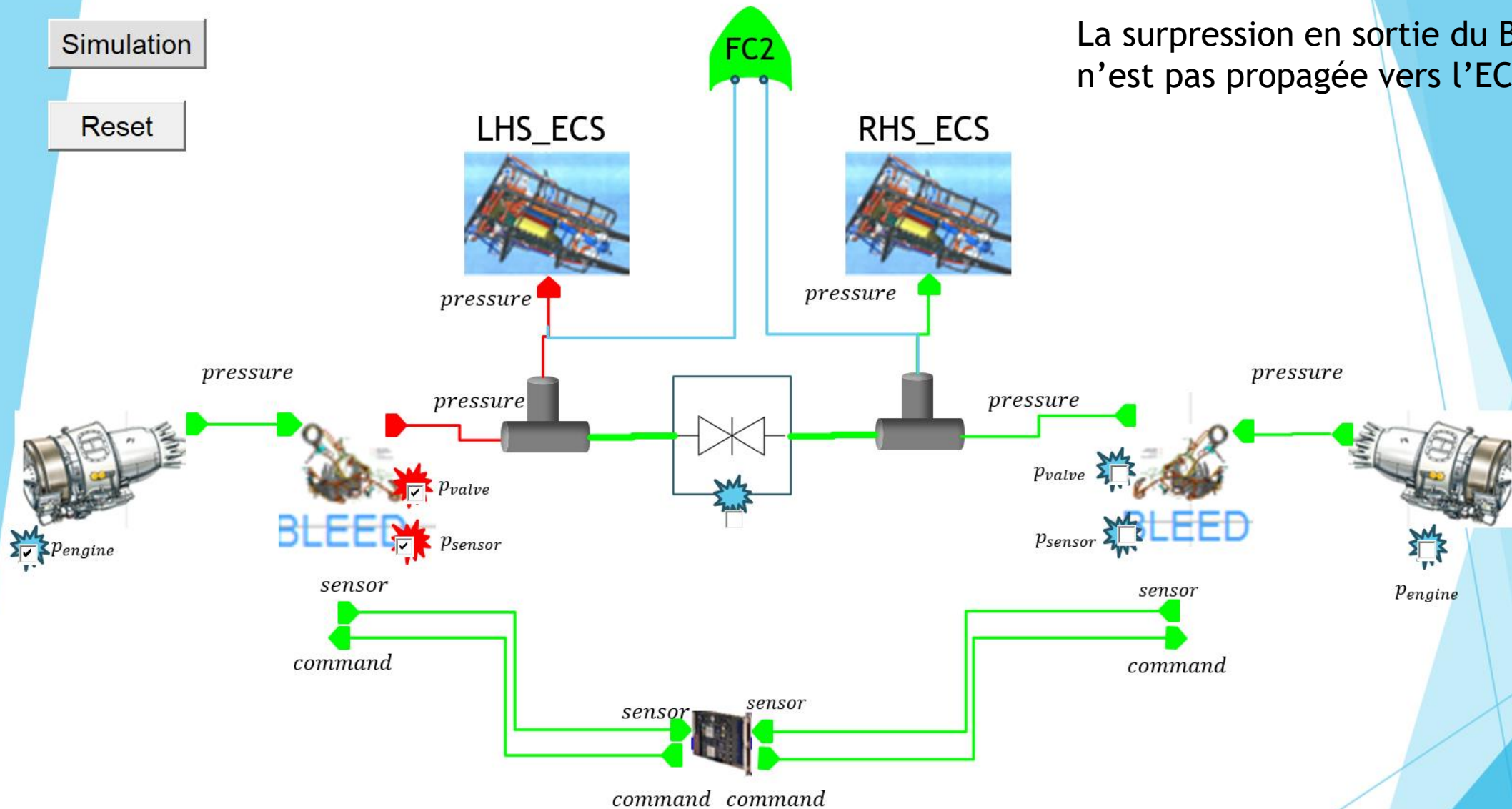
Modification de l'architecture pour
diminuer la probabilité de la FC2



Simulation

Reset

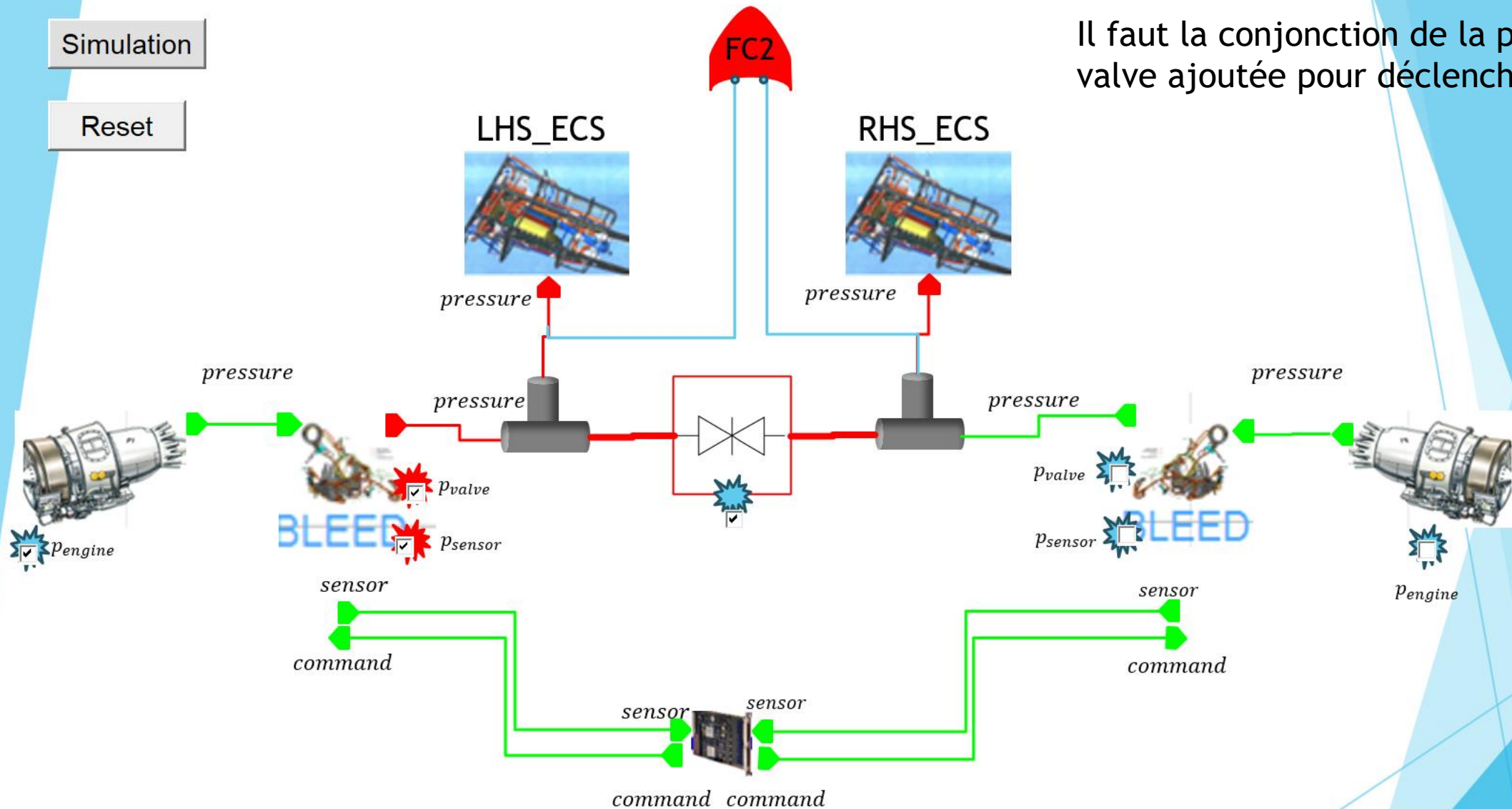
La suppression en sortie du BLEED gauche n'est pas propagée vers l'ECS droit



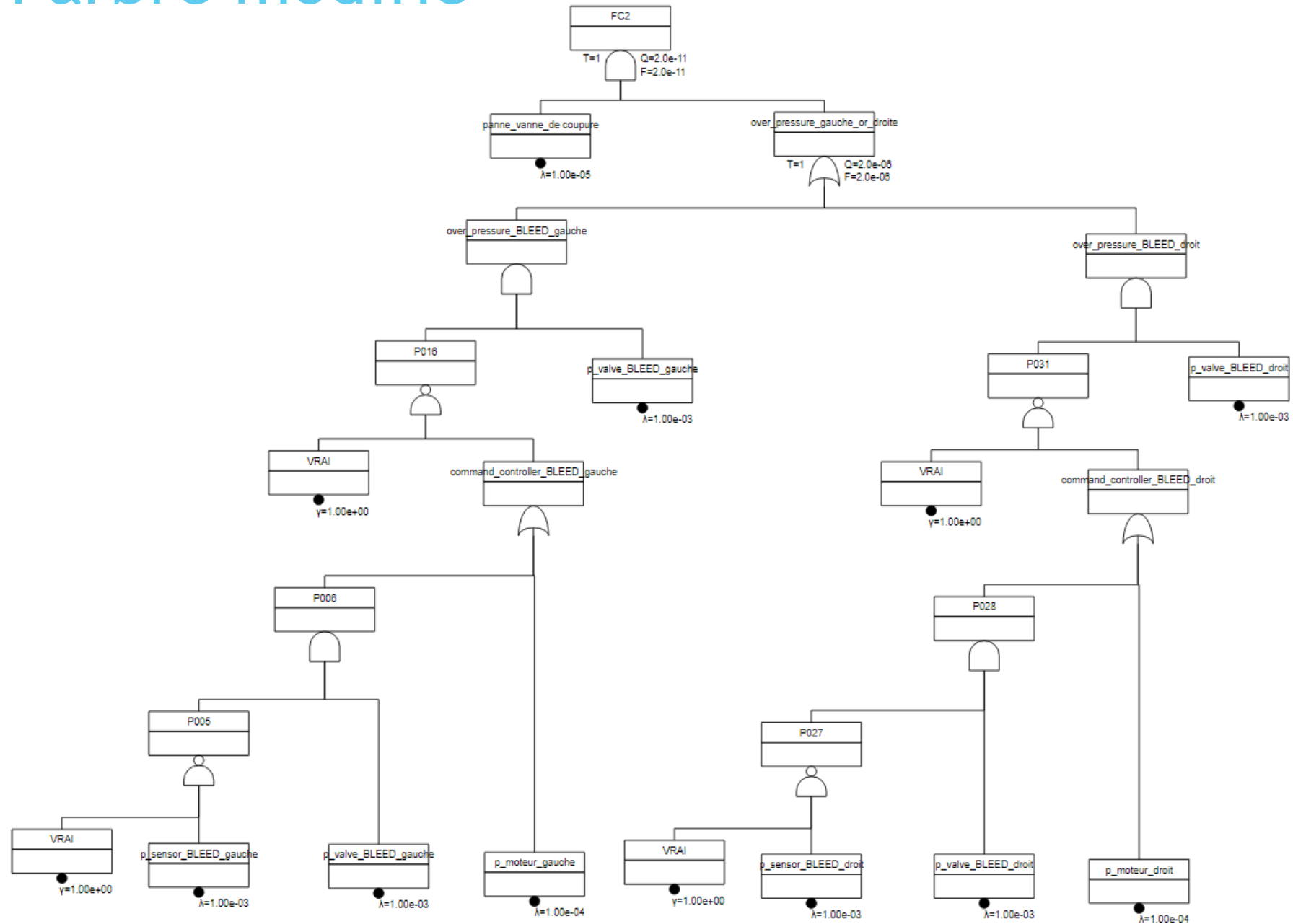
Simulation

Reset

Il faut la conjonction de la panne de la valve ajoutée pour déclencher la FC2



Génération arbre modifié



Comparatif avec les méthodes standards

▶ Analyse Standard des arbres de défaillance (CAFTA)

- ▶ Validation par la revue des arbres de défaillance
- ▶ Un arbre par condition de défaillance analysée
- ▶ En cas de changement d'architecture, toutes les conditions de défaillance peuvent être impactées
- ▶ Taille des arbres grandit avec la complexité du système
- ▶ Difficulté de relecture induite par la taille des arbres
- ▶ Outils bien connus et acceptés pour la certification

▶ Modélisation par outils

- ▶ Validation par la revue de la modélisation des dysfonctionnements des équipements : plus facile pour les concepteurs
- ▶ En cas de changement d'architecture, la modification se fait uniquement au niveau de l'architecture
- ▶ Pour fonctionner, le modèle doit être cohérent => permet d'éviter les erreurs mais peut être bloquant (par exemple, le comportement des systèmes externes)
- ▶ La modélisation des conditions de défaillance est ajoutée séparément
- ▶ Les modèles d'équipements sont totalement indépendants des conditions de défaillance analysées
- ▶ Le pire cas est pris en charge

Lien entre le modèle de safety et d'autres modèles

- ▶ Même architecture:
 - ▶ Mêmes composants (comportements différents)
 - ▶ Mêmes connexions (interfaces polymorphes)
- ▶ Les choix d'architecture sont guidés par la performance et la conformité aux exigences de sécurité
 - ▶ Garantir un rayon d'action implique des contraintes de sécurité sur les réservoirs
 - ▶ Implémenter des redondances impacte le poids donc la performance

=> Les impacts des choix de conception doivent être analysés conjointement sous l'angle de vue performance et sous l'angle de vue sécurité.

Conclusion et perspectives

- ▶ Gain de temps potentiel pour l'évaluation de la sécurité lors des phases préliminaires de conception d'architecture
 - ▶ Flexibilité
 - ▶ Robustesse
 - ▶ réduction de l'effort pour prendre en compte les impacts de sécurité liés aux changements d'architecture
- ▶ Meilleure identification des interdépendances des sous-systèmes
- ▶ Les autorités de certifications (FAA et EASA) commencent à intégrer les modèles formels simulables dans les justifications du respect des objectifs de sécurité