Système de train d'atterrissage

I. Introduction

Ce document présente un système de train d'atterrissage. Il décrit le système et fournit certaines de ses exigences. Nous proposons cette étude de cas comme référence pour les techniques et outils dédiés à la vérification des propriétés comportementales des systèmes. Le système d'atterrissage est en charge de la manœuvre des trains d'atterrissage et des portes associées. Le système d'atterrissage prend en charge 3 roues : avant, gauche et droite. Chaque sous-système contient une porte, un train d'atterrissage et les cylindres hydrauliques associés. Un schéma simplifié du sous-système d'atterrissage est présenté à la figure 1.

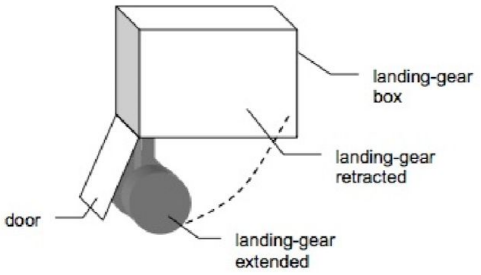


Fig. 1. Landing set

Le système est contrôlé numériquement en mode nominal et en analogique en mode d'urgence. Dans cette étude de cas, nous ne considérons pas le mode d'urgence. Cependant, afin de permettre au pilote d'activer la commande d'urgence, le système doit définir des paramètres de sûreté pour tous les équipements impliqués dans la fonction de train d'atterrissage. Cette partie sur la surveillance de la sûreté entre dans le cadre de l'étude de cas. En mode nominal, la séquence d'atterrissage est la suivante : ouvrir les portes des logements de train d'atterrissage, sortir les trains d'atterrissage et fermer les portes. Cette séquence est illustrée à la figure 2.

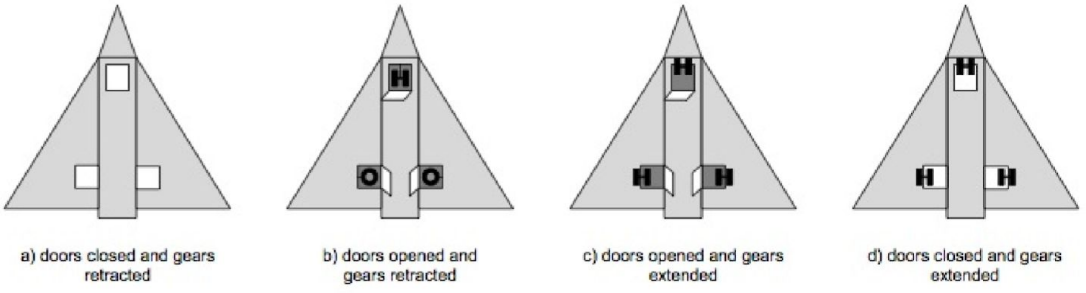


Fig. 2. The landing sequence

Une fois le décollage effectué, la séquence de rétraction à effectuer est la suivante : ouvrir les portes, rétracter les trains d'atterrissage et fermer les portes. Ce système est représentatif des systèmes embarqués critiques. L'action à effectuer à chaque instant dépend de l'état de tous les dispositifs physiques et de leur comportement temporel. Lors de l'examen de tels systèmes, le défi consiste tout d'abord à modéliser et à programmer la partie logicielle contrôlant la séquence d'atterrissage et de rentrée, puis à prouver les exigences de sécurité en tenant compte du comportement physique des dispositifs hydrauliques.

Le document est organisé comme suit :
- la section 2 décrit l'architecture du système;
- la section 3 décrit le comportement de l'équipement hydraulique;
- la section 4 spécifie le comportement attendu du système, c'est-à-dire le comportement à mettre en œuvre par le logiciel de contrôle;
- La section 5 présente les exigences du système, à savoir l'ensemble des propriétés à satisfaire par les unités de calcul du système.

II. Architecture du système

Comme le montre la figure 3, le système de train d'atterrissage est composé de trois parties :
- une partie mécanique contenant tous les dispositifs mécaniques et les trois ensembles d'atterrissage,
- une partie numérique incluant le logiciel de contrôle,
- et une interface pilote.

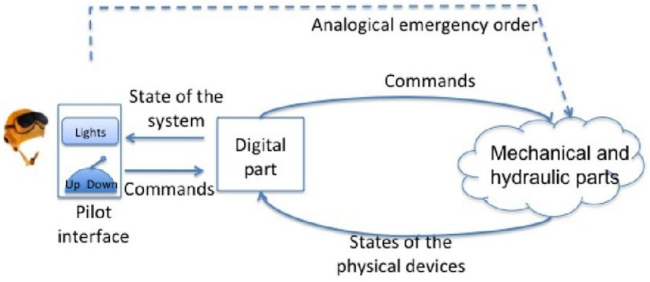


Fig. 3. Global architecture

2.1 L'interface pilote

Pour commander la rentrée et la sortie des roues, un levier haut / bas est fourni au pilote. Lorsque le levier commute sur «Up», la séquence de rentrée du train d'atterrissage est exécutée. Lorsque le levier est déplacé sur «Down», la séquence de sortie du train d'atterrissage est exécutée. Le pilote dispose d'un jeu de voyants indiquant la position actuelle des roues et des portes, ainsi que l'état de santé actuel du système et de ses équipements. Ces lumières sont :
- un feu vert : "les roues sont verrouillés en position sortie",
- un feu orange : "manœuvres",
- un feu rouge : "défaillance du système d'atterrisseur",

Aucune lumière n'est allumée lorsque les roues sont verrouillées en position rétractée. En cas de panne, le pilote peut activer manuellement le circuit hydraulique de secours. La conséquence attendue de cette action est de verrouiller les roues en position basse. En cas de succès et si les capteurs correspondants fonctionnent toujours, le voyant vert «Les roues sont verrouillées» doit être allumé.

2.2 Les parties mécaniques et hydrauliques

L'architecture de la partie hydraulique est décrite à la figure 4. Comme indiqué précédemment, le système est composé de trois sous-systèmes d'atterrissage : les sous-systèmes avant, gauche et droit. Chaque ensemble a :
- un logement supérieur du train d'atterrissage,
- et une porte avec deux mécanismes de verrouillage en position fermée.

Le mouvement des trains d'atterrissage et des portes est assuré par un ensemble de vérins. La position du cylindre correspond à la position de la porte ou du train d'atterrissage (lorsqu'une porte est ouverte, le cylindre correspondant est sorti). Le système d'atterrissage comporte les vérins suivants :
- Pour chaque porte, un cylindre ouvre et ferme la porte.
- Pour chaque train d'atterrissage, un cylindre rentre ou sort le train d'atterrissage.

L'énergie hydraulique est fournie aux cylindres par un ensemble d'électrovannes :
- Une électrovanne générale qui alimente les électrovannes spécifiques en énergie hydraulique à partir du circuit hydraulique de l'aéronef.
- Une électrovanne qui établit la pression sur la partie du circuit hydraulique liée à l'ouverture de la porte.

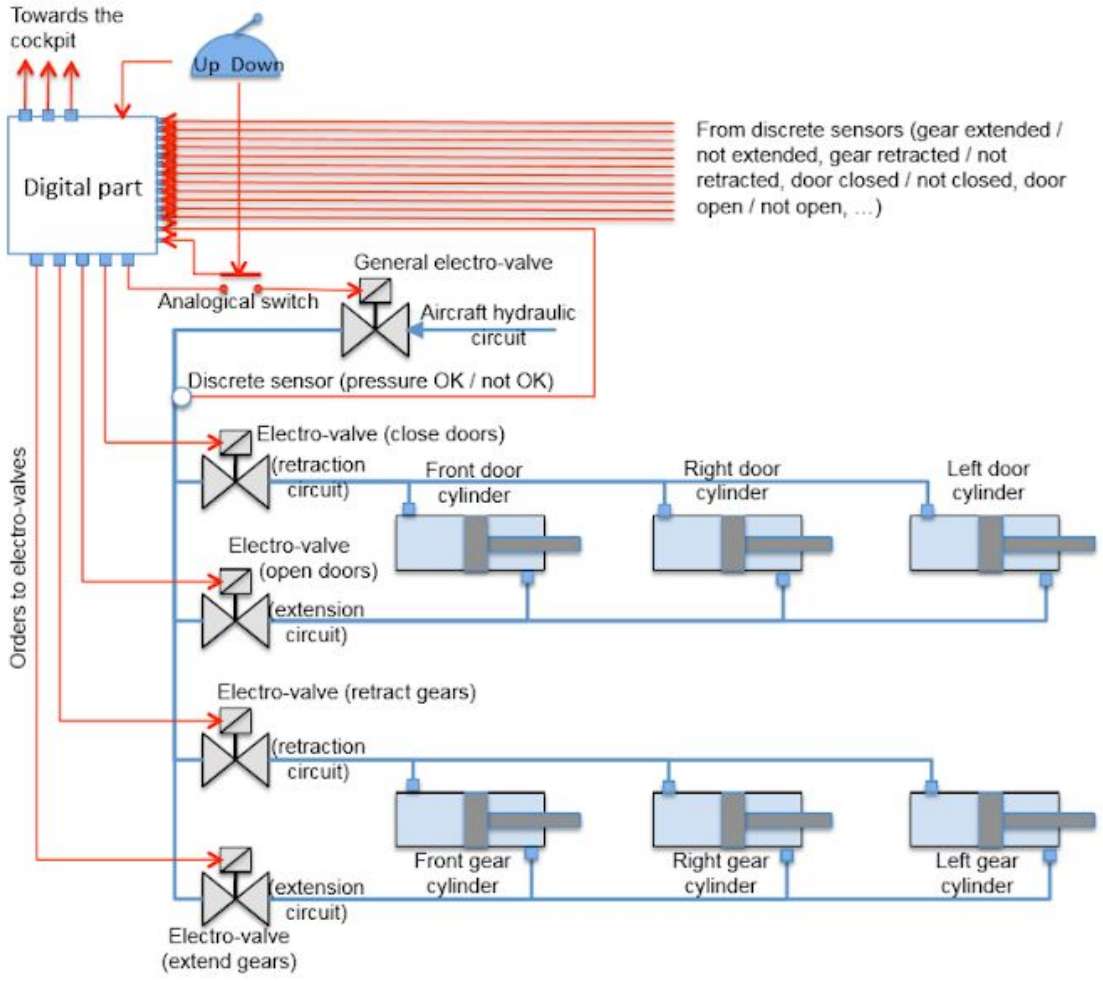


Fig. 4. Architecture of the hydraulic part

- Une électrovanne qui établit la pression sur la partie du circuit hydraulique liée à la fermeture de la porte.
- Une électrovanne qui établit la pression sur la partie du circuit hydraulique liée à la sortie du train d'atterrissage.
- Une électrovanne qui règle la partie du circuit hydraulique liée à la rentrée du train d'atterrissage.
Chaque électrovanne est activée par une commande électrique provenant de la partie numérique. Dans le cas particulier de l'électrovanne générale, cette commande passe par un commutateur analogique afin d'empêcher un comportement anormal de la partie numérique (par exemple, une activation anormale de l'électrovanne générale). Notez que les trois portes (resp. roues) sont contrôlées simultanément par la même électrovanne. En d'autres termes, il n'est pas possible de contrôler les portes (resp. Roues) séparément. Un ensemble de capteurs discrets informe la partie numérique sur l'état des équipements :

- La roue avant / droite / gauche est verrouillée / non verrouillée en position sortie.
- La roue avant / droite / gauche est verrouillée / non verrouillée en position rentrée.
- L'amortisseur de train avant / droit / gauche est au sol / en vol.
- La porte avant / droite / gauche est en position ouverte / non ouverte.
- La porte avant / droite / gauche est verrouillée / non verrouillée en position fermée.
- Le circuit hydraulique (après l'électrovanne générale) est pressurisé / non pressurisé.
- L'interrupteur analogique entre la partie numérique et l'électrovanne générale est fermé / ouvert.

Afin de prévenir les défaillances des capteurs, chaque capteur est triplé (c'est-à-dire que chaque capteur est divisé en trois micro-capteurs indépendants). Il délivre simultanément trois valeurs discrètes décrivant la même situation (par exemple «le pignon gauche est bloqué en position rétractée»). Le comportement de l'équipement physique impliqué dans l'architecture hydraulique est décrit à la section 3.

2.3 La partie numérique

La partie numérique est composée de deux modules de calcul identiques (voir figure 5). Chacun exécute en parallèle le même logiciel de contrôle. Ce logiciel est chargé de contrôler les roues et les portes, de détecter les anomalies et d'informer le pilote de l'état global du système et des anomalies (le cas échéant). Il fait partie d'une boucle de rétroaction avec le système physique et produit des commandes pour les éléments de distribution du système hydraulique en ce qui concerne les valeurs des capteurs et les ordres du pilote. Les deux modules informatiques reçoivent les mêmes entrées. Ces entrées sont (rappelez-vous que toutes les entrées sont triplées) :

- levier $handle_i \in$ {up, down} i = 1,2,3: $handle_i$ caractérise la position du levier. Si le levier est UP (resp. DOWN), alors $handle_i$ = up (resp. $handle_i$ = down).
- commutateur analogique $analogical\_switch_i \in$ {open, closed} i = 1,2,3: $analogical\_switch_i$ caractérise la position du commutateur analogique : ouvert ou fermé. Voir section 3.1.
- piston sorti $gear\_extended_i$ [x] ∈ {true, false} i = 1,2,3 et x ∈ {avant, droite, gauche}
- piston rétracté $gear\_retracted_i$ [x] ∈ {true, false} i = 1,2,3 et x ∈ {avant, droite, gauche}: $gear\_extended_i$ [x] est à true si le piston correspondant est verrouillé en position sortie et false dans les autres cas. $gear\_retracted_i$ [x] est true si le rapport correspondant est verrouillé en position rétractée et false dans les autres cas. Voir la section 3.3 et la figure 11.
- amortisseur de roue $gear\_shock\_absorber_i$ [x] ∈ {sol, vol} i = 1,2,3 et x ∈ {avant, droite, gauche} $gear\_shock\_absorber_i$ [x] est renvoyé par un capteur implanté directement sur l'engin correspondant (voir Figure 11). C'est vrai si et seulement si l'aéronef est au sol.

- porte fermée *door_closed*$_i$ [x] ∈ {true, false} i = 1,2,3 et x ∈ {avant, droite, gauche}
- porte ouverte *door_open*$_i$ [x] ∈ {true, false} i = 1,2,3 et x ∈ {avant, droite, gauche}:
door_closed$_i$ [x] est à true si et seulement si la porte correspondante est verrouillée fermée. *door_open*$_i$ [x] est à true si et seulement si la porte correspondante est verrouillée ouverte. Voir la section 3.3 et la figure 12.
- circuit pressurisé *circuit_pressurized*$_i$ ∈ {true, false} i = 1,2,3. *circuit_pressurized*$_i$ est renvoyé par un capteur de pression situé sur le circuit hydraulique entre l'électrovanne générale et l'électrovanne de manœuvre (voir Figure 4). *circuit_pressurized*$_i$ est à true si et seulement si la pression est élevée dans cette partie du circuit hydraulique.

La quantité totale de valeurs discrètes d'entrée reçues par chaque module de calcul est de 54 (3 *handle*, 3 *analogical_switch*, 9 *gear_extended*, 9 *gear_retracted*, 9 *gear_shock_absorber*, 9 *door_closed*, 9 *door_open*$_i$ et 3 *circuit_pressurized*).
A partir de ces entrées, chaque module calcule 5 ordres électriques pour les électrovannes :
- général *general_EV*$_k$ ∈ {true, false} k = 1,2
- fermer *close_EV*$_k$ ∈ {true, false} k = 1,2
- ouvrir *open_EV*$_k$ ∈ {true, false} k = 1,2
- retirer *retract_EV*$_k$ ∈ {true, false} k = 1,2
- étendre *extend_EV*$_k$ ∈ {true, false} k = 1,2

où «EV» signifie «Electro-Valve» et k représente le numéro du module de calcul considéré.

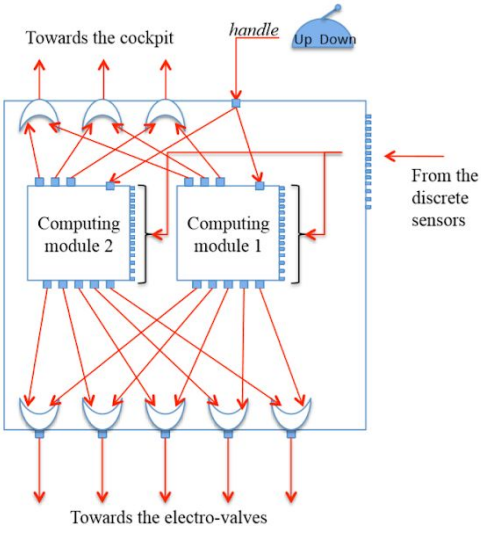


Fig. 5. Digital architecture

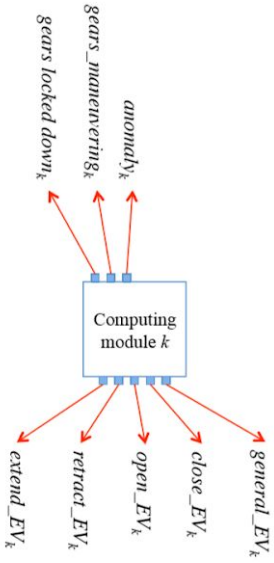


Fig. 6. Electrical outputs of the computing module k $(k = 1, 2)$

Les ordres électriques correspondants provenant des deux modules sont produits physiquement sur la même ligne électrique. La composition implicite de deux sorties est un «OU» électrique, comme illustré à la figure 5.

Considérons par exemple le paramètre *general_EV*. Si les deux modules produisent la même valeur sur *general_EV*$_1$ et sur *general_EV*$_2$, cette valeur est alors transmise à l'électrovanne générale. Sinon, si une seule d'entre elles est vraie (en raison d'une défaillance quelque part dans la partie numérique), la valeur true est alors transmise à l'électrovanne, même si ce n'est pas la valeur correcte. Le problème sera néanmoins détecté au cycle suivant, lorsque le module qui a généré la valeur fausse détectera un comportement inattendu par rapport à ses propres ordres. Ensuite, il informera le pilote d'une anomalie potentielle dans le système.

De même, les deux modules produisent des variables d'état booléennes globales dans le cockpit :
- roues verrouillées en position basse $gears\_locked\_down_k \in$ {true, false} k = 1,2
- roues en cours de manœuvre $gears\_maneuvering_k \in$ {true, false} k = 1,2
- anomalie $anomaly_k \in$ {true, false} k = 1,2

Ces sorties sont synthétisées par chaque module à partir des données des capteurs et de la connaissance de la situation. Comme pour les ordres électriques fournis aux électrovannes, les variables d'état de type booléen des deux modules sont composées à la suite d'une opération logique «OU». Si $gears\_locked\_down_k$ (pour certains k) sont envoyés à l'interface pilote avec la valeur true, le voyant vert «Les trains sont verrouillés» est allumé. Si $gears\_maneuvering_k$ (pour certains k) est envoyée à l'interface pilote avec la valeur true, le voyant orange «Manœuvres» est allumé. Si $anomaly_k$ (pour certains k) est envoyé à l'interface pilote avec la valeur true, le voyant rouge «défaillance du système d'atterrissage» est allumé. La spécification de la partie numérique est décrite à la section 4.
L'interface de sortie de chaque module est synthétisée à la figure 6.

III. Comportement de l'équipement hydraulique

3.1 Le commutateur analogique (entre la partie numérique et l'électrovanne générale)

Le but de ce commutateur est de protéger le système contre le comportement anormal de la partie numérique. Afin d'éviter l'envoi involontaire d'un ordre aux électrovannes, l'électrovanne générale ne peut être stimulée que si cet interrupteur est fermé. L'interrupteur est fermé chaque fois que le pilote actionne le levier «Haut / Bas» et il reste fermé 20 secondes. Après cette durée, le commutateur devient automatiquement ouvert. En position fermée, le commutateur transmet l'ordre électrique de la partie numérique à l'électrovanne générale.
En position ouverte, aucun ordre électrique n'est envoyé à l'électrovanne. Dans ce cas, la pression d'huile dans le circuit hydraulique diminue. Pour des raisons inertielles, la transition entre les deux états `fermé` et `ouvert` prend un certain temps :
- de open à closed : 0,8 seconde,
- de closed à open : 1,2 seconde,

En plus de ce comportement normal, le commutateur analogique peut échouer. Nous ne considérons que les pannes permanentes : l'interrupteur reste bloqué en position fermée ou ouverte. Un échec peut survenir à tout moment. Le comportement global du commutateur, y compris les défaillances, est spécifié par le modèle de la figure 7 et l'automate hybride hiérarchique de la figure 8.

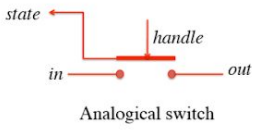


Fig. 7. Interface of the analogical switch

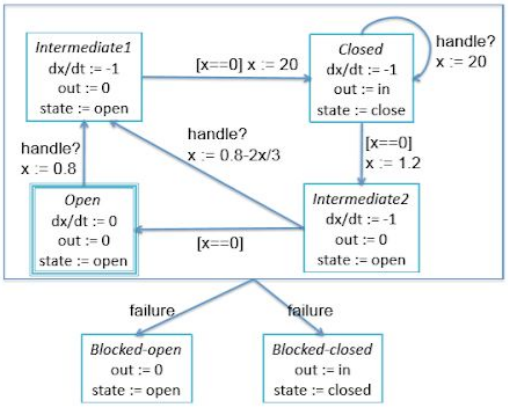


Fig. 8. Physical behavior of the analogical switch

Dans cette spécification, *in* représente la valeur d'entrée du commutateur. Dans l'architecture globale de la figure 4, le port *in* du commutateur analogique est connecté à la sortie *general_EV* de la partie numérique (c'est-à-dire, *in* = *general_EV*). La variable *out* représente la sortie électrique du commutateur. Il est connecté au port électrique de l'électrovanne générale.
La variable *state* est la sortie logique du commutateur. Il appartient à l'ensemble {open, closed}. Il est connecté au port d'entrée *analogical_switch* de la partie numérique. Notez que cette valeur de sortie est triplée, comme expliqué à la section 2.3.
L'événement *handle?* indique la détection d'un mouvement du levier par le pilote. Cet événement est reçu chaque fois que le pilote déplace le levier.
Et finalement *x* est une variable continue interne qui évolue en fonction de l'équation différentielle dans chaque état. Le but de cette variable est de compter le temps dans écoulé dans chaque état. Par exemple, dans l'état *Open*, *x* n'évolue pas, *state* est positionné sur *open* et *out* est positionné sur 0 quelle que soit la valeur de *in*. Lorsque *handle* est reçu, *x* est positionné sur 0.8, l'état *Intermediate1* est atteint et *x* commence à diminuer. Les valeurs d'état et de sortie restent inchangées. 0,8 seconde plus tard, *x*

atteint la valeur nulle. La transition entre *Intermediate1* et *Close* est alors déclenchée et *x* est positionné sur 20. *state* est maintenant positionné sur *closed* et *out* sur *in*. Et ainsi de suite. L'état initial de l'automate est *Open*. Notez que le commutateur est indépendant de la partie numérique.

3.2 Electro-valves

Toutes les électrovannes sont supposées avoir le même comportement. Comme le montre la figure 9, une électrovanne est un équipement hydraulique doté de deux ports hydrauliques *Hin* (port d'entrée hydraulique) et *Hout* (port de sortie hydraulique) et d'un port électrique (E ∈ {true, false}). Son comportement dépend de la valeur de l'ordre électrique connecté à E.

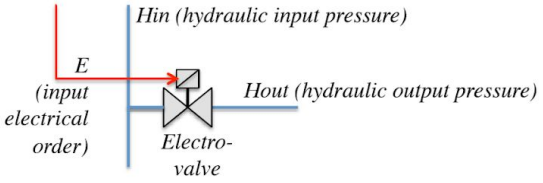


Fig. 9. An electro-valve equipment

- si E = false, alors *Hout* = 0 (pas de pression du côté de la sortie hydraulique, le circuit hydraulique est ouvert);
- si E = true, alors *Hout* = *Hin* (le circuit hydraulique est fermé);

Notez que l'ordre électrique doit être maintenu au niveau true pour maintenir l'électrovanne en position fermée. En d'autres termes, l'ordre électrique n'est pas un événement discret, mais peut être vu comme un signal analogique. Pour des raisons d'inertie, nous supposons que de la position ouverte à la position fermée, la pression augmente de façon continue de 0 à *Hin*. Dans cette étude de cas, nous supposons que la pression augmente de manière linéaire et que la durée totale de la phase de transition est de 1 seconde. De la même façon, la pression diminue continuellement de *Hin* à 0. Nous supposons que la pression diminue linéairement et que la durée totale de la phase de transition est de 3,6 secondes.

En plus de ce comportement normal, toute électrovanne peut échouer. Nous ne considérons que les pannes permanentes : l'électrovanne reste bloquée à l'état fermé ou open. Un échec peut survenir à tout moment.

3.3 Cylindres

Les cylindres sont de purs équipements hydrauliques. Comme le montre la figure 10, ils commencent à se déplacer lorsqu'ils reçoivent de la pression hydraulique et s'arrêtent lorsque la pression baisse ou lorsqu'ils atteignent la fin de leur course.

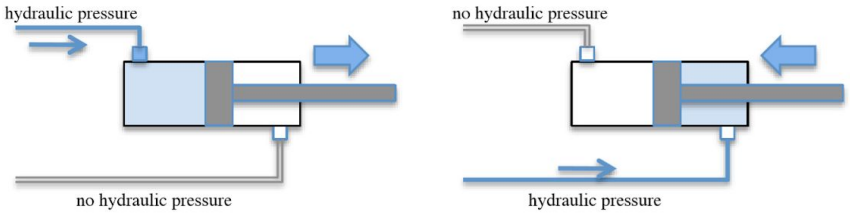


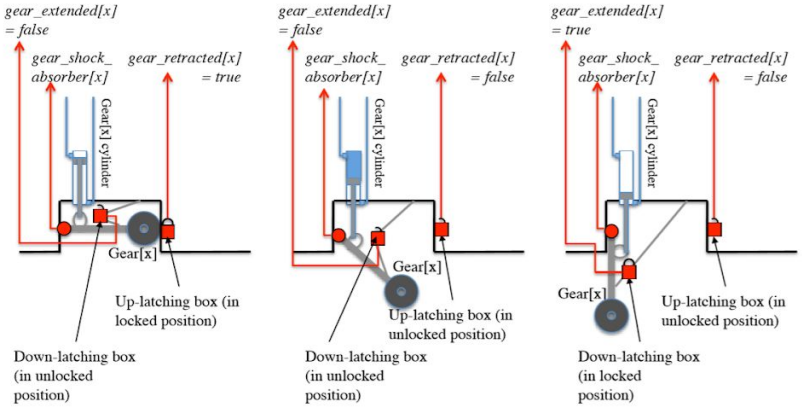
Fig. 10. Extension and retraction of a cylinder

Cylindres des roues. Les cylindres des roues sont verrouillés en position haute (high) ou basse (down) au moyen d'un mécanisme de verrouillage (les dispositifs de verrouillage se trouvent physiquement sur les roues, un pour chaque position). Lorsqu'un cylindre de roue est verrouillé en position haute (resp. basse) et lorsqu'il reçoit une pression du circuit hydraulique par le haut (resp. par le bas),
- en premier il est déverrouillé de la position high (resp. down)
- puis il passe à la position down (resp. high)
- et enfin il est verrouillé en position down (resp. high).

Le comportement de la roue (y compris les valeurs renvoyées par les capteurs de position de la roue) est décrit à la figure 11.

Cylindres des portes. Les cylindres des portes sont verrouillés (au moyen de deux boîtes de verrouillage sur chaque porte) uniquement en position fermée. Les portes sont maintenues ouvertes en maintenant la pression dans le circuit d'extension. Lorsqu'un cylindre de porte est verrouillé en position fermée et qu'il reçoit une pression du circuit hydraulique d'extension,
- il est d'abord déverrouillé à partir de la position fermée
- puis il passe en position ouverte
- et enfin il est maintenu en position ouverte tant que la pression est maintenue dans le circuit d'extension hydraulique.

Le comportement de la porte (y compris les valeurs renvoyées par les capteurs de position de la porte) est décrit à la figure 12.



(a) gear in the retracted position (b) gear in the intermediate position (c) gear in the extended position

Fig. 11. Integration Gear - cylinder for the block $x \in \{front, right, left\}$ (the door is not represented)

Comportement temporel des cylindres. Toutes ces opérations sont effectuées automatiquement avec la pression hydraulique uniquement. Aucune pièce électrique n'est impliquée dans les cylindres. Ces opérations prennent un certain temps en fonction de la position du cylindre dans l'aéronef et dans le circuit hydraulique. Les durées sont données dans le tableau ci-dessous. Les valeurs ne sont que des valeurs moyennes. Les durées réelles peuvent varier autour de ces valeurs jusqu'à 20%.

duration (in seconds) of ...	front gear	front door	right gear	right door	left gear	left door
unlock in down position	0.8	-	0.8	-	0.8	-
from down to high position	1.6	1.2	2	1.6	2	1.6
lock in high position	0.4	0.3	0.4	0.3	0.4	0.3
unlock in high position	0.8	0.4	0.8	0.4	0.8	0.4
from high to down position	1.2	1.2	1.6	1.5	1.6	1.5
lock in down position	0.4	-	0.4	-	0.4	-

Notez qu'il est possible d'arrêter et d'inverser le mouvement de n'importe quel cylindre à tout moment. Un exemple de mouvement avant est présenté à la figure 13.

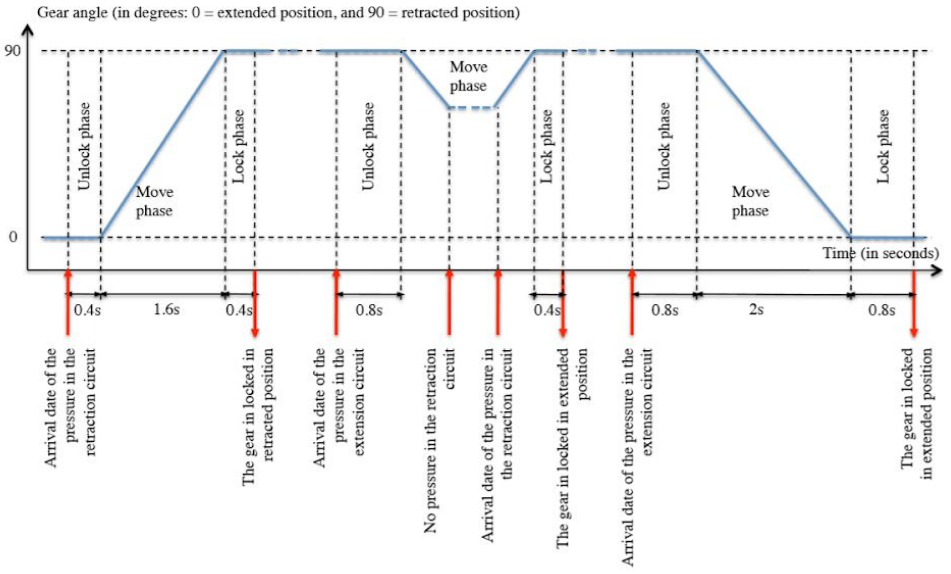


Fig. 13. Example of the front gear angle evolution (angle of the gear w.r.t the vertical: 0 (resp. 90) corresponds to the down (resp. up) position)

Ce scénario est basé sur les valeurs moyennes indiquées dans le tableau précédent.
Supposons que le train avant soit bloqué en position sortie lorsque la pression arrive dans le circuit de rétraction (première flèche rouge à gauche). Ensuite, la roue est déverrouillée 0,4s plus tard. Le train monte pendant les 1,6s. Enfin, il est verrouillé en position rentrée 2,4s après l'arrivée de la pression dans le circuit hydraulique.
Considérons maintenant que la pression arrive dans le circuit d'extension. La roue est déverrouillée 0,8s plus tard. Le train commence à descendre.
Supposons maintenant que la pression est arrêtée. Ensuite, le cylindre s'arrête également dans la position actuelle. Si la pression arrive à nouveau dans le circuit de rétraction, le train remonte immédiatement à partir de la position actuelle jusqu'à sa position rétractée.
De la même manière, la dernière partie du scénario décrit la phase d'extension sans interruption. En plus de ce comportement normal, n'importe quel cylindre peut échouer. Nous ne considérons que les défaillances permanentes : le cylindre reste bloqué dans la dernière position (basse, haute ou entre ces deux positions). Tout échec peut survenir à tout moment.

IV. Spécification du logiciel

La partie logicielle du système a un double objectif :
1. contrôler les dispositifs hydrauliques en fonction des ordres du pilote et des positions des dispositifs mécaniques;
2. surveiller le système et informer le pilote en cas d'anomalie.
Le premier objectif est décrit à la section 4.1. Le second est décrit à la section 4.3.

4.1 Scénarios attendus en mode normal

Lorsque la ligne de commande fonctionne (en mode normal), le système d'atterrissage réagit aux ordres du pilote en activant ou en inhibant les électrovannes des cylindres appropriés. Deux scénarios de base sont considérés : la séquence de sortie des trains et la séquence de rétraction de ces trains.

Séquence de sortie. La sortie des roues est décomposée en une séquence d'actions élémentaires. Lorsque les roues sont verrouillés en position rétractée et que les portes sont verrouillées en position fermée, si le pilote règle le levier sur «Down», le logiciel doit procéder comme suit :
1. stimuler l'électrovanne générale pour permettre l'envoi de pression hydraulique aux électrovannes de manoeuvre,
2. stimuler l'électrovanne d'ouverture de porte,
3. une fois les trois portes en position ouverte, stimuler l'électrovanne de sortie des roues,
4. une fois les trois roues verrouillés, arrêter la stimulation de l'électrovanne de sortie,
5. arrêtez la stimulation de l'électrovanne d'ouverture des portes,
6. stimulez l'électrovanne de fermeture des portes,
7. une fois que les trois portes sont verrouillées en position fermée arrêter la stimulation de l'électrovanne de fermeture de la porte,
8. enfin arrêter de stimuler l'électrovanne générale.

Séquence de rétraction. De la même manière, la rétraction des roues est décomposée en une séquence d'actions élémentaires. Lorsque les roues sont verrouillés en position basse et que les portes sont verrouillées en position fermée, si le pilote règle le levier sur «Up», le logiciel doit exécuter la séquence d'actions suivante :
1. stimuler l'électrovanne générale afin de permettre l'arrivée de pression hydraulique aux électrovannes de manœuvre,
2. stimulez l'électrovanne d'ouverture de la porte,
3. une fois les trois portes en position ouverte, si les trois roues sont sorties, stimuler l'électrovanne de rétraction des roues et passer à l'étape 4, sinon (sinon à l'étape 5),
4. une fois que les trois roues sont verrouillées, arrêter la stimulation de l'électrovanne de rétraction des roues,
5. arrêter la stimulation de l'électrovanne d'ouverture de porte,
6. stimuler l'électrovanne de fermeture de porte,
7. une fois que les trois portes sont verrouillées en position fermée, arrêter la stimulation de l'électrovanne de fermeture de porte,
8. et arrêter enfin de stimuler l'électrovanne générale.

Les séquences précédentes doivent pouvoir être interrompues (un ordre de rétraction survient pendant la séquence d'abaissement et inversement) à tout moment. Dans ce cas, le scénario continue à partir du point où il a été interrompu. Par exemple, si une séquence sortante est interrompue dans la phase de fermeture de la porte (étape 6 de la séquence sortante) par un ordre «Up», la stimulation de l'électrovanne de fermeture de la porte est arrêtée et la séquence de rétraction est exécutée à partir de l'étape 2 :

l'électrovanne d'ouverture de porte est stimulée et les portes recommencent à s'ouvrir. Ensuite, le scénario continue jusqu'à la dernière étape ou jusqu'à une nouvelle interruption.

Interaction avec le cockpit. Chaque logiciel de contrôle k ∈ {1,2} calcule les trois états booléens $gears\_locked\_down_k$, $gears\_maneuvering_k$ et $anomaly_k$.
- $gears\_locked\_down_k$ = true si et seulement si les trois roues sont considérées comme verrouillées en position étendue (capteur *gear_extended*[x] = true pour tout x ∈ {avant, droite, gauche}).
- $gears\_maneuvering_k$ = true si et seulement si au moins une porte ou une roue est en train de manœuvrer, c'est-à-dire qu'au moins une porte n'est pas verrouillée en position fermée ou qu'une roue n'est pas verrouillée en position d'extension ou de rétractation.
- $anomaly_k$ est spécifiée dans la section 4.3.

4.2 Contraintes de temps

En raison de contraintes hydrauliques, les contraintes de temps doivent être satisfaites par le logiciel de contrôle.

Stimulation électro-valve. En raison de l'inertie de la pression d'huile,
- les stimulations de l'électrovanne générale et de l'électrovanne de manœuvre doivent être espacées d'au moins 200 ms,
- les commandes d'arrêt de la stimulation de l'électrovanne générale et de l'électrovanne de manœuvre doivent être séparées d'au moins 1s.

Ordres contraires. En raison de l'inertie de la pression d'huile,
- deux ordres contraires (fermeture / ouverture des portes, extension / retrait) doivent être séparés d'au moins 100 ms.

4.3 Surveillance de la santé et scénarios prévus en cas d'incohérence

Le second objectif du logiciel de contrôle est de détecter les anomalies et d'informer le pilote. Les anomalies sont causées par des défaillances d'équipements hydrauliques, de composants électriques ou de modules informatiques.
Surveillance générique. Chaque capteur est triplé. La première activité du logiciel de contrôle consiste à sélectionner l'une de ces trois valeurs.
Appelons X un capteur et $X_i(t)$ i = 1,2,3 les trois valeurs de X reçues à l'instant t :
- Si en t les trois canaux sont considérés comme valides et égaux, alors la valeur considérée par le logiciel de contrôle est cette valeur commune.
- Si, pour la première fois, un canal est différent des deux autres (c'est-à-dire que les trois canaux étaient considérés comme valides jusqu'à t), ce canal est considéré comme invalide et définitivement éliminé. Seuls les deux canaux restants sont considérés à l'avenir. A l'instant t, la valeur considérée par le logiciel de contrôle est la valeur commune des deux canaux restants.
- Si un canal a été éliminé précédemment, et si les deux canaux restants ne sont pas égaux, le capteur est définitivement considéré comme non valide.

Une anomalie est détectée chaque fois qu'un capteur est définitivement considéré comme invalide.

Surveillance de commutateur analogique.
- Si le commutateur analogique est ouvert 1 seconde après le changement de position du levier, le commutateur est considéré comme non valide.
- Si le commutateur analogique est vu fermé 1,5 seconde après un intervalle de temps de 20 secondes pendant lequel la position du levier n'a pas changé, le commutateur est considéré comme non valide.
Dans ces deux cas, une anomalie est détectée.

Surveillance du capteur de pression.
- Si le circuit hydraulique n'est toujours pas sous pression 2 secondes après la stimulation de l'électrovanne générale, une anomalie est détectée dans le circuit hydraulique.
- Si le circuit hydraulique est toujours sous pression 10 secondes après l'arrêt de l'électrovanne générale, une anomalie est détectée dans le circuit hydraulique.

Surveillance du mouvement des portes.
- si le logiciel de contrôle ne voit pas la valeur *door_closed*[x] = false pour tout x ∈ {avant, gauche, droite} 7 secondes après la stimulation de l'électrovanne d'ouverture, les portes sont considérées comme bloquées et une anomalie est détectée.
- si le logiciel de contrôle ne voit pas la valeur *door_open*[x] = true pour tout x ∈ {avant, gauche, droite} 7 secondes après la stimulation de l'électrovanne d'ouverture, les portes sont considérées comme bloquées et une anomalie est détectée.
- si le logiciel de contrôle ne voit pas la valeur *door_open*[x] = false pour tout x ∈ {avant, gauche, droit} 7 secondes après la stimulation de l'électrovanne de fermeture, les portes sont considérées comme bloquées et une anomalie est détectée.
- si le logiciel de contrôle ne voit pas la valeur *door_closed*[x] = true pour tout x ∈ {avant, gauche, droite} 7 secondes après la stimulation de l'électrovanne de fermeture, les portes sont considérées comme bloquées et une anomalie est détectée.

Surveillance du mouvement des roues.
- si le logiciel de contrôle ne voit pas la valeur *gear_extended*[x] = false pour tout x ∈ {avant, gauche, droit} 7 secondes après la stimulation de l'électrovanne de rétraction, les roues sont considérés comme bloqués et une anomalie est détectée.
- si le logiciel de contrôle ne voit pas la valeur *gear_retracted*[x] = true pour tout x ∈ {avant, gauche, droit} 10 secondes après la stimulation de l'électrovanne de rétraction, les roues sont considérés comme bloqués et une anomalie est détectée.
- si le logiciel de contrôle ne voit pas la valeur *gear_retracted*[x] = false pour tout x ∈ {avant, gauche, droit} 7 secondes après la stimulation de l'électrovanne d'extension, les roues sont considérés comme bloqués et une anomalie est détectée.
- si le logiciel de contrôle ne voit pas la valeur *gear_extended*[x] = true pour tout x ∈ {avant, gauche, droit} 10 secondes après la stimulation de l'électrovanne d'extension, les roues sont considérés comme bloqués et une anomalie est détectée.

Comportement attendu en cas d'anomalie. Chaque fois qu'une anomalie est détectée, le système est globalement considéré comme non valide.
La donnée $anomaly_k$ = true est envoyée à l'interface pilote (où k est le numéro du module qui a détecté l'anomalie). Ce message est ensuite maintenu pour toujours. L'effet de cette action est d'allumer le feu rouge «défaillance du système d'atterrissage». Sinon (aucune anomalie ne s'est jamais produite), la donnée $anomaly_k$ = false est envoyée et maintenue à l'interface pilote. L'effet de cette action est de garder le feu rouge «défaillance du système d'atterrissage».

V. Conditions requises / Propriétés

Les exigences à prouver sur le système sont divisées en deux parties : exigences du mode normal et exigences du mode défaillance.

5.1 Conditions requises pour le mode normal

Exigence R1 :
- (R11) Lorsque la ligne de commande fonctionne (mode normal), si le levier de commande du train d'atterrissage a été abaissée et reste abaissée, les rapports seront verrouillés et les portes seront vues fermées moins de 15 secondes après que le levier a été poussé;
- (R12) Lorsque la ligne de commande fonctionne (mode normal), si le levier de commande du train d'atterrissage a été relevée et reste relevée, les rapports seront verrouillés et rentrés et les portes seront vues fermées moins de 15 secondes après que le levier a été poussé.
Notez qu'une version plus faible de ces deux exigences pourrait également être envisagée. Cette version plus faible ne prend pas en compte le temps quantitatif.
- (R11bis) Lorsque la ligne de commande fonctionne (mode normal), si le levier de commande du train d'atterrissage a été abaissée et reste abaissée, les rapports seront finalement verrouillés et les portes seront considérées comme fermées.
- (R12bis) Lorsque la ligne de commande fonctionne (mode normal), si le levier de commande du train d'atterrissage a été relevée et reste relevée, les rapports seront finalement verrouillés et rentrés et les portes seront vues fermées.

Exigence R2 :
- (R21) Lorsque la ligne de commande fonctionne (mode normal), si le levier de commande du train d'atterrissage reste en position BAS, la séquence de rentrée n'est pas respectée.
- (R22) Lorsque la ligne de commande fonctionne (mode normal), si le levier de commande du train d'atterrissage reste en position UP, la séquence sortante n'est pas observée.

Exigence R3 :
- (R31) Lorsque la ligne de commande est active (mode normal), les électrovannes de sortie ou les électrovannes de rétraction ne peuvent être stimulées que lorsque les trois portes sont verrouillées en position ouverte.
- (R32) Lorsque la ligne de commande fonctionne (mode normal), les électrovannes d'ouverture et de fermeture des portes ne peuvent être stimulées que lorsque les trois roues sont verrouillées ou en position haute.

Exigence R4 :
- (R41) Lorsque la ligne de commande fonctionne (mode normal), les électrovannes des portes d'ouverture et de fermeture ne sont pas stimulées simultanément.
- (R42) Lorsque la ligne de commande fonctionne (mode normal), les électrovannes des roues de sortie et de rétraction ne sont pas stimulées simultanément.

Exigence R5 :
- (R51) Lorsque la ligne de commande fonctionne (mode normal), il n’est pas possible de stimuler l’électrovanne de manœuvre (ouverture, fermeture, sortie ou rétraction) sans stimuler l’électrovanne générale.

5.2 Exigences relatives au mode de défaillance

Exigence R6 :
- (R61) Si une des trois portes est toujours verrouillée en position fermée plus de 7 secondes après la stimulation de l'électrovanne d'ouverture, le mode normal de sortie booléenne est défini sur False.
- (R62) Si l'une des trois portes est toujours vue verrouillée en position ouverte plus de 7 secondes après la stimulation de l'électrovanne de fermeture, le mode normal de sortie booléenne est défini sur false.
- (R63) Si l'une des trois roues est toujours vue verrouillée en position basse plus de 7 secondes après la stimulation de l'électrovanne de rétraction, le mode normal de sortie booléenne est défini sur false.
- (R64) Si l'une des trois roues est toujours verrouillée en position haute plus de 7 secondes après la stimulation de l'électrovanne de sortie, le mode normal de sortie booléenne est défini sur false.

Exigence R7 :
- (R71) Si l'une des trois portes n'est pas verrouillée en position ouverte plus de 7 secondes après la stimulation de l'électrovanne d'ouverture, le mode normal de sortie booléenne est défini sur false.
- (R72) Si l'une des trois portes ne se voit pas verrouillée en position fermée plus de 7 secondes après avoir stimulé l'électrovanne de fermeture, le mode normal de sortie booléenne est réglé sur false.
- (R73) Si l'une des trois roues ne se voit pas verrouillée en position haute plus de 10 secondes après la stimulation de l'électrovanne de rétraction, le mode normal de sortie booléenne est défini sur false.
- (R74) Si l'une des trois roues ne se voit pas verrouillée en position basse plus de 10 secondes après la stimulation de l'électrovanne de sortie, le mode normal de sortie booléenne est réglé sur false.

Exigence R8 :
- (R81) Lorsqu'au moins un module de calcul fonctionne, si le levier de commande du train d'atterrissage a été enfoncé pendant 15 secondes et si les roues ne sont pas verrouillés au bout de 15 secondes, le voyant rouge "Défaillance du système d'atterrissage" est allumé.
- (R82) Quand au moins un module de calcul fonctionne, si le levier de commande du train d'atterrissage a été levé pendant 15 secondes et si les roues ne sont pas verrouillés et rentrés au bout de 15 secondes, le voyant rouge «Défaillance du système d'atterrissage» est allumé.