(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

(43) Date de la publication internationale
05 mai 2022 (05.05.2022)

WIPO | PCT

(10) Numéro de publication internationale
WO 2022/090280 A1

(51) Classification internationale des brevets :
G05B 23/02 (2006.01)

(21) Numéro de la demande internationale :
PCT/EP2021/079761

(22) Date de dépôt international :
27 octobre 2021 (27.10.2021)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
20 10986 27 octobre 2020 (27.10.2020) FR

(71) Déposant : **THALES** [FR/FR] ; Tour Carpe Diem Place des Corolles, Esplanade Nord, 92400 Courbevoie (FR).

(72) Inventeur : **DE GRANCEY, Florence** ; CO Thales AVS, 105 Avenue du Général, Eisenhower BP 63647, 31036 Toulouse (FR).

(74) Mandataire : **HABASQUE, Etienne** et al. ; Lavoix, 2, place d'Estienne d'Orves, 75441 Paris Cedex 09 (FR).

(81) États désignés *(sauf indication contraire, pour tout titre de protection nationale disponible)* : AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, IT, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA,

(54) **Title:** ELECTRONIC SYSTEM FOR IMPLEMENTING A CRITICAL FUNCTION, AND ASSOCIATED METHOD AND COMPUTER PROGRAM

(54) **Titre :** SYSTÈME ÉLECTRONIQUE POUR LA MISE EN ŒUVRE D'UNE FONCTION CRITIQUE, PROCÉDÉ ET PROGRAMME D'ORDINATEUR ASSOCIÉS

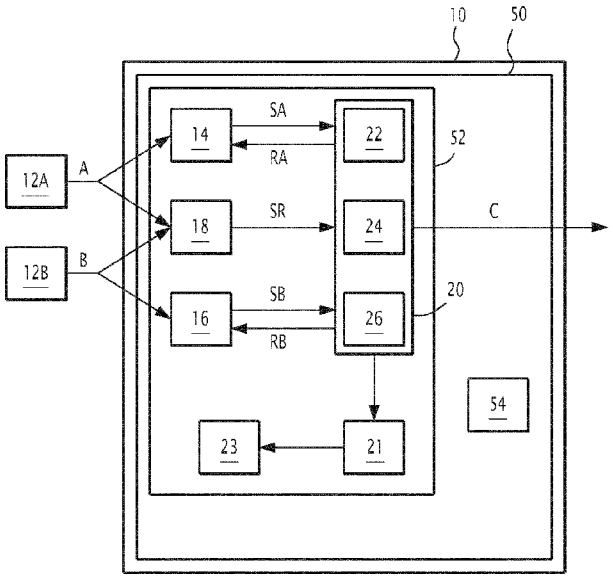


FIG.1

(57) **Abstract:** Said electronic system (10) for implementing a critical function comprises a first processing module (14) for calculating a first intermediate datum (SA) from a first input datum (A) and an reinforcement learning algorithm; a second processing module (16) for calculating a second intermediate datum (SB) from the algorithm and a second input datum (B); an auxiliary processing module (18) for calculating a reference intermediate datum (SR) from the first and/or second input datum and from a reference algorithm; and a monitoring device (20) for verifying whether the intermediate data belong to a security domain and for comparing them in order to detect any inconsistency; and for generating an output datum (C) on the basis of the intermediate data if they consistently belong to the security domain, the output datum otherwise being the reference intermediate datum.

WO 2022/090280 A1

[Suite sur la page suivante]

SC, SD, SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW.

(84) **États désignés** *(sauf indication contraire, pour tout titre de protection régionale disponible)* : ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), eurasien (AM, AZ, BY, KG, KZ, RU, TJ, TM), européen (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Publiée:

— *avec rapport de recherche internationale (Art. 21(3))*

(57) Abrégé : Ce système électronique (10) de mise en œuvre une fonction critique comprend un premier module de traitement (14) pour calculer une première donnée intermédiaire (SA) à partir d'une première donnée d'entrée (A) et d'un algorithme d'apprentissage par renforcement; un deuxième module de traitement (16) pour calculer une deuxième donnée intermédiaire (SB) à partir dudit algorithme et d'une deuxième donnée d'entrée (B); un module de traitement auxiliaire (18) pour calculer une donnée intermédiaire de référence (SR) à partir de la première et/ou deuxième donnée d'entrée et d'un algorithme de référence; et un dispositif de surveillance (20) pour vérifier si les données intermédiaires appartiennent à un domaine de sécurité et pour les comparer afin de détecter une éventuelle incohérence; et pour générer une donnée de sortie (C) en fonction des données intermédiaires si elles appartiennent au domaine de sécurité et sans incohérence, la donnée de sortie étant la donnée intermédiaire de référence sinon.

TITRE : Système électronique pour la mise en œuvre d'une fonction critique, procédé et programme d'ordinateur associés

La présente invention concerne un système électronique configuré pour mettre en œuvre une fonction critique.

L'invention concerne également un procédé de mise en œuvre d'une fonction critique par un tel système électronique.

L'invention concerne également un programme d'ordinateur comportant des instructions logicielles qui, lorsqu'elles sont exécutées par un ordinateur, mettent en œuvre un tel procédé.

Le système électronique est notamment embarqué dans une installation ou dans un appareil. L'appareil est de préférence un véhicule, tel qu'un véhicule aérien, en particulier un aéronef, un véhicule ferroviaire ou véhicule automobile. En variante, l'installation est par exemple une usine ou une centrale électrique.

En particulier, l'invention concerne la mise en œuvre de fonctions critiques, c'est-à-dire qui sont critiques pour la sécurité de l'appareil ou de l'installation. Les commandes de pilotage du véhicule, telles que les commandes de vol d'un aéronef, le système de freinage du véhicule, l'arrêt d'urgence d'une usine chimique ou d'une centrale électrique sont des exemples de telles fonctions critiques.

Dans le domaine avionique, une fonction critique est par exemple définie par la norme ARP-4754A (*Aerospace Recommended Practice* en anglais).

Par mise en œuvre d'une fonction critique, on entend la réalisation d'un ou plusieurs calculs permettant de générer au moins une donnée de sortie associée à cette fonction critique, à partir d'au moins une donnée d'entrée.

Afin d'assurer la sécurité de l'appareil ou de l'installation, il est ainsi nécessaire de s'assurer que la mise en œuvre de la fonction critique s'effectue sans défaillance. En particulier, une telle fonction critique est de manière conventionnelle associée à un domaine d'usage de sécurité définissant une plage de valeur(s) autorisée(s) pour la donnée de sortie associée à cette fonction critique. Une donnée de sortie hors de la plage de valeur(s) autorisée(s) sera refusée, et une alerte sera alors émise. Dans le domaine avionique, cette plage de valeur(s) autorisée(s) est par exemple des valeurs comprises entre une limite minimum et une limite maximum telles que par exemple des limites maximale et minimale d'altitude de l'aéronef. La plage de valeur(s) correspond en variante une limite maximum ou une limite minimale à ne pas dépasser telle qu'une limite de vitesse ascensionnelle de l'aéronef ou une puissance maximale du moteur de l'aéronef.

En variante encore, la plage de valeur(s) correspond à une valeur unique, typiquement 0 ou 1, associé à un indicateur booléen, tel qu'un état de marche d'un système avionique de l'aéronef.

On connait des algorithmes d'apprentissage par renforcement qui ont pour objectif d'apprendre progressivement une fonction ou un modèle de comportement, par la réalisation d'expériences successives et avec un retour d'un indicateur de performance de la fonction. Une fois l'apprentissage réalisé, ces algorithmes d'apprentissage par renforcement permettent d'améliorer les performances de mise en œuvre de la fonction critique. En outre, les algorithmes par renforcement permettent de modéliser des fonctions critiques qui ne sont pas modélisables de manière conventionnelle, via par exemple des lois physiques, du fait d'une complexité du système trop importante.

Toutefois, ces algorithmes présentent des vulnérabilités qui affectent la sécurité du système électronique. En effet, la mise en œuvre de la fonction critique par ces algorithmes d'apprentissage par renforcement donne, dans certains cas, un résultat n'appartenant pas au domaine de sécurité associé à la fonction critique, ce qui entraine éventuellement des conséquences importantes sur la sécurité de l'installation ou de l'appareil dans lequel le système est embarqué. Ces vulnérabilités limitent ainsi grandement l'utilisation de ces algorithmes pour la mise en œuvre de fonction(s) critique(s).

Il existe donc un besoin d'obtenir un système électronique plus performant de mise en œuvre d'une fonction critique tout en étant suffisamment sûr.

A cet effet, l'invention a pour objet un système électronique configuré pour mettre en œuvre une fonction critique, le système électronique étant propre à recevoir des première et deuxième données d'entrée et à délivrer une donnée de sortie associée à ladite fonction critique, la donnée de sortie étant associée à un domaine de sécurité prédéterminé, le domaine de sécurité étant en forme d'une plage de valeurs prédéfinies,

le système électronique comprenant :

- un premier module de traitement configuré pour calculer une première donnée intermédiaire à partir de la première donnée d'entrée et d'un algorithme d'apprentissage par renforcement, pour la mise en œuvre de la fonction critique pour la première donnée d'entrée,

- un deuxième module de traitement configuré pour calculer une deuxième donnée intermédiaire à partir de la deuxième donnée d'entrée et de l'algorithme d'apprentissage par renforcement, pour la mise en œuvre de la fonction critique pour la deuxième donnée d'entrée, la deuxième donnée d'entrée étant différente de la première donnée d'entrée,

- un module de traitement auxiliaire configuré pour calculer une donnée intermédiaire de référence à partir de la première donnée d'entrée et/ou de la deuxième donnée d'entrée et d'un algorithme de référence différent de l'algorithme d'apprentissage par renforcement, pour la mise en œuvre de la fonction critique pour la première donnée d'entrée et/ou la deuxième donnée d'entrée via l'algorithme de référence,

- un dispositif de surveillance comportant :

+ un module de contrôle configuré pour vérifier si les première et deuxième données intermédiaires appartiennent au domaine de sécurité et pour comparer les première et deuxième données intermédiaires entre elles afin de détecter une éventuelle incohérence;

+ un module de génération configuré pour générer la donnée de sortie en fonction des première et deuxième données intermédiaires si les première et deuxième données intermédiaires appartiennent au domaine de sécurité et si aucune incohérence n'est détectée, la donnée de sortie étant égale à la donnée intermédiaire de référence sinon.

Suivant d'autres aspects avantageux de l'invention, le système électronique comprend une ou plusieurs des caractéristiques suivantes, prises isolément ou suivant toutes les combinaisons techniquement possibles :

- l'ensemble des mises en œuvre de la fonction critique par l'algorithme de référence définit un domaine d'arrivée de l'algorithme de référence, le domaine d'arrivée étant inclus dans le domaine de sécurité ;

- le dispositif de surveillance comporte un module de récompense configuré pour calculer une première récompense pour la mise en œuvre de la fonction critique par le premier module de traitement et une deuxième récompense pour la mise en œuvre de la fonction critique par le deuxième module de traitement,

le premier module de traitement étant configuré pour mettre en œuvre l'algorithme d'apprentissage par renforcement en fonction d'une première pluralité de paramètres algorithmiques, le premier moule de traitement étant configuré, à chaque itération, pour recevoir la première récompense et pour modifier la première pluralité de paramètres algorithmiques en fonction de la première récompense reçue afin de maximiser la prochaine première récompense reçue,

le deuxième module de traitement étant configuré pour mettre en œuvre l'algorithme d'apprentissage par renforcement en fonction d'une deuxième pluralité de paramètres algorithmiques, le deuxième module de traitement étant configuré, à chaque itération, pour recevoir la deuxième récompense et pour modifier la deuxième pluralité de

paramètres algorithmiques en fonction de la deuxième récompense reçue afin de maximiser la prochaine deuxième récompense reçue ;

- le module de récompense est configuré pour pénaliser chaque première récompense et/ou respectivement chaque deuxième récompense lorsque la première donnée intermédiaire et/ou respectivement la deuxième donnée intermédiaire n'appartiennent pas au domaine de sécurité ;

- lorsque les première et deuxième données intermédiaires appartiennent au domaine de sécurité et en l'absence d'incohérence détectée, le module de génération est configuré pour délivrer, en donnée de sortie, la donnée intermédiaire associée à la récompense la plus élevée calculée par le module de récompense ;

- le module de contrôle est en outre configuré pour comparer les première et deuxième récompenses entre elles afin de détecter une éventuelle incohérence,

et dans lequel le système électronique comprend en outre un module d'alerte configuré pour générer un signal d'alerte en fonction de chaque incohérence entre les données intermédiaires et/ou entre les récompenses ;

- le module de contrôle est configuré en outre pour comptabiliser le nombre de fois où respectivement les première et deuxième données intermédiaires ne respectent pas le domaine de sécurité et pour réinitialiser respectivement la première pluralité de paramètres algorithmiques et la deuxième pluralité de paramètres algorithmiques lorsque ledit nombre est supérieur à un seuil prédéterminé ; et

- le système est un système avionique propre à être embarqué dans un poste de commande d'un aéronef, notamment un système de navigation de l'aéronef.

L'invention concerne également un procédé de mise en œuvre d'une fonction critique par un système électronique, le système électronique étant configuré pour mettre en œuvre une fonction critique, le système électronique étant propre à recevoir des première et deuxième données d'entrée et à délivrer une donnée de sortie associée à ladite fonction critique, la donnée de sortie étant associée à un domaine de sécurité prédéterminé, le domaine de sécurité étant en forme d'une plage de valeur(s) prédéfinie(s),

le procédé comprenant les étapes suivantes :

- calcul d'une première donnée intermédiaire à partir de la première donnée d'entrée et d'un algorithme d'apprentissage par renforcement, pour la mise en œuvre de la fonction critique pour la première donnée d'entrée,

- calcul d'une deuxième donnée intermédiaire à partir de la deuxième donnée d'entrée et de l'algorithme d'apprentissage par renforcement, pour la mise en œuvre de la

fonction critique pour la deuxième donnée d'entrée, la deuxième donnée d'entrée étant différente de la première donnée d'entrée,

- calcul d'une donnée intermédiaire de référence à partir de la première donnée d'entrée et/ou de la deuxième donnée d'entrée et d'un algorithme de référence différent de l'algorithme d'apprentissage par renforcement, pour la mise en œuvre de la fonction critique pour la première donnée d'entrée et/ou la deuxième donnée d'entrée via l'algorithme de référence,

- vérification si les première et deuxième données intermédiaires appartiennent au domaine de sécurité et comparaison des première et deuxième données intermédiaires entre elles afin de détecter une éventuelle incohérence;

- génération de la donnée de sortie en fonction des première et deuxième données intermédiaires si les première et deuxième données intermédiaires appartiennent au domaine de sécurité et si aucune incohérence n'est détectée, la donnée de sortie étant égale à la donnée de référence sinon.

L'invention a également pour objet un programme d'ordinateur comportant des instructions logicielles qui, lorsqu'elles sont exécutées par un ordinateur, mettent en œuvre un procédé tel que défini ci-dessus.

Ces caractéristiques et avantages de l'invention apparaîtront plus clairement à la lecture de la description qui va suivre, donnée uniquement à titre d'exemple non limitatif, et faite en référence aux dessins annexés, sur lesquels :

[Fig 1] la figure 1 est une représentation schématique d'un système électronique selon l'invention,

[Fig 2] la figure 2 est une représentation schématique de la mise en œuvre d'un algorithme de renforcement par apprentissage, et

[Fig 3] la figure 3 est un organigramme d'un procédé, selon l'invention, de mise en œuvre d'une fonction critique par le système électronique de la figure 1.

Un système électronique 10 est représenté sur la figure 1. Le système électronique 10 est configuré pour mettre en œuvre au moins une fonction critique.

Dans l'exemple de la figure 1, le système électronique 10 est embarqué dans un aéronef. L'aéronef est typiquement un avion, un hélicoptère, ou encore un drone. Autrement dit, l'aéronef est un engin volant pilotable par un pilote via un poste de commande, le poste de commande étant disposé à l'intérieur de l'aéronef ou bien à distance de l'aéronef, notamment dans le cas d'un drone.

Dans cet exemple, le système électronique 10 est alors un système avionique configuré pour mettre en œuvre une fonction critique avionique.

La fonction critique avionique est alors typiquement choisie parmi le groupe consistant en : un calcul de trajectoire de l'aéronef, une commande de vol de l'aéronef, la stratégie d'évitement d'un obstacle sur la trajectoire de l'aéronef, une fonction de freinage de l'aéronef, etc.

L'homme du métier comprendra que l'invention s'applique également à d'autres fonctions critiques, telles qu'à un processus de contrôle de la réactivité dans un réacteur nucléaire, à un contrôle de la température dans un fourneau d'une usine, à une commande de navigation d'un véhicule automobile autonome, à une commande de vitesse d'un véhicule ferroviaire, etc.

Le système électronique 10 est propre à recevoir des première et deuxième données d'entrée, notées A et B par la suite, et à délivrer une donnée de sortie C associée à ladite fonction critique.

La deuxième donnée d'entrée B est distincte et différente de la première donnée d'entrée A.

Chaque donnée d'entrée A, B est fournie par un dispositif électronique amont 12A, 12B respectif.

Le dispositif électronique amont 12A associé à la donnée d'entrée A est différent du dispositif électronique amont 12B associé à la donnée d'entrée B.

Chaque dispositif électronique amont 12A, 12B est par exemple embarqué à bord de l'aéronef. Chaque dispositif électronique amont 12A, 12B est notamment un capteur embarqué dans l'aéronef, par exemple une caméra, un capteur de position ou un capteur de température. En variante, chaque dispositif électronique amont 12A, 12B est un autre système, notamment un autre système avionique.

En variante encore, chaque dispositif électronique amont 12A, 12B est un système externe à l'aéronef, tel qu'une tour de contrôle communiquant la donnée d'entrée A, B associée à l'aéronef.

Avantageusement, les première et deuxième données d'entrée A, B sont de même type. Autrement dit, le type des valeurs susceptibles d'être prises par les première et deuxièmes données est identique pour ces première et deuxième données.

En particulier, ce type est choisi parmi le groupe consistant en : une image, un flux vidéo, une mesure ou une succession de mesures d'un ou plusieurs paramètres de fonctionnement du système électronique 10, un signal de mesure issu d'un capteur, une commande d'un utilisateur du système électronique 10, un texte (c'est-à-dire une

succession de caractères alphanumériques) issu de notices d'informations ou de reconnaissance vocale.

A titre d'exemple, les première et deuxième données d'entrée A, B sont des images de l'environnement de l'aéronef provenant de deux caméras embarquées différentes, des données de localisation de l'aéronef issus de deux capteurs différents, des paramètres avioniques, tels que le niveau de carburant ou l'état de fonctionnement d'un ou plusieurs système avioniques, ou encore sont des commandes de vol issues de deux systèmes de pilotage différents redondés.

En variante, les première et deuxième données d'entrée A, B sont de types différents.

A titre d'exemple, la première donnée d'entrée A est une image de l'environnement de l'aéronef issue d'une caméra embarquée sur l'aéronef, et la deuxième donnée d'entrée B est une représentation numérique du terrain survolé par l'aéronef issue d'une base de données géographiques.

La donnée de sortie C est avantageusement une valeur numérique ou indicateur booléen, typiquement égal à 0 ou 1.

La donnée de sortie C est par exemple une valeur d'une commande de vol, d'une consigne de vitesse ou d'altitude pour l'aéronef, d'une consigne d'activation/désactivation d'un système avionique, etc.

La donnée de sortie C est associée à un domaine de sécurité prédéterminé, le domaine de sécurité étant en forme d'une plage de valeur(s) prédéfinie(s).

Ainsi, lorsque la donnée de sortie C est une valeur numérique, le domaine de sécurité est par exemple un intervalle de valeurs entre deux bornes prédéterminées ou un intervalle ouvert défini par une valeur seuil minimale ou maximale ou encore un ensemble de tels intervalles. Lorsque la donnée de sortie est un indicateur booléen, typiquement égal à 0 ou 1, le domaine de sécurité est alors une valeur unique.

Le système électronique 10 comprend un premier module de traitement 14, un deuxième module de traitement 16, un module de traitement auxiliaire 18 et un dispositif de surveillance 20.

En complément facultatif, le système électronique comprend en outre un module d'alerte 21 et un module d'affichage 23.

Le premier module de traitement 14, le deuxième module de traitement 16 et le module de traitement auxiliaire 18 sont par exemple embarqués chacun sur un calculateur électronique distinct respectif.

Chaque calculateur électronique comprend avantageusement sa propre alimentation électrique et sa propre unité de calcul. Le calculateur électronique est, par

exemple, en forme d'un module électronique indépendant d'autre(s) module(s) électronique(s) et apte à être installé dans un rack, non représenté, ou encore en forme d'une carte électronique, indépendante d'autre(s) carte(s) électronique (s), et apte à être installée dans un coffret électronique. En variante, le calculateur électronique a son propre coffret électronique, et est alors le seul calculateur disposé à l'intérieur d'un boitier de protection associé au coffret.

Le premier module de traitement 14 est configuré pour calculer une première donnée intermédiaire SA à partir de la première donnée d'entrée A et d'un algorithme d'apprentissage par renforcement pour la mise en œuvre de la fonction critique.

Autrement dit, le premier module de traitement 14 est configuré pour mettre en œuvre la fonction critique pour la première donnée d'entrée A, en appliquant l'algorithme d'apprentissage par renforcement à la première donnée d'entrée A, ceci afin d'obtenir la première donnée intermédiaire SA.

Le fonctionnement d'un algorithme d'apprentissage par renforcement est représenté schématiquement sur la figure 2. De manière connue, l'apprentissage par renforcement consiste, pour un agent X autonome tel qu'un algorithme, dans un état courant S, à apprendre des actions F à effectuer, à partir d'expériences, de façon à optimiser une récompense R quantitative au cours du temps. L'agent X est plongé au sein de l'environnement E, et prend ses décisions en fonction de son état courant S. En retour, l'environnement E procure à l'agent X une récompense R, positive ou négative et l'agent X évolue dans un nouvel état courant S'. L'agent X cherche, au travers d'expériences itérées, à optimiser un comportement décisionnel appelé stratégie ou politique, et qui est une fonction associant à l'état courant S l'action F à exécuter, afin de maximiser la somme des récompenses R au cours du temps.

Ainsi, dans un tel problème, on dit que l'agent X interagit avec l'environnement E pour trouver la solution optimale. L'apprentissage par renforcement diffère fondamentalement des problèmes supervisés et non-supervisés par ce côté interactif et itératif : l'agent X essaie plusieurs solutions (on parle « d'exploration »), observe la réaction de l'environnement E et adapte son comportement pour trouver la meilleure stratégie.

Les principales familles d'algorithmes d'apprentissage par renforcement sont notamment les méthodes dite de « Q-learning», les variantes du Q-learning telles que les méthodes dite de « Deep Q-learning », les méthodes dites « Actor-Critic », les algorithmes de bandits, les algorithmes de décisions markovien et les arbres de jeu.

Comme cela sera expliqué par la suite, une récompense est déterminée par le dispositif de contrôle 20 en réponse à la première donnée intermédiaire SA et est renvoyé

au premier module de traitement 14. Le premier module de traitement 14 est alors propre à faire évoluer l'algorithme d'apprentissage par renforcement en fonction de cette récompense pour le calcul de la prochaine première donnée intermédiaire SA afin de maximiser la prochaine récompense reçue.

En particulier, le premier module de traitement 14 est configuré pour appliquer préférentiellement une méthode dite de « Q-learning », une méthode dite « Actor-Critic » ou une variante de ces méthodes connues de l'homme du métier.

Avantageusement, le premier module de traitement 14 est configuré pour mettre en œuvre l'algorithme d'apprentissage par renforcement en fonction d'une première pluralité de paramètres algorithmiques.

Chaque paramètre algorithmique permet notamment de contrôler l'importance d'une variable ou d'une fonction dans les calculs effectués par l'algorithme d'apprentissage par renforcement. Ainsi, la modification d'un ou plusieurs paramètres algorithmiques permet de faire évoluer et d'ajuster l'algorithme d'apprentissage par renforcement au cours de son exploitation.

La méthode dite de « Q-learning » a typiquement pour objectif de construire une table permettant de lier chaque donnée d'entrée possible à un cout, en ajustant au fur et à mesure les coûts, correspondant aux valeurs de la table.

Le premier module de traitement 14 est configuré pour mettre en œuvre l'algorithme d'apprentissage par renforcement avec la méthode dite de « Q-learning » si le nombre de données d'entrée possibles, ou encore considérées ou prises en compte, pour la première donnée d'entrée A est faible, typiquement si ce nombre de données d'entrée est inférieur à un seuil prédéfini. Le premier module de traitement 14 est typiquement configuré pour mettre en œuvre l'algorithme d'apprentissage par renforcement avec la méthode dite de « Q-learning » si une combinatoire de données d'entrée pour la première donnée d'entrée A est faible, telle qu'inférieure à un seuil correspondant prédéfini.

La méthode dite de « Deep Q-learning » construit typiquement un réseau de neurones qui calcule le coût à partir de chaque donnée d'entrée possible, avec un ajustement des paramètres, tels que poids, du réseau de neurones, par exemple par une méthode de descente de gradient.

Le premier module de traitement 14 est configuré pour mettre en œuvre l'algorithme d'apprentissage par renforcement avec la méthode dite de « Deep Q-learning » si le nombre de données d'entrée possibles, ou encore considérées ou prises en compte, pour la première donnée d'entrée A est élevé, en particulier trop grand pour réaliser une table, typiquement si ce nombre de données d'entrée est supérieur au seuil prédéfini. Le premier module de traitement 14 est typiquement configuré pour mettre en œuvre

l'algorithme d'apprentissage par renforcement avec la méthode dite de « Deep Q-learning » si la combinatoire de données d'entrée pour la première donnée d'entrée A est élevée, telle que supérieure au seuil correspondant prédéfini.

Pour la méthode dite « Actor-Critic », le principe est d'estimer une fonction de coût et de valeur. Ces fonctions sont généralement modélisées par des réseaux de neurones, en ajustant les poids de ces réseaux de neurones.

Le premier module de traitement 14 est typiquement configuré pour mettre en œuvre l'algorithme d'apprentissage par renforcement avec la méthode dite « Actor-Critic » si le nombre de données d'entrée possibles, ou encore considérées ou prises en compte, pour la première donnée d'entrée A est élevé, en particulier trop grand pour réaliser une table, typiquement si ce nombre de données d'entrée est supérieur au seuil prédéfini.

Le paramètre algorithmique est alors typiquement le nombre de données d'entrée possibles, considérées ou prises en compte ; ou encore la combinatoire de données d'entrée pour la première donnée d'entrée A.

Le premier module de traitement 14 est en outre configuré pour envoyer la première donnée intermédiaire SA au dispositif de surveillance 20.

Le deuxième module de traitement 16 est configuré pour calculer une deuxième donnée intermédiaire SB à partir de la deuxième donnée d'entrée B et de l'algorithme d'apprentissage par renforcement pour la mise en œuvre de la fonction critique.

Autrement dit, le deuxième module de traitement 16 est configuré pour mettre en œuvre la fonction critique pour la deuxième donnée d'entrée B, en appliquant l'algorithme d'apprentissage par renforcement à la deuxième donnée d'entrée B, ceci afin d'obtenir la deuxième donnée intermédiaire SB.

La fonction critique est donc mise en œuvre par le deuxième module de traitement 16 avec le même algorithme que celui utilisé par le premier module de traitement 14, mais avec une donnée d'entrée différente.

Avantageusement, le deuxième module de traitement 16 est configuré pour mettre en œuvre l'algorithme d'apprentissage par renforcement en fonction d'une deuxième pluralité de paramètres algorithmiques.

L'homme du métier comprendra que la première pluralité de paramètres algorithmiques et la deuxième pluralité de paramètres algorithmiques sont semblables et permettent d'ajuster les mêmes variables ou fonctions, mais présentent éventuellement des valeurs numériques pour chaque paramètre algorithmique différentes en fonction respectivement des premières et deuxièmes récompenses reçues.

Le deuxième module de traitement 16 est en outre configuré pour envoyer la deuxième donnée intermédiaire SB au dispositif de surveillance 20.

Le module de traitement auxiliaire 18 est configuré pour calculer une donnée intermédiaire de référence SR à partir de de la première donnée d'entrée A et/ou de la deuxième donnée d'entrée B et d'un algorithme de référence pour la mise en œuvre de la fonction critique.

Autrement dit, le module de traitement auxiliaire 18 est configuré pour mettre en œuvre la fonction critique pour la première donnée d'entrée A et/ou la deuxième donnée d'entrée B, en appliquant l'algorithme de référence à la première donnée d'entrée A et/ou à la deuxième donnée d'entrée B, ceci afin d'obtenir la donnée intermédiaire de référence SR.

Le module de traitement auxiliaire 18 est par exemple configuré pour mettre en œuvre la fonction critique uniquement à partir de la première donnée d'entrée A ou uniquement à partir de la deuxième donnée d'entrée B. En particulier, le module de traitement auxiliaire 18 est configuré pour prendre en entrée prioritairement la première donnée d'entrée A, et sinon, notamment en cas de défaillance du premier dispositif électronique amont 12A, pour prendre en entrée la deuxième donnée d'entrée B.

En variante, le module de traitement auxiliaire 18 est configuré pour mettre la fonction critique à partir à la fois de la première donnée d'entrée A et de la deuxième donnée d'entrée B.

En variante encore, le module de traitement auxiliaire 18 est configuré pour mettre en œuvre la fonction critique uniquement à partir de la première donnée d'entrée A ; et séparément mettre en œuvre la fonction critique uniquement à partir de la deuxième donnée d'entrée B. Selon cette variante, le module de traitement auxiliaire 18 est alors configuré pour fournir en outre au dispositif de surveillance 20 une deuxième donnée intermédiaire de référence SR' associée à la deuxième mise en œuvre de la fonction critique.

L'algorithme de référence est différent de l'algorithme d'apprentissage par renforcement. Ainsi, l'algorithme de référence n'est pas configuré pour mettre en œuvre un apprentissage par renforcement.

L'ensemble des mises en œuvre de la fonction critique par l'algorithme de référence définit un domaine d'arrivée de l'algorithme de référence. Avantageusement, le domaine d'arrivée est inclus dans le domaine de sécurité. Ainsi, la mise en œuvre de la fonction critique par le module de traitement auxiliaire 18 donne en sortie une donnée intermédiaire de référence SR toujours comprise dans le domaine de sécurité de la fonction critique, garantissant ainsi la sécurité de l'aéronef.

L'algorithme de référence est notamment un algorithme ne mettant pas en œuvre une méthode d'apprentissage automatique. En particulier, l'algorithme de référence est un

algorithme déterministe constitué, par exemple, d'une succession d'instructions conditionnelles (de type « if, then ») et/ou basé sur la mise en œuvre d'un modèle physique constitué d'un ensemble d'équations décrivant le fonctionnement du système, les équations étant notamment établies par un homme du métier à partir de lois physiques, éventuellement simplifiées., ou encore des méthodes de traitement du signal ou de filtrage. Les méthodes de traitement du signal ou de filtrage sont par exemple des méthodes mettant en œuvre des filtres numériques, des filtres de Kalman, connus en soi.

L'homme du métier comprendra alors que l'algorithme de référence est un algorithme déterministe, c'est-à-dire entièrement justifiable, ce qui n'est pas le cas l'algorithme d'apprentissage par renforcement qui est construit au fur et à mesure des essais, notamment de son apprentissage.

La fonction critique est donc mise en œuvre par le module de traitement auxiliaire 18 avec les même données d'entrée A, B que les premier et deuxième modules de traitement 14, 16 mais avec un algorithme différent.

Le module de traitement auxiliaire 18 est en outre configuré pour envoyer la ou les donnée(s) intermédiaire(s) de référence SR, SR' au dispositif de surveillance 20.

Le dispositif de surveillance 20 comporte un module de contrôle 22 et un module de génération 24.

En complément, le dispositif de surveillance 20 comporte en outre un module de récompense 26.

Le module de récompense 26 est configuré pour calculer une première récompense RA associée à la mise en œuvre de la fonction critique par le premier module de traitement 14 et une deuxième récompense RB associée à la mise en œuvre de la fonction critique par le deuxième module de traitement 16.

En particulier, le module de récompense 26 est configuré pour calculer les première et deuxième récompenses RA, RB en fonction d'une règle de récompense prédéterminée.

Comme expliqué ci-dessus, la règle de récompense prédéterminée définit si le calcul réalisé par le premier ou le deuxième module de traitement 14, 16 est proche d'un objectif prédéterminé.

A titre d'exemple, l'objectif est par exemple une trajectoire de l'aéronef à suivre et la règle de récompense est définie par la distance entre la trajectoire réelle suivie par l'aéronef et la trajectoire visée. Ainsi, plus la distance entre les deux trajectoires est proche, plus la récompense est élevée en réponse, de telle sorte que les premier et deuxième modules de traitement 14, 16 prennent en compte de manière privilégiée les actions conduisant à une trajectoire la plus proche possible de la trajectoire visée.

Le module de récompense 26 est en outre configuré pour pénaliser chaque première récompense RA et/ou respectivement chaque deuxième récompense RB, si la première donnée intermédiaire SA et/ou respectivement si la deuxième donnée intermédiaire SB n'appartiennent pas au domaine de sécurité.

Le module de récompense 26 est par exemple configuré pour multiplier chaque première récompense RA et/ou respectivement chaque deuxième récompense RB par un coefficient multiplicateur strictement inférieur à 1 si la première donnée intermédiaire SA et/ou respectivement si la deuxième donnée intermédiaire SB n'appartiennent pas au domaine de sécurité. Plus l'écart entre la première et/ou deuxième données intermédiaires SA, SB par rapport au domaine de sécurité est important, plus le coefficient multiplicateur est petit afin de pénaliser la première ou deuxième récompense RA, RB associée.

En variante, le module de récompense 26 est configuré pour soustraire à chaque première récompense RA et/ou respectivement à chaque deuxième récompense RB, une valeur proportionnelle à l'écart entre la première ou deuxième récompense RA, RB par rapport au domaine de sécurité.

Le premier module de traitement 14 est configuré pour recevoir la première récompense RA à chaque itération, et pour modifier la première pluralité de paramètres algorithmiques en fonction de la première récompense reçue RA à chaque itération afin de maximiser la prochaine première récompense RA reçue.

Le deuxième module de traitement 16 est configuré pour recevoir la deuxième récompense RB à chaque itération, et pour modifier la deuxième pluralité de paramètres algorithmiques en fonction de la deuxième récompense reçue RB à chaque itération afin de maximiser la prochaine deuxième récompense RB reçue.

Le module de contrôle 22 est configuré pour vérifier si les première et deuxième données intermédiaires SA, SB appartiennent au domaine de sécurité.

En particulier, si les première et deuxième données intermédiaires SA, SB sont des valeurs numériques, le module de contrôle 22 est configuré pour vérifier si les première et deuxième données intermédiaires SA, SB appartiennent à la plage de valeurs définissant le domaine de sécurité.

Si les première et deuxième données intermédiaires SA, SB sont des indicateurs booléens, le module de contrôle 22 est configuré pour vérifier si les première et deuxième données intermédiaires SA, SB sont égale à la valeur associée au domaine de sécurité, typiquement 0 ou 1.

Le module de contrôle 22 est en outre configuré pour comparer les première et deuxième données intermédiaires SA, SB entre elles afin de détecter une éventuelle incohérence.

La comparaison entre les deux données intermédiaires SA, SB détermine si ces deux données intermédiaires sont cohérentes entre elles ou non selon une règle de cohérence prédéterminée. La règle de cohérence définit un critère sur le résultat de la comparaison permettant de définir si les données intermédiaires sont cohérentes entre elles.

Typiquement, si les données intermédiaires sont des valeurs numériques, la règle de cohérence définit un calcul d'une métrique, telle qu'une distance entre les données, par exemple la valeur absolue de la différence, et un seuil de cohérence. Les données intermédiaires SA, SB sont alors cohérentes entre elles si la métrique, telle que la distance entre les valeurs est inférieure au seuil de cohérence.

A titre d'exemple, deux données intermédiaires représentant des consignes de vitesse de l'aéronef présentant une différence de valeur de plus de 10% sont considérées comme incohérentes entre elles.

Le module de contrôle 22 est configuré en outre pour comptabiliser le nombre de fois où respectivement les première et deuxième données intermédiaires SA, SB ne respectent pas le domaine de sécurité.

Le module de contrôle 22 est configuré pour réinitialiser respectivement la première pluralité de paramètres algorithmiques et la deuxième pluralité de paramètres algorithmiques lorsque ledit nombre est supérieur à un seuil prédéterminé.

En particulier, les algorithmes d'apprentissage par renforcement mis en œuvre dans les premier et deuxième modules de traitement 14, 16 sont entrainés dans un environnement contrôlé de type simulation, avant l'exploitation en conditions réelles du système 10. Cet entraînement permet l'établissement d'un comportement des algorithmes assurant un fonctionnement des algorithmes assurant des performances et une sécurité jugées suffisantes par un homme du métier avant l'exploitation du système 10. Les paramètres algorithmiques de l'algorithme obtenus après l'entraînement sont sauvegardés dans une base de données embarquée dans le système 10.

Ainsi, on entend par « réinitialiser la première pluralité de paramètres algorithmiques et la deuxième pluralité de paramètres algorithmiques, le fait de réinitialiser les algorithmes d'apprentissage par renforcement mis en œuvre dans les premier et deuxième modules de traitement 14, 16 selon les paramètres algorithmiques définis lors de l'entrainement avant l'exploitation du système 10.

Avantageusement, lorsque le module de traitement auxiliaire 18 est configuré pour fournir deux données intermédiaires de référence associées à partir de respectivement la première donnée d'entrée A et la deuxième donnée d'entrée B pour la mise en œuvre de la fonction critique, le module de contrôle 22 est configuré pour comparer la première donnée intermédiaire SA avec la donnée intermédiaire de référence SR associée à la première donnée d'entrée A, et respectivement pour comparer la deuxième donnée intermédiaire SB avec la donnée intermédiaire de référence SR' associée à la deuxième donnée d'entrée B.

Ainsi, en cas d'incohérence détectée entre les première et deuxième données intermédiaires SA, SB, le module de contrôle 22 est propre à détecter si la défaillance est due aux données d'entrée A, B ou bien à la mise en œuvre de la fonction critique par les premier et deuxième modules de traitement 14, 16.

En effet, si la première donnée intermédiaire SA et la donnée intermédiaire de référence SR associée à la première donnée d'entrée A sont cohérentes et si la deuxième donnée intermédiaire SB n'est pas cohérente avec la donnée intermédiaire de référence associée à la deuxième donnée d'entrée B, alors la défaillance provient du deuxième module de traitement 16.

Si la première donnée intermédiaire SA et la donnée intermédiaire de référence SR associée à la première donnée d'entrée A sont cohérentes et si la deuxième donnée intermédiaire SB est cohérente avec la donnée intermédiaire de référence associée à la deuxième donnée d'entrée B, alors la défaillance provient de l'un des deux dispositifs électroniques amont 12A, 12B.

Le module de contrôle 22 est, en outre, configuré pour comparer les première et deuxième récompenses RA, RB entre elles afin de détecter une éventuelle incohérence.

En particulier, le module de contrôle 22 calcule une métrique, telle qu'une distance entre les récompenses RA, RB, par exemple la valeur absolue de la différence, et un deuxième seuil de cohérence. Les récompenses RA, RB sont alors cohérentes entre elles si la métrique, telle que la distance entre les valeurs est inférieure au deuxième seuil de cohérence.

Le module de génération 24 est configuré pour générer la donnée de sortie C en fonction des première et deuxième données intermédiaires SA, SB lorsque les première et deuxième données intermédiaires SA, SB appartiennent au domaine de sécurité et en l'absence d'incohérence détectée.

La donnée de sortie C est par exemple égale à l'une des deux données intermédiaires SA, SB. Typiquement, lorsque les première et deuxième données intermédiaires SA, SB appartiennent au domaine de sécurité et en l'absence

d'incohérence détectée, la donnée de sortie C est égale à la première donnée intermédiaire SA.

En variante, lorsque les première et deuxième données intermédiaires SA, SB appartiennent au domaine de sécurité et en l'absence d'incohérence détectée, la donnée de sortie C est égale à la donnée intermédiaire SA, SB associée à la récompense RA, RB la plus élevée calculée par le module de récompense 26.

En variante encore, le module de génération 24 est configuré pour appliquer une formule mathématique aux première et deuxième données intermédiaires SA, SB pour obtenir la donnée de sortie C. Par exemple, le module de génération 24 est configuré pour effectuer une moyenne des données intermédiaires SA, SB.

Si l'une des première et deuxième données intermédiaires SA, SB n'appartient pas au domaine de sécurité et/ou si une incohérence est détectée, la donnée de sortie C est alors égale à la donnée de référence SR.

Le module d'alerte 21 est configuré pour générer un signal d'alerte en fonction de chaque incohérence détectée par le module de contrôle 22 entre les données intermédiaires SA, SB et/ou entre les récompenses RA, RB.

Le signal d'alerte comporte avantageusement une alerte relative à la défaillance des dispositifs électroniques amont 12A, 12B ou de l'un des modules de traitement 14, 16.

Optionnellement, le module d'affichage 23 est configuré pour afficher l'alerte à destination d'un utilisateur du système électronique 10. En particulier, lorsque le système 10 est un système avionique, le module d'affichage 23 est configuré pour afficher l'alerte sur un écran d'affichage tête basse ou un écran d'affichage tête haute devant le pilote qui prend alors en compte la défaillance détectée.

Dans l'exemple de la figure 1, le système électronique 10 comprend une unité de traitement d'informations 50 formée par exemple d'une mémoire 52 et d'un processeur 54 associé à la mémoire 52. Le premier module de traitement 14, le deuxième module de traitement 16, le module de traitement auxiliaire 18 et le dispositif de surveillance 20, et en complément facultatif le module d'alerte 21 et le module d'affichage 23, sont réalisés chacun sous forme d'un logiciel, ou d'une brique logicielle, exécutables par le processeur 54. La mémoire 52 est alors apte à stocker un premier logiciel de traitement, un deuxième logiciel de traitement, un logiciel de traitement auxiliaire et un logiciel de surveillance, et en complément facultatif un logiciel d'alerte et un logiciel d'affichage. Le processeur 54 est alors apte à exécuter chacun de ces logiciels.

En variante non représentée, le premier module de traitement 14, le deuxième module de traitement 16, le module de traitement auxiliaire 18 et le dispositif de surveillance 20, et en complément facultatif le module d'alerte 21 et le module d'affichage

23, sont réalisés chacun sous forme d'un composant logique programmable, tel qu'un FPGA (de l'anglais *Field Programmable Gate Array*), ou encore sous forme d'un circuit intégré dédié, tel qu'un ASIC (de l'anglais *Application Specific Integrated Circuit*). Le premier module de traitement 14, le deuxième module de traitement 16, le module de traitement auxiliaire 18 et le dispositif de surveillance 20 sont alors de préférence embarqués chacun sur un calculateur électronique respectif.

Lorsque le système électronique 10 est réalisé sous forme d'un ou plusieurs logiciels, c'est-à-dire sous forme d'un programme d'ordinateur, il est en outre apte à être enregistré sur un support, non représenté, lisible par ordinateur. Le support lisible par ordinateur est par exemple, un médium apte à mémoriser les instructions électroniques et à être couplé à un bus d'un système informatique. A titre d'exemple, le support lisible est un disque optique, un disque magnéto-optique, une mémoire ROM, une mémoire RAM, tout type de mémoire non-volatile (par exemple EPROM, EEPROM, FLASH, NVRAM), une carte magnétique ou une carte optique. Sur le support lisible est alors mémorisé un programme d'ordinateur comportant des instructions logicielles.

Le fonctionnement du système électronique 10 selon l'invention va désormais être expliqué à l'aide de la figure 3 représentant un organigramme du procédé, selon l'invention, de mise en œuvre d'une fonction critique par le système 10.

Par la suite, un exemple de mise en œuvre du procédé va être décrite pour un système avionique, et l'homme du métier comprendra que ce procédé s'applique plus généralement à tout système électronique 10.

Initialement, l'aéronef est par exemple en train de voler en direction d'un aéroport.

Le système avionique 10 met alors en œuvre une fonction critique avionique, telle qu'un calcul d'une commande de vol de l'aéronef, un calcul d'une trajectoire de vol optimisée selon un critère prédéterminé, tel que la consommation de carburant de l'aéronef, ou encore le calcul d'une stratégie d'évitement d'un obstacle par l'aéronef. Lors d'une première étape de calcul 100, le premier module de traitement 14 calcule la première donnée intermédiaire SA à partir de la première donnée d'entrée A et de l'algorithme d'apprentissage par renforcement, pour la mise en œuvre de la fonction critique pour la première donnée d'entrée A.

Dans l'exemple du calcul d'une commande de vol, la première donnée d'entrée A est notamment une première donnée de localisation de l'aéronef, une première donnée relative à l'état d'un système avionique ou une première donnée relative à la trajectoire à suivre par l'aéronef. Le premier module de traitement 14 calcule alors la première donnée intermédiaire SA, telle qu'une première commande de vol pour l'aéronef, afin de se rapprocher au plus proche d'une trajectoire visée, ceci à partir de cette première donnée

d'entrée A en lui appliquant l'algorithme d'apprentissage par renforcement. La première donnée intermédiaire SA est ainsi représentative d'une première commande de vol pour l'aéronef afin de suivre au mieux la trajectoire visée.

Dans l'exemple du calcul d'une trajectoire optimisée, la première donnée d'entrée A est notamment une première donnée de localisation de l'aéronef, une première donnée relative à l'état de l'aéronef, une première donnée relative à la destination programmée pour l'aéronef. La première donnée intermédiaire SA est alors représentative d'une première trajectoire à suivre.

Dans l'exemple du calcul d'une stratégie d'évitement d'un obstacle, la première donnée d'entrée A est notamment une première donnée de localisation de l'aéronef, une première donnée de localisation de l'obstacle ou une première donnée relative à l'état d'un système avionique. La première donnée intermédiaire SA est alors représentative d'une première stratégie d'évitement à suivre par l'aéronef.

Lors d'une deuxième étape de calcul 110, le deuxième module de traitement 16 calcule la deuxième donnée intermédiaire SB à partir de la deuxième donnée d'entrée B et de l'algorithme d'apprentissage par renforcement, pour la mise en œuvre de la fonction critique pour la deuxième donnée d'entrée B.

Dans l'exemple du calcul d'une commande de vol, la deuxième donnée d'entrée B est notamment une deuxième donnée de localisation de l'aéronef, de préférence issue d'un capteur différent de celui ayant fourni la première donnée de localisation, une deuxième donnée relative à l'état dudit système avionique ou une deuxième donnée relative à la trajectoire à suivre. Le deuxième module de traitement 16 calcule la deuxième donnée intermédiaire SB, telle qu'une deuxième commande de vol pour l'aéronef afin de se rapprocher au plus proche de la trajectoire visée, ceci à partir de cette deuxième donnée d'entrée B en lui appliquant l'algorithme d'apprentissage par renforcement. La deuxième donnée intermédiaire SB est ainsi représentative d'une deuxième commande de vol pour l'aéronef afin de suivre au mieux la trajectoire visée.

Dans l'exemple du calcul d'une trajectoire optimisée, la deuxième donnée d'entrée B est notamment une deuxième donnée de localisation de l'aéronef, une deuxième donnée relative à l'état de l'aéronef, une deuxième donnée relative à la destination programmée pour l'aéronef. La deuxième donnée intermédiaire SB est alors représentative d'une deuxième trajectoire à suivre.

Dans l'exemple du calcul d'une stratégie d'évitement d'un obstacle, la deuxième donnée d'entrée B est notamment une deuxième donnée de localisation de l'aéronef, une deuxième donnée de localisation de l'obstacle ou une deuxième donnée relative à l'état

d'un système avionique. La deuxième donnée intermédiaire SB est alors représentative d'une deuxième stratégie d'évitement à suivre par l'aéronef.

Lors d'une troisième étape de calcul 120, le module de traitement auxiliaire 18 calcule la donnée intermédiaire de référence SR à partir de la première donnée d'entrée A et/ou de la deuxième donnée d'entrée B et de l'algorithme de référence, pour la mise en œuvre de la fonction critique via l'algorithme de référence pour la première donnée d'entrée A et/ou la deuxième donnée d'entrée B.

Par exemple, le module de traitement auxiliaire 18 calcule la donnée intermédiaire de référence SR, telle qu'une troisième commande de vol pour l'aéronef afin de se rapprocher au plus proche de la trajectoire visée, une troisième trajectoire à suivre ou une troisième stratégie d'évitement, ceci à partir de la première donnée d'entrée A et/ou de la deuxième donnée d'entrée B en lui ou en leur appliquant l'algorithme de référence.

Dans l'exemple du calcul d'une commande de vol, l'algorithme de référence est par exemple un modèle physique simplifié fournissant une formule déterministe donnant la commande de vol en fonction de l'écart entre la trajectoire de l'aéronef et la trajectoire visée.

Dans l'exemple du calcul d'une trajectoire optimisée, l'algorithme de référence est par exemple un modèle physique simplifié fournissant une formule déterministe donnant une trajectoire à faible consommation de carburant en fonction de la position de l'aéronef et de sa destination.

Dans l'exemple du calcul d'une stratégie d'évitement d'un obstacle, l'algorithme de référence est par exemple un modèle physique simplifié fournissant une formule déterministe donnant une stratégie d'évitement en fonction de la position de l'aéronef et la position de l'obstacle.

Les étapes de calcul 100, 110 et 120 sont réalisées indépendamment l'une de l'autre, en même temps ou bien successivement dans un ordre quelconque.

Le dispositif de surveillance 20 reçoit les première et deuxième données intermédiaires SA, SB puis vérifie, lors d'une étape de contrôle 130, si les première et deuxième données intermédiaires SA, SB appartiennent au domaine de sécurité et compare les première et deuxième données intermédiaires SA, SB entre elles afin de détecter une éventuelle incohérence.

A titre d'exemple, si la commande de vol est une consigne de vitesse, le domaine de sécurité est alors notamment un intervalle de vitesse associé. Si la commande de vol est une consigne d'altitude, le domaine de sécurité est alors un intervalle d'altitude. Si la commande de vol est une commande moteur, le domaine de sécurité est alors notamment un intervalle de puissance moteur. Si la commande de vol est une commande

de direction, le domaine de sécurité est par exemple une limite de changement de direction de l'aéronef, etc.

En outre, deux commandes de vol sont par exemple détectées comme étant incohérentes entre elles, si les trajectoires associées à ces deux commandes présentent un écart spatial supérieur à une distance seuil prédéterminée.

Lorsque les première et deuxième données intermédiaires SA, SB appartiennent au domaine de sécurité et en l'absence d'incohérence détectée, le dispositif de surveillance 20 délivre la donnée de sortie C en fonction des première et deuxième données intermédiaires SA, SB lors d'une étape de génération 140.

Par exemple, la donnée de sortie C est égale à la première commande de vol ou est égale à la moyenne entre les première et deuxième commandes de vol.

Si une incohérence est détectée, le dispositif de surveillance 20 délivre alors la donnée de sortie C égale à la donnée de référence SR lors de l'étape de génération 140. En outre, le module d'alerte 21 génère un signal d'alerte lors d'une étape d'alerte 150 et, optionnellement, lors d'une étape d'affichage 160, le module d'affichage 25 affiche l'alerte à destination d'un utilisateur du système électronique 10, notamment du pilote de l'aéronef.

Lors d'une étape de récompense 170, le module de récompense 26 reçoit les première et deuxième données intermédiaires SA, SB et calcule une première récompense RA associée à la mise en œuvre de la fonction critique par le premier module de traitement 14 et une deuxième récompense RB associée à la mise en œuvre de la fonction critique par le deuxième module de traitement 16.

Dans l'exemple du calcul d'une commande de vol, plus la distance entre la trajectoire calculée et la trajectoire visée est proche, plus la récompense est élevée.

Dans l'exemple du calcul d'une trajectoire optimisée, la récompense est calculée en fonction de la consommation de carburant réel mesurée. Plus la consommation est faible, plus la récompense est alors élevée.

Dans l'exemple du calcul d'une stratégie d'évitement d'un obstacle, la récompense est calculée après l'évitement de l'obstacle en fonction de l'écart minimal en distance entre l'aéronef et l'obstacle. Plus cet écart de distance est élevé, plus la récompense est également élevée.

Le module de récompense 26 envoie la première récompense RA et respectivement la deuxième récompense RB au premier et respectivement deuxième module de traitement 14, 16.

A la prochaine itération de la première étape de calcul 100, le premier module de traitement 14 reçoit la première récompense RA et modifie la première pluralité de

paramètres algorithmiques afin de maximiser la prochaine première récompense RA reçue, et ainsi par exemple calculer une trajectoire plus proche de la trajectoire visée.

A la prochaine itération de la deuxième étape de calcul 110, le deuxième module de traitement 16 reçoit la deuxième récompense RB et modifie la deuxième pluralité de paramètres algorithmiques afin de maximiser la prochaine deuxième récompense RB reçue, et ainsi par exemple calculer une trajectoire consommant moins de carburant ou une stratégie d'évitement plus efficace.

On conçoit alors que la présente invention présente un certain nombre d'avantages.

En effet, la mise en œuvre de la fonction critique par les premier et deuxièmes modules de traitement 14, 16 via l'algorithme d'apprentissage par renforcement permettent d'améliorer la performance du système 10 durant son exploitation. En effet, un tel algorithme permet de s'adapter à des évènements nouveaux et inattendus rencontrés par le système électronique 10 lors de son exploitation.

En outre, la comparaison entre ces deux données intermédiaires SA, SB issues de deux données d'entrée différentes et la vérification de l'appartenance au domaine de sécurité permet de détecter une éventuelle incohérence et de fournir le cas échéant une donnée de sortie C égale à la donnée intermédiaire de référence SR appartenant au domaine de sécurité, et ainsi de garantir la sécurité du système 10 même en cas d'incohérence détectée.

Enfin, le système 10 selon l'invention permet d'alerter le cas échéant l'utilisateur d'une défaillance due aux données d'entrées ou bien à la mise en œuvre des algorithme d'apprentissage par renforcement.

Ainsi, l'invention permet d'obtenir un système électronique 10 performant tout en étant suffisamment sûr, notamment au regard des exigences de sécurité dans le domaine avionique.

REVENDICATIONS

1. Système électronique (10) configuré pour mettre en œuvre une fonction critique, le système électronique (10) étant propre à recevoir des première et deuxième données d'entrée (A, B) et à délivrer une donnée de sortie (C) associée à ladite fonction critique, la donnée de sortie (C) étant associée à un domaine de sécurité prédéterminé, le domaine de sécurité étant en forme d'une plage de valeurs prédéfinies,

le système électronique (10) comprenant :

- un premier module de traitement (14) configuré pour calculer une première donnée intermédiaire (SA) à partir de la première donnée d'entrée (A) et d'un algorithme d'apprentissage par renforcement, pour la mise en œuvre de la fonction critique pour la première donnée d'entrée (A),

- un deuxième module de traitement (16) configuré pour calculer une deuxième donnée intermédiaire (SB) à partir de la deuxième donnée d'entrée (B) et de l'algorithme d'apprentissage par renforcement, pour la mise en œuvre de la fonction critique pour la deuxième donnée d'entrée (B), la deuxième donnée d'entrée (B) étant différente de la première donnée d'entrée (A),

- un module de traitement auxiliaire (18) configuré pour calculer une donnée intermédiaire de référence (SR) à partir de la première donnée d'entrée (A) et/ou de la deuxième donnée d'entrée (B) et d'un algorithme de référence différent de l'algorithme d'apprentissage par renforcement, pour la mise en œuvre de la fonction critique pour la première donnée d'entrée (A) et/ou la deuxième donnée d'entrée (B) via l'algorithme de référence,

- un dispositif de surveillance (20) comportant :

  + un module de contrôle (22) configuré pour vérifier si les première et deuxième données intermédiaires (SA, SB) appartiennent au domaine de sécurité et pour comparer les première et deuxième données intermédiaires (SA, SB) entre elles afin de détecter une éventuelle incohérence;

  + un module de génération (24) configuré pour générer la donnée de sortie (C) en fonction des première et deuxième données intermédiaires (SA, SB) si les première et deuxième données intermédiaires (SA, SB) appartiennent au domaine de sécurité et si aucune incohérence n'est détectée, la donnée de sortie (C) étant égale à la donnée intermédiaire de référence (SR) sinon.

2. Système (10) selon la revendication 1, dans lequel l'ensemble des mises en œuvre de la fonction critique par l'algorithme de référence définit un domaine d'arrivée de l'algorithme de référence, le domaine d'arrivée étant inclus dans le domaine de sécurité.

3. Système (10) selon la revendication 1 ou 2, dans lequel le dispositif de surveillance (20) comporte un module de récompense (26) configuré pour calculer une première récompense (RA) pour la mise en œuvre de la fonction critique par le premier module de traitement (14) et une deuxième récompense (RB) pour la mise en œuvre de la fonction critique par le deuxième module de traitement (16),

le premier module de traitement (14) étant configuré pour mettre en œuvre l'algorithme d'apprentissage par renforcement en fonction d'une première pluralité de paramètres algorithmiques, le premier moule de traitement (14) étant configuré, à chaque itération, pour recevoir la première récompense (RA) et pour modifier la première pluralité de paramètres algorithmiques en fonction de la première récompense reçue (RA) afin de maximiser la prochaine première récompense (RA) reçue,

le deuxième module de traitement (14) étant configuré pour mettre en œuvre l'algorithme d'apprentissage par renforcement en fonction d'une deuxième pluralité de paramètres algorithmiques, le deuxième module de traitement (16) étant configuré, à chaque itération, pour recevoir la deuxième récompense (RB) et pour modifier la deuxième pluralité de paramètres algorithmiques en fonction de la deuxième récompense reçue (RB) afin de maximiser la prochaine deuxième récompense (RB) reçue.

4. Système (10) selon la revendication 3, dans lequel le module de récompense (26) est configuré pour pénaliser chaque première récompense (RA) et/ou respectivement chaque deuxième récompense (RB) lorsque la première donnée intermédiaire (SA) et/ou respectivement la deuxième donnée intermédiaire (SB) n'appartiennent pas au domaine de sécurité.

5. Système (10) selon les revendications 3 ou 4, dans lequel, lorsque les première et deuxième données intermédiaires (SA, SB) appartiennent au domaine de sécurité et en l'absence d'incohérence détectée, le module de génération (24) est configuré pour délivrer, en donnée de sortie, la donnée intermédiaire associée à la récompense (RA, RB) la plus élevée calculée par le module de récompense (26).

6. Système (10) selon l'une quelconque des revendications précédentes, dans lequel le module de contrôle (22) est en outre configuré pour comparer les première et deuxième récompenses (RA, RB) entre elles afin de détecter une éventuelle incohérence,

et dans lequel le système électronique (10) comprend en outre un module d'alerte (21) configuré pour générer un signal d'alerte en fonction de chaque incohérence entre les données intermédiaires (SA, SB) et/ou entre les récompenses (RA, RB).

7. Système (10) selon l'une quelconque des revendications 3 à 5, dans lequel le module de contrôle (22) est configuré en outre pour comptabiliser le nombre de fois où respectivement les première et deuxième données intermédiaires (SA, SB) ne respectent pas le domaine de sécurité et pour réinitialiser respectivement la première pluralité de paramètres algorithmiques et la deuxième pluralité de paramètres algorithmiques lorsque ledit nombre est supérieur à un seuil prédéterminé.

8. Système (10) selon l'une quelconque des revendications précédentes, dans lequel le système (10) est un système avionique propre à être embarqué dans un poste de commande d'un aéronef, notamment un système de navigation de l'aéronef.

9. Procédé de mise en œuvre d'une fonction critique par un système électronique (10), le système électronique (10) étant configuré pour mettre en œuvre une fonction critique, le système électronique (10) étant propre à recevoir des première et deuxième données d'entrée (A,B) et à délivrer une donnée de sortie (C) associée à ladite fonction critique, la donnée de sortie (C) étant associée à un domaine de sécurité prédéterminé, le domaine de sécurité étant en forme d'une plage de valeur(s) prédéfinie(s),

le procédé comprenant les étapes suivantes :

- calcul (100) d'une première donnée intermédiaire (SA) à partir de la première donnée d'entrée (A) et d'un algorithme d'apprentissage par renforcement, pour la mise en œuvre de la fonction critique pour la première donnée d'entrée (A),
- calcul (110) d'une deuxième donnée intermédiaire (SB) à partir de la deuxième donnée d'entrée (B) et de l'algorithme d'apprentissage par renforcement, pour la mise en œuvre de la fonction critique pour la deuxième donnée d'entrée (B), la deuxième donnée d'entrée (B) étant différente de la première donnée d'entrée (A),
- calcul (120) d'une donnée intermédiaire de référence (SR) à partir de la première donnée d'entrée (A) et/ou de la deuxième donnée d'entrée (B) et d'un algorithme de référence différent de l'algorithme d'apprentissage par renforcement, pour la mise en

œuvre de la fonction critique pour la première donnée d'entrée (A) et/ou la deuxième donnée d'entrée (B) via l'algorithme de référence,

- vérification (130) si les première et deuxième données intermédiaires (SA, SB) appartiennent au domaine de sécurité et comparaison des première et deuxième données intermédiaires (SA, SB) entre elles afin de détecter une éventuelle incohérence;

- génération (140) de la donnée de sortie (C) en fonction des première et deuxième données intermédiaires (SA, SB) si les première et deuxième données intermédiaires (SA, SB) appartiennent au domaine de sécurité et si aucune incohérence n'est détectée, la donnée de sortie (C) étant égale à la donnée de référence (SR) sinon.

10. Programme d'ordinateur comportant des instructions logicielles qui, lorsqu'elles sont exécutées par un ordinateur, mettent en œuvre un procédé selon la revendication précédente.

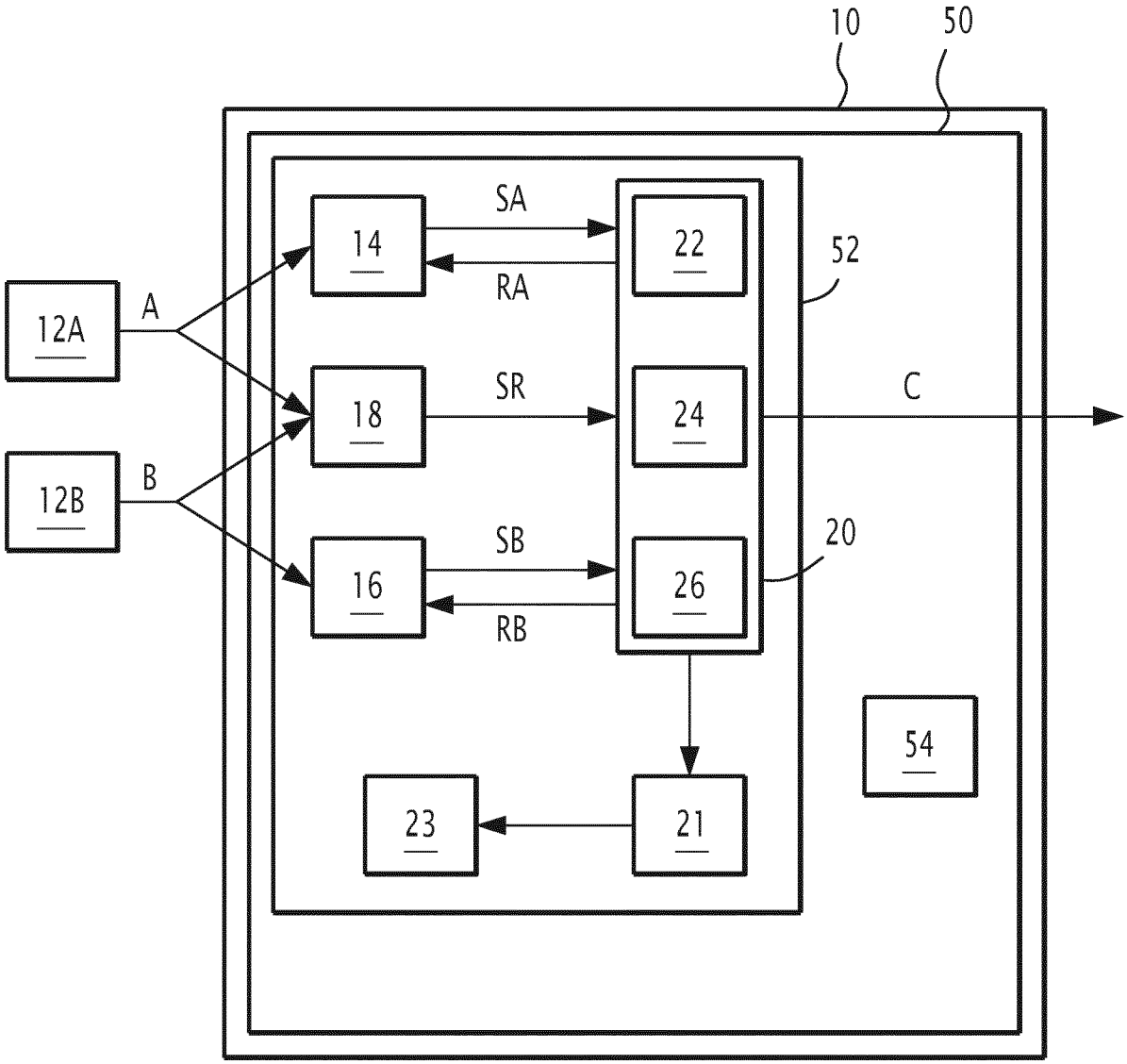


FIG.1

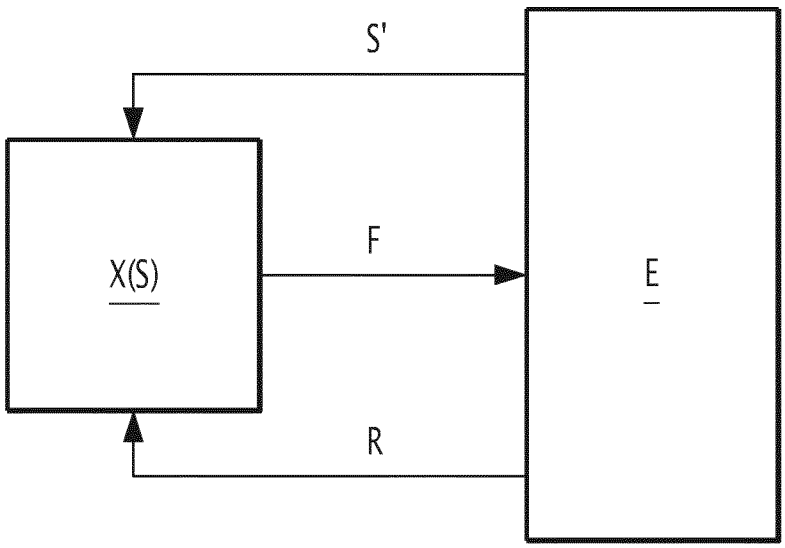


FIG.2

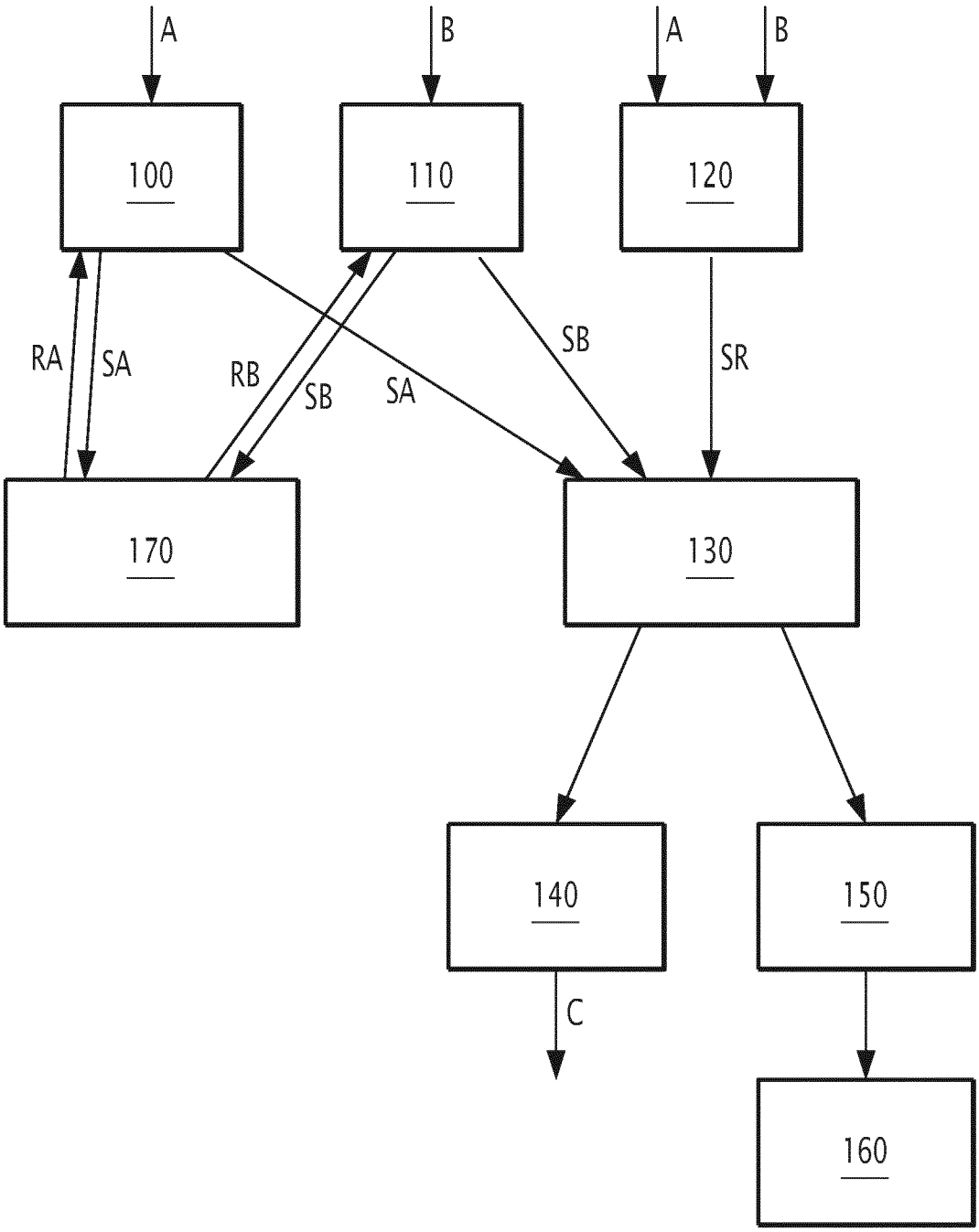


FIG.3

INTERNATIONAL SEARCH REPORT

International application No.
PCT/EP2021/079761

A. CLASSIFICATION OF SUBJECT MATTER

G05B 23/02(2006.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G05B

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP 3506096 A1 (THALES SA [FR]) 03 July 2019 (2019-07-03) the whole document	1-10
A	FR 3077666 A1 (PSA AUTOMOBILES SA [FR]) 09 August 2019 (2019-08-09) the whole document	1-10

☐ Further documents are listed in the continuation of Box C.

☑ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
18 January 2022	**31 January 2022**

Name and mailing address of the ISA/EP

European Patent Office
p.b. 5818, Patentlaan 2, 2280 HV Rijswijk
Netherlands

Telephone No. **(+31-70)340-2040**
Facsimile No. **(+31-70)340-3016**

Authorized officer

Fulcheri, Alessandro

Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/EP2021/079761

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
EP 3506096 A1	03 July 2019	CA 3027277 A1	26 June 2019
		CN 110058972 A	26 July 2019
		EP 3506096 A1	03 July 2019
		FR 3075997 A1	28 June 2019
		US 2019196927 A1	27 June 2019
FR 3077666 A1	09 August 2019	NONE	

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale n°
PCT/EP2021/079761

A. CLASSEMENT DE L'OBJET DE LA DEMANDE

INV. G05B23/02
ADD.

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
G05B

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si cela est réalisable, termes de recherche utilisés)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie*	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	EP 3 506 096 A1 (THALES SA [FR]) 3 juillet 2019 (2019-07-03) le document en entier -----	1-10
A	FR 3 077 666 A1 (PSA AUTOMOBILES SA [FR]) 9 août 2019 (2019-08-09) le document en entier -----	1-10

☐ Voir la suite du cadre C pour la fin de la liste des documents

☒ Les documents de familles de brevets sont indiqués en annexe

* Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent
"E" document antérieur, mais publié à la date de dépôt international ou après cette date
"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)
"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens
"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée
"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention
"X" document particulièrement pertinent;; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément
"Y" document particulièrement pertinent;; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier
"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
18 janvier 2022	31/01/2022

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Fulcheri, Alessandro

Formulaire PCT/ISA/210 (deuxième feuille) (avril 2005)

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Demande internationale n°

PCT/EP2021/079761

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
EP 3506096 A1	03-07-2019	CA 3027277 A1	26-06-2019
		CN 110058972 A	26-07-2019
		EP 3506096 A1	03-07-2019
		FR 3075997 A1	28-06-2019
		US 2019196927 A1	27-06-2019
FR 3077666 A1	09-08-2019	AUCUN	