(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

COURBEVOIE

(11) **N° de publication :** ***3 135 062***

(à n'utiliser que pour les commandes de reproduction)

(21) **N° d'enregistrement national :** **22 04073**

(51) Int Cl[8] : ***H 04 L 9/00*** *(2024.01), H 04 W 4/42, B 64 F 1/36*

(12) **BREVET D'INVENTION** **B1**

(54) Passerelle de sécurité réseau embarquée à bord d'un aéronef pour connecter des domaines de confiance basse et haute d'une infrastructure informatique avionique.

(22) **Date de dépôt :** 29.04.22.

(30) **Priorité :**

(43) **Date de mise à la disposition du public de la demande :** 03.11.23 Bulletin 23/44.

(45) **Date de la mise à disposition du public du brevet d'invention :** 20.12.24 Bulletin 24/51.

(56) **Liste des documents cités dans le rapport de recherche :**

Se reporter à la fin du présent fascicule

(60) **Références à d'autres documents nationaux apparentés :**

◯ **Demande(s) d'extension :**

(71) **Demandeur(s) :** *THALES Société anonyme* — FR.

(72) **Inventeur(s) :** MONNIER Stéphane, NOINSKI Alexandre et FINE Alexandre.

(73) **Titulaire(s) :** THALES Société anonyme.

(74) **Mandataire(s) :** Lavoix.

FR 3 135 062 - B1

Description

Titre de l'invention : Passerelle de sécurité réseau embarquée à bord d'un aéronef pour connecter des domaines de confiance basse et haute d'une infrastructure informatique avionique.

[0001] La présente invention a pour domaine celui des passerelles de sécurité réseau destinées à être embarquées à bord d'aéronefs, civils ou militaires.

[0002] Une passerelle de sécurité réseau permet une interconnexion entre deux domaines informatiques qui sont caractérisés par des niveaux de criticité différents, en particulier entre un domaine de faible confiance et un domaine critique pour la sécurité (concept de « safety » en anglais) de l'aéronef, comme par exemple le domaine de contrôle de l'avion - ACD (« Aircraft Control Domain »).

[0003] Cette interconnexion peut être permanente, dans le cas par exemple de deux réseaux de l'avion mis à contribution durant une phase de vol, ou temporaire, dans le cas par exemple d'un équipement de maintenance connecté à l'avion durant une phase de maintenance au sol.

[0004] La passerelle permet de protéger le domaine de plus haute criticité en filtrant les flux de données provenant du domaine de plus faible criticité, en en rejetant les flux de données qui ne sont pas compatibles avec le niveau de criticité le plus haut, notamment les flux de données correspondant à des attaques informatiques malveillantes.

[0005] Une telle passerelle doit être développée avec le plus haut niveau de développement pour la sécurité (niveau « SAL 3 » dans le référentiel défini par la norme ED-203A) tout en assurant de bonnes propriétés de cyber-sécurité, notamment l'impossibilité pour un attaquant de contourner les fonctions de filtrage mises en œuvre par la passerelle.

[0006] Cependant, le respect de telles exigences de développement ainsi que la vérification permettant de garantir le niveau de sécurité effectivement fourni constituent des difficultés majeures.

[0007] Le but de la présente invention est de proposer une architecture de passerelle permettant de répondre à ces problèmes.

[0008] Pour cela l'invention a pour objet une passerelle de sécurité réseau destinée à être embarquée à bord d'un aéronef pour connecter un domaine de confiance basse et un domaine de confiance haute d'une infrastructure informatique avionique, la passerelle offrant une pluralité de fonctions de sécurité, chaque fonction étant réalisée par un nœud de traitement de données, la passerelle comportant, connectés en série le long d'une chaîne de filtrage d'un flux de données reçu depuis le domaine de confiance basse : un nœud de traitement de données de pare-feu ; un nœud de traitement de

données de rupture protocolaire ; un nœud de traitement de données maître ; et un nœud de traitement de données de rupture protocolaire inverse, la passerelle comportant en outre un nœud de service relié à chacun des nœuds de traitement de données de la chaîne de filtrage, les différents nœuds de traitement de données étant ségrégés physiquement.

[0009] Suivant des modes particuliers de réalisation, la passerelle comporte une ou plusieurs des caractéristiques suivantes, prises isolément ou suivant toutes les combinaisons techniquement possibles :

[0010] - les nœuds de la chaîne de filtrage sont connectés par des liaisons bidirectionnelles , de préférence au format Ethernet, de préférence encore au format Ethernet 1 Gbit/ s, présentant une bande passante supérieure à celle des connexions permettant de connecter la passerelle aux domaines de confiance haute et basse.

[0011] - le nœud de service est connecté à la pluralité de nœuds de la chaîne de filtrage par des liaisons unidirectionnelles, de préférence au format série, de préférence encore au format série synchronisé.

[0012] - la passerelle constitue une interface Ethernet et/ou ARINC 429 et/ou ARINC 664, avec le domaine de confiance haute et une interface Ethernet et/ou ARINC 429 et/ou ARINC 664 avec le domaine de confiance basse.

[0013] - le un nœud de traitement de données de pare-feu est connecté au domaine de confiance basse par un premier module de conversion, réalisant une conversion d'un format d'un flux de données provenant du domaine de confiance basse, de préférence le format ARINC 429, en un format de données attendu par le nœud de traitement de données de pare-feu.

[0014] - le un nœud de traitement de rupture protocolaire inverse est connecté au domaine de confiance haute par un second module de conversion, réalisant une conversion d'un format d'un flux de données délivré par le nœud de traitement de rupture protocolaire inverse, de préférence le format Ethernet 100 Mbit/s, en un format attendu par le domaine de confiance basse, de préférence le format ARINC 664, de préférence encore ARINC 664 P3 ou P7.

[0015] - le nœud de traitement de données maître filtre un flux de données en fonction d'un contexte ou en fonction d'un niveau de priorité.

[0016] le nœud de traitement de données maître exécute une application de détection d'intrusion et les informations de détection générées par ladite application sont adressées au nœud de service en tant qu'entrées d'un fichier de journalisation.

[0017] - tout flux de données provenant du domaine de confiance basse passe par le nœud de traitement de données maître, à condition de n'avoir pas été rejeté par le nœud de traitement de données de pare-feu ou le nœud de traitement de données de rupture protocolaire.

[0018] - outre son interface avec le domaine de confiance basse, le nœud de traitement de données de pare-feu ne comporte qu'un port de sortie forçant l'acheminement de tout flux de données opérationnelles provenant du domaine de confiance basse vers le nœud de traitement de données de rupture protocolaire, et dans laquelle, outre son interface avec le nœud de traitement de données de pare-feu, le nœud de traitement de données de rupture protocolaire ne comporte qu'un port de sortie forçant l'acheminement de tout flux de données opérationnelles provenant du domaine de confiance basse vers le nœud de traitement de données maître.

[0019] - tout flux de données provenant du domaine de confiance haute et à destination du domaine de confiance basse et qui ne passe pas par le nœud de traitement de données maître est acheminé à travers la passerelle via au moins une liaison unidirectionnelle.

[0020] - la passerelle ne comporte qu'un seul nœud de traitement de données de pare-feu situé en entrée de la chaine de filtrage du côté du domaine de confiance basse.

[0021] L'invention et ses avantages seront mieux compris à la lecture de la description détaillée qui va suivre d'un mode de réalisation particulier, donné uniquement à titre d'exemple non limitatif, cette description étant faite en se référant aux dessins annexés sur lesquels :

[0022] [Fig.1] La [Fig.1] est une représentation schématique d'un mode de réalisation préféré de la passerelle de sécurité avionique selon l'invention ; et,

[0023] [Fig.2] La [Fig.2] est un chronogramme représentant différents exemples de fonctionnement de la passerelle de la [Fig.1].

STRUCTURE

[0024] En se référant à la [Fig.1], l'architecture de la passerelle selon l'invention va être présentée. Sur cette figure, les liaisons bidirectionnelles sont en traits pleins tandis que les liaisons unidirectionnelles sont en traits pointillés.

[0025] La passerelle de sécurité réseau 10 est embarquée à bord d'un aéronef. Elle est placée à l'interface entre un domaine de confiance basse 12, ou domaine « LTD », et un domaine de confiance haute 13, ou domaine « HTD », d'une infrastructure informatique avionique. Par exemple le domaine 13 correspond au domaine de contrôle de l'avion et le domaine 12 correspond à un autre domaine à bord de l'aéronef ou connecté temporairement à l'aéronef.

[0026] La passerelle 10 a pour fonction d'assurer un transfert sécurisé des données au moins du domaine de confiance basse 12 vers le domaine de confiance haute 13. Pour cela, la passerelle 10 filtre les flux de données, tout en étant robuste aux attaques informatiques cherchant à contourner ce filtrage.

[0027] De préférence, la passerelle 10 est une passerelle Ethernet / Ethernet. Alternativement, il s'agit d'une passerelle ARINC 429 / ARINC 429. Plus généralement, il s'agit d'une passerelle Ethernet et/ou ARINC 429 et/ou ARINC 664

(de préférence ARINC 664 P3 ou P7) côté domaine de confiance basse et Ethernet et/ ou ARINC 429 et/ou ARINC 664 (de préférence ARINC 664 P3 ou P7) côté domaine de confiance haute.

[0028] L'architecture de la passerelle 10 est de préférence fondée sur une unique carte électronique 11 portant plusieurs nœuds de traitement de données (ou « Data Processing Node » en anglais), chaque nœud étant dédié à la réalisation d'une ou plusieurs fonctions de sécurité spécifiques. Il s'agit donc d'une architecture distribuée.

[0029] Un nœud peut être tout type de dispositif disposant de ses propres ressources de calcul, mémoire, et port de communication. De préférence, il s'agit d'un microcontrôleur, dans la mesure où un tel composant présente une consommation réduite, ce qui par conséquent limite les problèmes de dissipation de chaleur, question critique dans le domaine avionique. Alternativement, il s'agit d'un circuit logique programmable, comme par exemple un FPGA (« Field-Programmable Gate Array »).

[0030] Les différentes fonctions sont par conséquent ségrégées physiquement.

[0031] La carte 11 porte ainsi un nœud maître 1. Le nœud maître 1 réalise la fonction de filtrage en tant que telle.

[0032] La carte 11 porte également plusieurs nœuds esclaves. Dans le mode de réalisation de la [Fig.1], quatre nœuds esclaves sont prévus, numérotés 2, 4, 5 et 6. Ils réalisent des fonctions respectivement de sécurité, de pare-feu, de formatage et de formatage inverse.

[0033] La carte 11 porte également une pluralité de dispositifs de conversion. Dans le mode de réalisation de la [Fig.1], trois dispositifs de conversion sont prévus, numérotés 3, 7 et 8.

[0034] Ces nœuds et dispositifs de conversion communiquent entre eux par des liaisons.

[0035] Les nœuds de traitement de données de pare-feu 4, de formatage 5, maître 1, et de rupture protocolaire inverse 6 sont connectés en série pour former une chaîne de filtrage des flux de données.

[0036] Le nœud de service 2 est relié à chacun des nœuds de traitement de données de la chaîne de filtrage.

[0037] Le nœud maître 1 est ainsi « enfoui » au cœur de la carte 11, au sens où il ne présente aucune interface directe avec l'un ou l'autre des domaines 12 et 13.

[0038] L'architecture de la passerelle est telle qu'un flux de données provenant du domaine de confiance basse 12 est contraint de passer successivement à travers les nœuds de pare-feu 4, de formatage 5 et maître 1. Cette contrainte est réalisée physiquement au moyen des liaisons de communication entre ces nœuds : l'unique canal de communication opérationnelle sortant du nœud 4 (hors de l'interface vers le domaine de confiance basse) amène au nœud 5 et l'unique canal de communication opérationnelle sortant du nœud 5 (hors de l'interface vers le nœud 4) amène au nœud 1.

[0039] Côté niveau de confiance basse de la passerelle (c'est-à-dire les nœuds 4, 5 et 1), il y a bien des canaux de communication entre chacun des nœuds 4, 5 et 1 d'une part et le nœud 2 d'autre part, mais ces canaux, le long des liaisons U42, U52 et U12, permettent uniquement la remontée d'informations de fonctionnement générées par un nœud vers un fichier de journalisation (fichier « log ») mémorisé par le nœud 2.

[0040] Pour la communication entre une application du domaine de confiance basse 12 et un service du nœud 2 (comme une application de contrôle exploitant le fichier de journalisation mémorisé par le nœud 2), les communications montantes d'interrogation sont reçues par le nœud 1 puis transmises après filtrage vers le nœud 2 via la liaison B12, et les communications descendantes de réponse sont transmises par le nœud 2 soit vers le nœud 1 via la liaison B12 (cas par exemple d'un filtrage contextuel mis en œuvre par le nœud 1), soit directement vers le nœud 4 via la liaison U24 (pour communiquer directement et par conséquent plus rapidement avec le domaine 12).

Nœud de pare-feu 4

[0041] Le nœud de pare-feu 4 est positionné en frontal avec le domaine de confiance basse 12 d'où peuvent provenir les attaques informatiques.

[0042] Il présente au moins un port d'entrée/sortie pour l'établissement d'une liaison bidirectionnelle avec le domaine 12. De préférence, il comporte trois ports permettent d'établir :

[0043] - une première liaison B4a, directe avec le domaine 12, par exemple un réseau de l'avion durant une phase de vol. Il s'agit par exemple d'une liaison Ethernet 100 Mbit/s ;

[0044] - une seconde liaison B4b, directe avec le domaine 12, par exemple de connexion à un équipement de maintenance durant une phase de maintenance au sol. Il s'agit par exemple d'une liaison Ethernet 100 Mbit/s;

[0045] - une troisième liaison B34, indirecte avec le domaine 12, via le premier module de conversion 3.

[0046] Le premier module de conversion 3 permet de convertir un flux de données provenant du domaine 12, par exemple au format ARINC 429, en un flux de données au format requis sur le liaison B34. La liaison B34 est par exemple un bus SPI ou une liaison série asynchrone.

[0047] Le premier module 3 est lui-même connecté directement au domaine 12 par une liaison bidirectionnelle B3, par exemple constituée de deux liaisons unidirectionnelles pour assurer la bidirectionnalité.

[0048] Le nœud de pare-feu 4 présente également un port d'entrée/sortie pour l'établissement d'une liaison B45, bidirectionnelle, avec le nœud de déformatage 5.

[0049] Le nœud de pare-feu 4 présente un port de sortie pour l'établissement d'une liaison U42, unidirectionnelle, avec le nœud de service 2.

[0050] Le nœud de pare-feu 4 présente un port d'entrée pour l'établissement d'une liaison U24, unidirectionnelle, avec le nœud de service 2.

[0051] Le nœud de pare-feu 4 présente un port d'entrée pour l'établissement d'une liaison U64, unidirectionnelle, avec le nœud de reformatage 6.

[0052] Ce premier nœud 4 dans la chaîne de filtrage des données assure un premier niveau de filtrage de type pare-feu (« firewall » en anglais). Il exécute différentes règles de vérification de sécurité sur les flux de données reçus du domaine 12.

[0053] Si le flux de donnée provenant du domaine 12 est accepté par le nœud 4, il est réémis vers le nœud 5.

[0054] En revanche, si le flux est rejeté, le nœud 4 génère des informations de journalisation et les transmet au nœud de service 2.

[0055] Le nœud de pare-feu 4 réalise par exemple les filtrages suivants :

[0056] - n'accepter un flux du domaine de confiance basse que s'il est déclaré, par exemple qu'il comporte l'identifiant d'un port UDP déclaré ;

[0057] - vérifier la taille des trames du flux du domaine de confiance basse, cette taille devant être conforme à des valeurs configurables (taille minimale / taille maximale) ;

[0058] - vérifier que, pour un flux donné, la fréquence de réception des trames est conforme à des valeurs qui sont également configurables ;

[0059] - vérifier que l'adresse IP de la source du flux est conforme à une liste de valeurs autorisée, cette liste étant configurable.

[0060] Au cas où le module 4 rejette une trame du flux, les informations de l'entête de cette trame sont envoyées vers le module de service 2. Une agrégation des informations d'entête est avantageusement réalisée par le module 4 lorsqu'un trop grand nombre de trames sont rejetées.

Nœud de formatage 5

[0061] Le nœud 5 est positionné entre le nœud 4 et le nœud maître 1 dans la chaîne de filtrage des données.

[0062] Il présente un port d'entrée/sortie pour l'établissement de la liaison B45, bidirectionnelle, avec le nœud 4 et un port d'entrée/sortie pour l'établissement d'une liaison B51, bidirectionnelle, avec le nœud maître 1.

[0063] Le nœud 5 présente un port de sortie pour l'établissement d'une liaison U52, unidirectionnelle, vers le nœud de service 2.

[0064] Le nœud 5 assure un deuxième niveau de filtrage en réalisant une modification du format des flux.

[0065] Ainsi, pour un flux de données provenant du domaine de confiance basse, le module 5 réalise une rupture protocolaire. Il détermine la nature du flux incident, c'est-à-dire son format. Par exemple le flux de données est relatif à un plan de vol ou encore au téléchargement d'un logiciel. Le nœud 5 convertit ensuite ce flux incident dans un

format neutre. Si la rupture protocolaire est réussie (dans le sens où le message contenu dans le flux de données incident est cohérent, sans erreur de syntaxe), le flux est réémis, dans ce format neutre, vers le nœud maître 1. En revanche, si le flux incident est rejeté, le nœud 5 génère de nouvelles entrées de journalisation et les transmet au nœud de service 2 via la liaison U52.

[0066] Pour un flux de données provenant du domaine de confiance haute, le module 5 réalise une rupture protocolaire inverse. Il reçoit un flux de données dans le format neutre depuis le nœud maître 1. Il convertit ce flux dans le format requis avant de le transmettre au nœud de pare-feu 4.

[0067] Le format neutre n'est pas standardisé et dépend des implémentations.

Nœud maître 1

[0068] Dans la chaîne de filtrage des données, le nœud maître 1 est positionné entre le nœud de déformatage 5 et le nœud de reformatage 6.

[0069] Il présente un port d'entrée/sortie pour l'établissement d'une liaison B51 bidirectionnelle avec le nœud 5 et un port d'entrée/sortie pour l'établissement d'une liaison B16 bidirectionnelle avec le nœud 6.

[0070] Il présente, de plus, un port de sortie pour l'établissement d'une liaison U12 unidirectionnelle avec le nœud de service 2.

[0071] Le nœud maître 1 effectue différents filtrages.

[0072] Par exemple, le nœud maître réalise un filtrage de type domaine d'usage, où chaque donnée présentée dans le format neutre de la rupture protocolaire est filtrée par rapport à la valeur qu'elle est censée représenter. Par exemple : filtrer un champ de type texte en éliminant certains caractères spéciaux ; filtrer un champ vitesse par rapport aux valeurs potentiellement atteintes par l'aéronef ; interdire des flux de certaine nature en fonction des phases de l'aéronef (vol, roulage au sol, maintenance au sol, etc.), où telle ou telle donnée n'a pas raison d'être.

[0073] Par exemple encore, le nœud maître 1 applique un filtrage rapide ou un filtrage lent de manière à respecter un temps de latence adapté à la nature du flux incident, telle qu'identifiée par le nœud 5. Cela permet de limiter le temps de traversée de certains flux dits critiques. Le nœud maître 1 priorise ainsi les flux critiques en assurant un traitement dans une tache dédiée, les autres flux, non critiques, étant traités dans une tache générale.

[0074] Par exemple encore, le nœud maître 1 applique un filtrage contextuel. Par exemple si un premier message de requête circule du domaine 13 vers le domaine 12, le nœud maître 1 s'attend à devoir filtrer le message de réponse correspondant que le domaine 13 adressera au nœud 12. Le nœud maître 1 applique ainsi un traitement de vérification de la cohérence des échanges entre les deux domaines.

[0075] Le nœud maître 1 effectue avantageusement des tests de surveillance du bon fonctionnement de la carte électronique 11 et de ses composants. L'exécution d'un test est par exemple déclenchée dans une phase de maintenance au sol.

[0076] Le nœud maître 1 effectue avantageusement un filtrage des requêtes de passage en téléchargement, en particulier sur le bon format de telles requêtes, le téléchargement consistant ensuite à importer des informations pour le fonctionnement de la passerelle (valeur de configuration du pare-feu, mise à jour logicielle pour réaliser la rupture protocolaire d'un format de données vers le format neutre, etc.)

[0077] Par exemple, dans une phase de maintenance au sol, on connecte un équipement de maintenance à la passerelle 10 permettant de mettre à jour un logiciel du module de pare-feu 4. Cet équipement transmet une requête de téléchargement, qui est donc filtrée par le module de pare-feu 4, qui la retransmet vers le module de rupture protocolaire 5, qui lui-même la retransmet vers le module maitre 1.

[0078] Constatant qu'il s'agit d'une requête de téléchargement, le nœud maitre 1 vérifie toute une série de conditions. Parmi ces conditions il y a par exemple le fait qu'un équipement soit effectivement connecté à la passerelle, que la phase de fonctionnement de l'aéronef corresponde à une phase de maintenance au sol, etc. En cas de vérification positive, le nœud 1 est propre à modifier le mode de fonctionnement de la passerelle pour passer d'un mode par exemple de maintenance dans un mode de téléchargement.

[0079] Le nœud 1 est propre à générer un signal d'interruption conduisant au redémarrage de la passerelle, c'est-à-dire au redémarrage de chacun des nœuds.

[0080] Le nœud maître 1 exécute avantageusement une application de détection d'intrusion HIDS (pour « Host-based Intrusion Detection System ») sur tous les flux qu'il filtre. Pour l'exécution de cette application, l'application de détection d'intrusion a besoin de données d'environnement issues de l'ensemble des nœuds et centralisées par le nœud de service 2. D'où la présence de la liaison de communication bidirectionnelle B12 entre le nœud maître 1 et le nœud de service 2 pour l'échange de ces données.

[0081] Les informations de détection générées par cette application constituent des entrées du journal maintenu à jour par le nœud de service 2. Ces informations sont adressées par le nœud 1 au nœud 2 via la liaison U12.

[0082] Une fois le flux filtré, le nœud maître 1 renvoie celui-ci vers le nœud de reformatage 6.

[0083] Si le flux est rejeté, des informations de journalisation sont générées et transmises au nœud de service 2 via la liaison U12.

[0084] Le nœud maître 1 est développé avec le plus haut niveau d'assurance qualité cyber (SAL3).

Nœud de formatage inverse 6

[0085] Le nœud 6, en aval du nœud maître 1 dans la chaîne de filtrage, réalise une fonction de formatage inverse de celle réalisée par le nœud de formatage 5.

[0086] Ainsi, pour un flux de données provenant du domaine de confiance basse ayant subi une rupture protocolaire à la traversée du nœud 5, le nœud 6 réalise une rupture protocolaire inverse pour passer du format neutre vers un format attendu par le domaine de confiance haute 13.

[0087] Inversement, pour un flux de données provenant du domaine de confiance haute et devant être aiguillé vers le nœud 1, le nœud 6 réalise une rupture protocolaire. De l'autre côté du nœud maître 1, ce sera au nœud 5 de réaliser la rupture protocolaire inverse pour passer du format neutre vers un format attendu par le nœud de pare-feu ou domaine de confiance basse.

[0088] Dans le mode de réalisation de la [Fig.1], le nœud 6 présente un port d'entrée/sortie pour l'établissement de la liaison B16 bidirectionnelle avec le nœud maître 1.

[0089] Il présente un port d'entrée/sortie pour l'établissement d'une liaison B67 bidirectionnelle avec le second module de conversion 7.

[0090] Il présente un port d'entrée/sortie pour l'établissement d'une liaison B68 bidirectionnelle avec le troisième module de conversion 8.

[0091] Il présente un port d'entrée/sortie pour l'établissement d'une liaison B62 avec le nœud de service 2. Cette liaison est utilisée en monodirectionnel du nœud 6 vers le nœud 2. Elle n'est utilisée en bidirectionnel que lors d'un téléchargement depuis un équipement de téléchargement positionné dans le domaine 13.

[0092] Le nœud 6 présente également un port de sortie pour l'établissement d'une liaison U62 unidirectionnelle vers le nœud de service 2.

[0093] Le nœud 6 présente un port de sortie pour l'établissement du liaison U64 unidirectionnelle vers le nœud de pare-feu 4.

[0094] Si la rupture protocolaire inverse est réussie, le flux est réémis vers le domaine de confiance haute 13.

[0095] En revanche, si le flux est rejeté, le nœud 6 génère des informations de journalisation et les transmet au nœud de service 2.

[0096] Le second module de conversion 7 permet de convertir un flux de données provenant du nœud 6 en un flux de données au format requis par le domaine 13. Le second module 7 est connecté directement au domaine 13 par un liaison B7 bidirectionnelle, de préférence ARINC 664 P3 ou ARINC 664 P7, en 100 Mbit/s ou éventuellement plus.

[0097] Le troisième module de conversion 8 permet de convertir un flux de données provenant du nœud 6 en un flux de données au format requis par le domaine 13. Le troisième module de conversion 8 est connecté directement au domaine 13 par une liaison B8, bidirectionnelle, de préférence ARINC 429.

[0098] Il est à noter qu'un flux venant de domaine de confiance haute doit être transmis par le nœud de formatage inverse 6 soit par le nœud maître 1 soit directement vers le nœud de pare-feu 4. La condition d'aiguillage d'un flux par le nœud 6 résulte d'une configuration de ce dernier. Par exemple la condition d'aiguillage dépend du format des données du flux à traiter.

Nœud de service 2

[0099] Le nœud 2 réalise différentes fonctions de sécurité.

[0100] Il présente un port d'entrée/sortie pour l'établissement de la liaison B12 bidirectionnelle avec le nœud maître 1, et un port d'entrée/sortie pour l'établissement de la liaison B62 bidirectionnelle avec le nœud 6.

[0101] Il présente des ports d'entrée pour l'établissement des liaisons U42, U52, U12, et U62.

[0102] Il présente un port de sortie pour l'établissement d'une liaison U24, unidirectionnelle, avec le module de pare-feu 4.

[0103] Le nœud de service 2 assure la sauvegarde des évènements de sécurité et leurs émissions dans un fichier de journalisation (fichier « log »). Par exemple le fichier de journalisation est sauvegardé au format SYSLOG.

[0104] Le nœud de service 2 assure la sauvegarde et l'émission des données associées au bon fonctionnement de la passerelle. Cette fonction est par exemple connue de l'homme du métier sous la dénomination « BITE » (« Built In Test Equipment »). Il s'agit d'effectuer cycliquement ou en fonction d'évènements déclencheurs des tests adaptés sur les différents composants de la passerelle.

[0105] Le nœud de service 2 a en charge les échanges de téléchargement avec un équipement externe, une fois que le passage en téléchargement a été validé par le nœud maître 1. Pour répondre à une requête de téléchargement du fichier de journalisation émise par une application du domaine de confiance basse 12 et validée par le nœud 1, le nœud 2 peut transmettre les données via la liaison B12, ou lorsqu'il y a simple interrogation, via la liaison U24 directement vers le nœud de pare-feu 4. Le Lien U24 est ainsi utilisé pour répondre efficacement aux requêtes de téléchargement simples.

[0106] Les communications internes à la carte 11 utilisent des technologies distinctes, par exemple Ethernet et série. Par exemple :

[0107] - les liaisons bidirectionnelles B45, B51 et B16 sont des bus de données Ethernet, de préférence à 1Gbit/s ;

[0108] - les liaisons bidirectionnelles B62 sont des bus de données Ethernet, de préférence 100 Mbit/s ;

[0109] - la liaison B34 est un bus synchronisés (SPI pour « Serial Peripheral Interface ») ou une liaison série asynchrone ;

[0110] - les liaisons B67 et B68 est un bus PCI ou PCI Express ;

[0111] - et les différentes liaisons unidirectionnelles sont par exemple des bus de données série, de préférence synchronisés (SPI pour « Serial Peripheral Interface »), mais pouvant en variante être asynchrones.

[0112] Cette spécificité permet de renforcer les propriétés de non contournement du filtrage.

[0113] L'utilisation du protocole Ethernet gigabits le long de la chaîne de filtrage assure des temps de traversée limités entre les domaines 12 et 13 de manière à obtenir des temps de traversée inférieurs à 50ms, conformément aux exigences avioniques. En effet, le protocole Ethernet permet de renvoyer très rapidement un flux après avoir reçu le dernier fragment d'un message. Sans réémission rapide vers le nœud suivant, le temps de traversée de la passerelle serait fortement impacté, notamment pour des messages longs fragmentés, car la rupture protocolaire ne peut se faire que sur un message complet et non un fragment de ce dernier. Les liaisons internes le long de la chaîne de filtrage présentent donc une bande passante supérieure à celle des connexions permettant de connecter la passerelle aux domaines de confiance haute et basse.

[0114] Tous les nœuds prévus sur la carte sont synchronisés par une même horloge, qui est sous le contrôle du nœud maitre 1. De cette manière, avec de simples séquenceurs logiciels où chaque nœud est décalé dans l'exécution de ses tâches pour que la fin d'une tâche d'un nœud soit synchronisée avec le début de la tâche du nœud suivant le long de la chaîne de filtrage, le temps de traversée de la passerelle est optimisé en tenant compte du temps des traitements effectués de manière indépendante par chacun des nœuds disposés en série le long de la chaine de filtrage.

FONCTIONNEMENT/UTILISATION

[0115] La [Fig.2] illustre plusieurs fonctionnements possibles de la passerelle 10 venant d'être présentée.

[0116] Selon un premier fonctionnement 100, le nœud maitre 1 effectue un filtrage simple des flux de données circulant depuis le domaine de confiance basse 12 vers le domaine de confiance haute 13.

[0117] Un message de requête est émis depuis le domaine 13 à destination d'un serveur du domaine 12. La passerelle 10, en coupure entre les deux domaines reçoit le message de requête.

[0118] Le message de requête est d'abord reçu (étape 110) par le nœud 6, qui le retransmet (112) directement et sans modification de format au nœud de pare-feu 4 via la liaison U64. Le nœud 4 le retransmet (114) à son tour vers le domaine 12.

[0119] Sur le domaine 12, le message de requête est acheminé vers le serveur destinataire, qui élabore un message de réponse adapté.

[0120] Le message de réponse est renvoyé du domaine de confiance basse 12 vers le domaine de confiance haute 13. Le message de réponse traverse par conséquent la passerelle 10.

[0121] Plus précisément, le message de réponse est reçu (115) par le nœud de pare-feu 4. Après vérification positive, le nœud 4 le retransmet (116) au nœud de formatage 5.

[0122] Celui-ci effectue la rupture protocolaire et, en cas de succès, retransmet (117) au nœud maître 1 le message de réponse transcrit dans le format neutre.

[0123] En recevant le message de réponse, le nœud maître 1 applique des traitements de filtrage adaptés.

[0124] En cas de filtrage positif, le message de réponse est transmis (118) par le nœud maître 1 vers le nœud de formatage inverse 6. Ce dernier convertit le message de réponse selon le format requis et le réémet (119) sur domaine de confiance haute 13.

[0125] Selon un second fonctionnement 200, le nœud maitre 1 effectue un filtrage contextuel, en l'occurrence une vérification de cohérence entre messages de requête et de réponse.

[0126] Un message de requête est émis depuis le domaine de confiance haute 13 à destination d'un serveur du domaine de confiance basse 12. La passerelle 10, en coupure entre les deux domaines, reçoit le message de requête.

[0127] Ce message de requête est reçu (étape 210) par le nœud de formatage inverse 6. Compte tenu par exemple de la valeur d'un champ de l'en-tête du message de requête, le nœud 6 applique une rupture protocolaire sur le message de requête et retransmet (211) le message de requête dans le format neutre vers le nœud maitre 1.

[0128] Constatant qu'il s'agit d'une requête, le nœud maître 1 mémorise par exemple l'identifiant de cette requête pour effectuer ultérieurement la vérification de cohérence.

[0129] Le nœud maître 1 retransmet (étape 212) le message de requête vers le nœud de formatage 5, qui applique une rupture protocolaire inverse et retransmet (213) le message de requête dans le format adapté vers le nœud 4.

[0130] Ce dernier le retransmet (214) à son tour le message de requête vers le domaine 12.

[0131] Sur le domaine 12, le message de requête est acheminé vers le serveur destinataire, qui élabore un message de réponse adapté.

[0132] Le message de réponse est renvoyé du domaine de confiance basse vers le domaine de confiance élevé. Le message de réponse traverse par conséquent la passerelle 10.

[0133] Le message de réponse est renvoyé du domaine de confiance basse 12 vers le domaine de confiance haute 13. Le message de réponse traverse par conséquent la passerelle 10.

[0134] Plus précisément, le message de réponse est reçu (215) par le nœud de pare-feu 4, qui le retransmet (216), après vérification, au nœud de formatage 5.

[0135] Celui-ci effectue la rupture protocolaire et, en cas de succès, retransmet (217) au nœud maître 1 le message de réponse dans le format neutre.

[0136] En recevant le message de réponse, le nœud maître 1 applique les traitements de filtrage adaptés ainsi que la vérification de cohérence. Pour cela, il vérifie si

l'identifiant contenu dans le message de réponse correspond à l'identifiant contenu dans le message de requête précédemment traité par le nœud maître 1.

[0137] En cas de vérification positive, le message de réponse est retransmis (étape 218) par le nœud maître 1 vers le nœud 6, qui, après rupture protocolaire inverse, le renvoie (219) vers le domaine de confiance haute 13.

[0138] En cas de vérification négative, le message de réponse est rejeté par le nœud maître 1 et une entrée relative à l'échec du traitement de cohérence est ajoutée au fichier de journalisation tenu à jour par le nœud de service 2.

[0139] Selon un troisième fonctionnement 300, le domaine de confiance basse 12 applique à la passerelle un message de requête de passage en téléchargement, par exemple en vue de télécharger une mise à jour logicielle pour le nœud de pare-feu 4.

[0140] Un message de requête de passage en téléchargement est reçu (étape 310) depuis le domaine de confiance basse 12 par le nœud de pare-feu 4.

[0141] Après vérification positive, le nœud de pare-feu 4 le transmet (311) vers le nœud de formatage 5.

[0142] Le nœud 5 effectue la rupture protocolaire et retransmet (312) un message de requête de passage en téléchargement au format neutre vers le nœud maitre 1.

[0143] Le nœud maître 1 analyse le message de requête de passage en téléchargement. Notamment il vérifie que le fonctionnement courant de l'aéronef est compatible avec un basculement dans un mode de téléchargement de la passerelle. En effet, par exemple si l'aéronef est en vol, le nœud maître 1 rejette la requête de téléchargement car cela risque de nuire à la sécurité de fonctionnement globale de l'aéronef.

[0144] En cas de vérification positive, le nœud maître 1 bascule la passerelle dans un mode de fonctionnement de téléchargement.

[0145] Il transmet (313) un message de commande de gestion du téléchargement à destination du nœud de service 2, mais via le nœud 6.

[0146] Constatant qu'il s'agit d'un message à destination du nœud 2, le nœud 6 route (314) le message de commande vers le nœud 2 le long de la liaison B62.

[0147] Sur réception du message de commande, le module de service 2 gère le téléchargement. Le fichier est téléchargé depuis le domaine 12 vers le nœud 2 en passant par les nœuds 4, 5, 1 et 6.

[0148] Par exemple, le nœud 2 enregistre (315) le fichier téléchargé dans une mémoire flash du nœud de pare-feu 4.

[0149] A l'issue du téléchargement, le nœud 2 indique au nœud maître 1 la fin de l'opération.

[0150] Le nœud maître 1 commande alors un redémarrage de la passerelle 10, au cours duquel le nœud de pare-feu 4 réinitialise le contenu de sa mémoire vive - RAM

avec les informations contenues dans la mémoire flash qui lui est associée, et par conséquent avec le fichier de mise à jour venant d'être téléchargé.

AVANTAGES

[0151] En ségrégant physiquement les différentes fonctions, la passerelle venant d'être présentée atteint les niveaux de sécurité requis pour le domaine avionique, ce qui ne serait pas le cas d'une simple ségrégation logicielle.

[0152] L'architecture de la passerelle, fondée sur différents nœuds physiquement indépendants, permet de simplifier les preuves d'un bon développement des fonctions de sécurité. Par exemple, selon la norme ED-203A, les nœuds maitre 1 et de rupture protocolaire 5 sont avantageusement développés selon le niveau le plus élevé, SAL3 ; le nœud de pare feu 4 selon le niveau intermédiaire, SAL2 ; et les nœuds de service 2 et de rupture protocolaire inverse 6 selon le niveau le plus bas, SAL 1.

[0153] Notamment, la rupture protocolaire doit être développée en SAL3 pour pouvoir atteindre un bon niveau de filtrage avec le plus haut niveau d'assurance qualité de cybersécurité.

[0154] On notera que ces deux derniers nœuds, puisqu'ils sont situés en aval du nœud maître 1 et que tous les flux de données qu'ils reçoivent sont d'abord filtrés par les nœuds de pare-feu, de rupture protocolaire et maître, bénéficient du niveau de criticité du domaine de criticité haute.

[0155] Le nœud de service présente souvent une grande complexité. Il serait compliqué et couteux de le développer selon le niveau SAL2. L'invention permet par conséquent de relâcher les contraintes de développement sur ce composant, tout en garantissant qu'il ne peut pas être utilisé pour contourner le filtrage des flux, qui repassent toujours vers le nœud maître.

[0156] L'architecture permet par conséquent d'isoler les tâches en fonction de leurs criticités et de leurs niveaux d'assurance qualité associés, tout en assurant un point de passage des différents flux pour assurer un filtrage systématique. La passerelle permet de réaliser un filtrage de grande qualité en utilisant des technologies différentes en fonction des flux.

[0157] La solution proposée assure que tous les flux de données provenant du domaine de sécurité basse passent par le nœud maître. Cette architecture permet de garantir le non contournement de la fonction de filtrage.

[0158] Avec cette architecture, les temps de traversée peuvent être assez faible tout en assurant des propriétés de non contournement demandées par le haut niveau d'assurance qualité de cyber-sécurité requis.

[0159] Selon cette architecture, le nœud maître n'est pas en relation directe avec le domaine de faible confiance : il ne reçoit que des flux passés par deux filtrages, celui réalisé par le pare-feu et celui réalisé par la rupture protocolaire.

[0160] Dans le mode de réalisation préféré présenté précédemment, les différents nœuds de traitement de données sont intégrés sur une même carte électronique, ce qui conduit à une solution présentant un facteur de forme réduit, ce qui est avantageux dans la mesure où les contraintes de volume sont des contraintes fortes dans le domaine avionique. En variante, les nœuds de traitement sont implantés sur plusieurs cartes électroniques connectées les unes aux autres de manière adaptée.

[0161] L'aspect modulaire facilite le développement, la certification, la maintenance, et la mise à jour de la passerelle.

[0162] On notera que la présente passerelle ne comporte qu'un seul par feu, disposé en entrée connectée au domaine réseau de faible confiance.

[0163] On notera également que la passerelle est configurable, ce qui permet de paramétrer les différentes fonctions de filtrage en fonction des menaces courantes.

Revendications

[Revendication 1] Passerelle de sécurité réseau (10) destinée à être embarquée à bord d'un aéronef pour connecter un domaine de confiance basse (12) et un domaine de confiance haute (13) d'une infrastructure informatique avionique, la passerelle offrant une pluralité de fonctions de sécurité, chaque fonction étant réalisée par un nœud de traitement de données, la passerelle comportant, connectés en série le long d'une chaîne de filtrage d'un flux de données reçu depuis le domaine de confiance basse :

- un nœud de traitement de données de pare-feu (4) ;
- un nœud de traitement de données de rupture protocolaire (5) ;
- un nœud de traitement de données maître (1) ; et,
- un nœud de traitement de données de rupture protocolaire inverse (6),

la passerelle comportant en outre un nœud de service (2) relié à chacun des nœuds de traitement de données de la chaîne de filtrage, le nœud de service (2) réalisant différentes fonctions de sécurité, notamment la mémorisation d'un fichier de journalisation et de centralisation de données d'environnement issues de l'ensembles des nœuds ;

les différents nœuds de traitement de données étant ségrégés physiquement,

le nœud de traitement de données maître (1) exécutant une application de détection d'intrusion en utilisant les données d'environnement centralisées par le nœud de service (2) et les informations de détection générées par ladite application étant adressées au nœud de service (2) en tant qu'entrées du fichier de journalisation.

[Revendication 2] Passerelle selon la revendication 1, dans laquelle les nœuds de la chaîne de filtrage sont connectés par des liaisons bidirectionnelles, de préférence au format Ethernet, de préférence encore au format Ethernet 1 Gbit/s, présentant une bande passante supérieure à celle des connexions permettant de connecter la passerelle aux domaines de confiance haute et basse.

[Revendication 3] Passerelle selon l'une quelconque des revendications 1 à 2, dans laquelle le nœud de service (2) est connecté à la pluralité de nœuds de la chaîne de filtrage par des liaisons unidirectionnelles, de

préférence au format série, de préférence encore au format série synchronisé.

[Revendication 4] Passerelle selon l'une quelconque des revendication 1 à 3, dans laquelle la passerelle constitue une interface Ethernet et/ou ARINC 429 et/ou ARINC 664, avec le domaine de confiance haute (13) et une interface Ethernet et/ou ARINC 429 et/ou ARINC 664 avec le domaine de confiance basse (12).

[Revendication 5] Passerelle selon l'une quelconque des revendications 1 à 4, dans laquelle le nœud de traitement de données de pare-feu (4) est connecté au domaine de confiance basse (12) par un premier module de conversion (3), réalisant une conversion d'un format d'un flux de données provenant du domaine de confiance basse (12), de préférence le format ARINC 429, en un format de données attendu par le nœud de traitement de données de pare-feu (4).

[Revendication 6] Passerelle selon l'une quelconque des revendications 1 à 5, dans laquelle le nœud de traitement de rupture protocolaire inverse (6) est connecté au domaine de confiance haute (13) par un second module de conversion (7), réalisant une conversion d'un format d'un flux de données délivré par le nœud de traitement de rupture protocolaire inverse (6), de préférence le format Ethernet 100 Mbit/s, en un format attendu par le domaine de confiance basse (12), de préférence le format ARINC 664, de préférence encore ARINC 664 P3 ou P7.

[Revendication 7] Passerelle selon l'une quelconque des revendications 1 à 6, dans laquelle le nœud de traitement de données maître (1) filtre un flux de données en fonction d'un contexte ou en fonction d'un niveau de priorité.

[Revendication 8] Passerelle selon l'une quelconque des revendications 1 à 7, dans laquelle tout flux de données provenant du domaine de confiance basse (12) passe par le nœud de traitement de données maître (1), à condition de n'avoir pas été rejeté par le nœud de traitement de données de pare-feu (4) ou le nœud de traitement de données de rupture protocolaire (5).

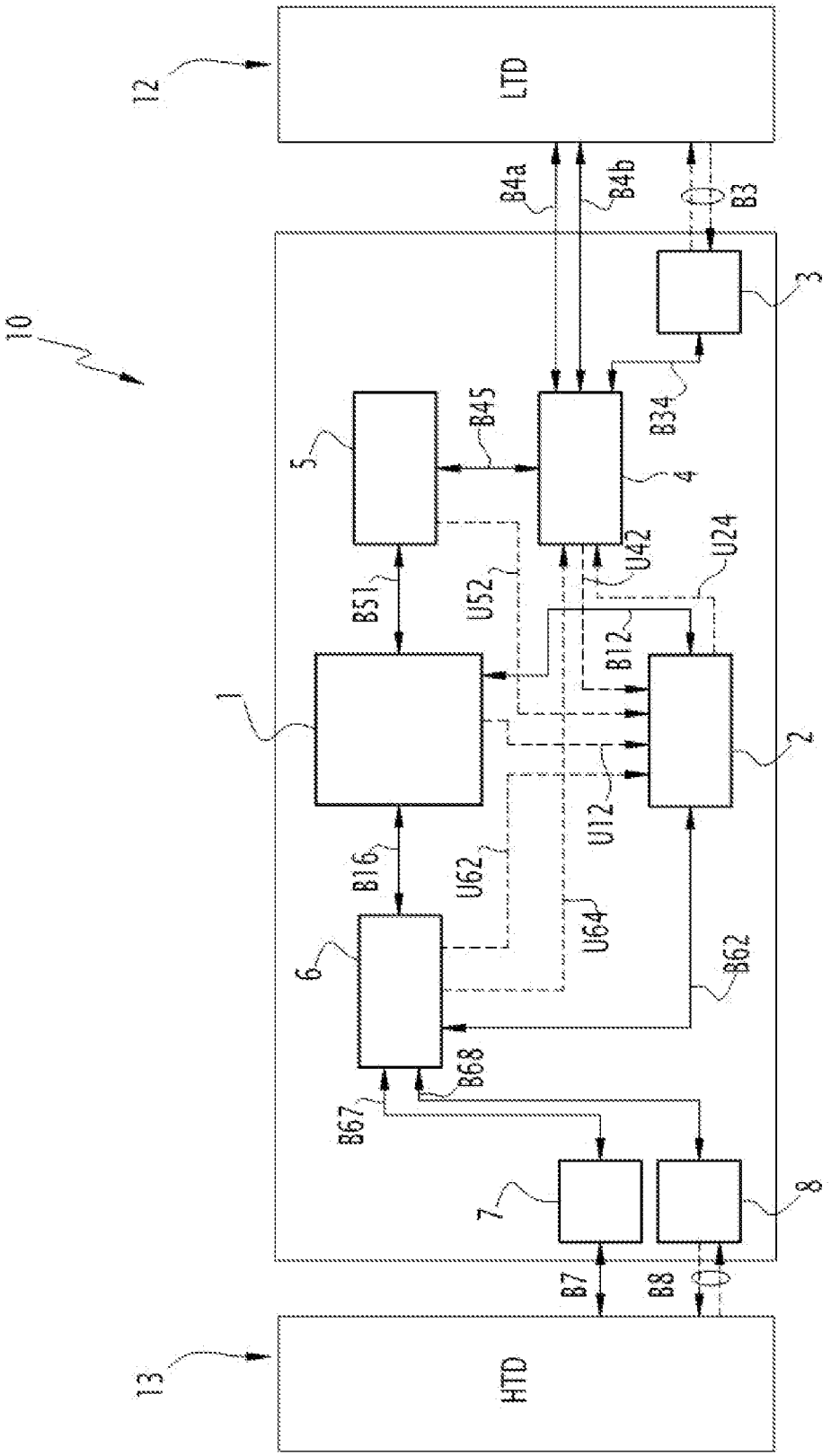
[Revendication 9] Passerelle selon l'une quelconque des revendications 1 à 8, dans laquelle, outre son interface avec le domaine de confiance basse (12), le nœud de traitement de données de pare-feu (4) ne comporte qu'un port de sortie forçant l'acheminement de tout flux de données opérationnelles provenant du domaine de confiance basse (12) vers le nœud de traitement de données de rupture protocolaire (5),

et dans laquelle, outre son interface avec le nœud de traitement de données de pare-feu (4), le nœud de traitement de données de rupture protocolaire (5) ne comporte qu'un port de sortie forçant l'acheminement de tout flux de données opérationnelles provenant du domaine de confiance basse (12) vers le nœud de traitement de données maître (1).

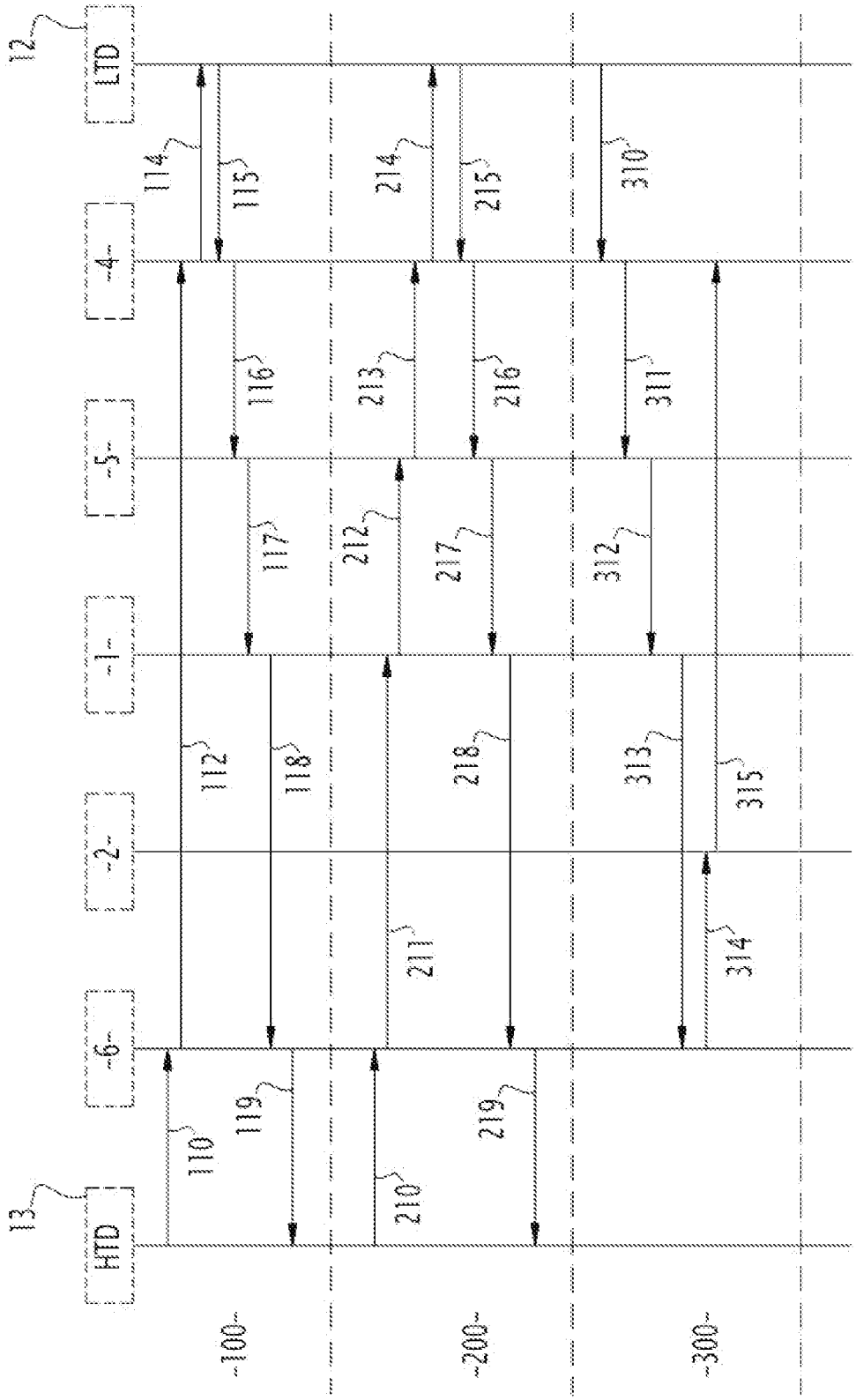
[Revendication 10] Passerelle selon l'une quelconque des revendications 1 à 9, dans laquelle tout flux de données provenant du domaine de confiance haute (13) et à destination du domaine de confiance basse (12) et qui ne passe pas par le nœud de traitement de données maître (1), est acheminé à travers la passerelle via au moins une liaison unidirectionnelle.

[Revendication 11] Passerelle selon l'une quelconque des revendications 1 à 10, ne comportant qu'un seul nœud de traitement de données de pare-feu (4) situé en entrée de la chaine de filtrage du côté du domaine de confiance basse (12).

[Fig. 1]


10
12
LTD
B4a
B4b
B3
3
B34
4
B45
5
U42
U24
B51
U52
B12
1
2
U12
B16
U62
U64
6
B62
B68
B67
7
8
B7
B8
13
HTD

[Fig. 2]


12
LTD
-4-
-5-
-1-
-2-
-6-
13
HTD
-100-
-200-
-300-
110
112
114
115
116
117
118
119
210
211
212
213
214
215
216
217
218
219
310
311
312
313
314
315

RAPPORT DE RECHERCHE

articles L.612-14, L.612-53 à 69 du code de la propriété intellectuelle

OBJET DU RAPPORT DE RECHERCHE

L'I.N.P.I. annexe à chaque brevet un "RAPPORT DE RECHERCHE" citant les éléments de l'état de la technique qui peuvent être pris en considération pour apprécier la brevetabilité de l'invention, au sens des articles L. 611-11 (nouveauté) et L. 611-14 (activité inventive) du code de la propriété intellectuelle. Ce rapport porte sur les revendications du brevet qui définissent l'objet de l'invention et délimitent l'étendue de la protection.
Après délivrance, l'I.N.P.I. peut, à la requête de toute personne intéressée, formuler un "AVIS DOCUMENTAIRE" sur la base des documents cités dans ce rapport de recherche et de tout autre document que le requérant souhaite voir prendre en considération.

CONDITIONS D'ETABLISSEMENT DU PRESENT RAPPORT DE RECHERCHE

[x] Le demandeur a présenté des observations en réponse au rapport de recherche préliminaire.

☐ Le demandeur a maintenu les revendications.

[x] Le demandeur a modifié les revendications.

☐ Le demandeur a modifié la description pour en éliminer les éléments qui n'étaient plus en concordance avec les nouvelles revendications.

☐ Les tiers ont présenté des observations après publication du rapport de recherche préliminaire.

☐ Un rapport de recherche préliminaire complémentaire a été établi.

DOCUMENTS CITES DANS LE PRESENT RAPPORT DE RECHERCHE

La répartition des documents entre les rubriques 1, 2 et 3 tient compte, le cas échéant, des revendications déposées en dernier lieu et/ou des observations présentées.

[x] Les documents énumérés à la rubrique 1 ci-après sont susceptibles d'être pris en considération pour apprécier la brevetabilité de l'invention.

[x] Les documents énumérés à la rubrique 2 ci-après illustrent l'arrière-plan technologique général.

☐ Les documents énumérés à la rubrique 3 ci-après ont été cités en cours de procédure, mais leur pertinence dépend de la validité des priorités revendiquées.

☐ Aucun document n'a été cité en cours de procédure.

1. ELEMENTS DE L'ETAT DE LA TECHNIQUE SUSCEPTIBLES D'ETRE PRIS EN CONSIDERATION POUR APPRECIER LA BREVETABILITE DE L'INVENTION
FR 2 922 705 A1 (SAGEM DEFENSE SECURITE [FR]) 24 avril 2009 (2009-04-24)
2. ELEMENTS DE L'ETAT DE LA TECHNIQUE ILLUSTRANT L'ARRIERE-PLAN TECHNOLOGIQUE GENERAL
EP 3 068 101 B1 (THALES LAS FRANCE SAS [FR]) 18 novembre 2020 (2020-11-18)
3. ELEMENTS DE L'ETAT DE LA TECHNIQUE DONT LA PERTINENCE DEPEND DE LA VALIDITE DES PRIORITES
NEANT