

(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
28 juin 2018 (28.06.2018)



(10) Numéro de publication internationale
WO 2018/115359 A1

(51) Classification internationale des brevets :
G06F 21/60 (2013.01) *H04L 29/06* (2006.01)

(21) Numéro de la demande internationale :
PCT/EP2017/084232

(22) Date de dépôt international :
21 décembre 2017 (21.12.2017)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
16 63262 22 décembre 2016 (22.12.2016) FR

(71) Déposant : AIRBUS DEFENCE AND SPACE SAS
[FR/FR] ; 31 rue des Cosmonautes ZI du Palays, 31402
TOULOUSE CEDEX 4 (FR).

(72) Inventeurs : DUPONT, Gérard ; C/O Emmanuel AJDARI, Service Propriété Intellectuelle, Airbus Defence and Space, 31 rue des Cosmonautes, ZI du Palays, 31402 TOULOUSE Cedex 4 (FR). LAGARDE, Olivier ; C/O Emmanuel AJDARI, Service Propriété Intellectuelle, Airbus Defence and Space, 31 rue des Cosmonautes, ZI du Palays, 31402 TOULOUSE Cedex 4 (FR). MARTY, Jean-Luc ; C/O Emmanuel AJDARI, Service Propriété Intellectuelle, Airbus Defence and Space, 31 rue des Cosmonautes, ZI du Palays, 31402 TOULOUSE Cedex 4 (FR).

(74) Mandataire : CABINET PLASSERAUD ; 66 rue de la
Chaussée d'Antin, 75440 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,

(54) Title: UNIDIRECTIONAL COMMUNICATION SYSTEM AND METHOD

(54) Titre : SYSTÈME ET PROCÉDÉ DE COMMUNICATION UNIDIRECTIONNEL

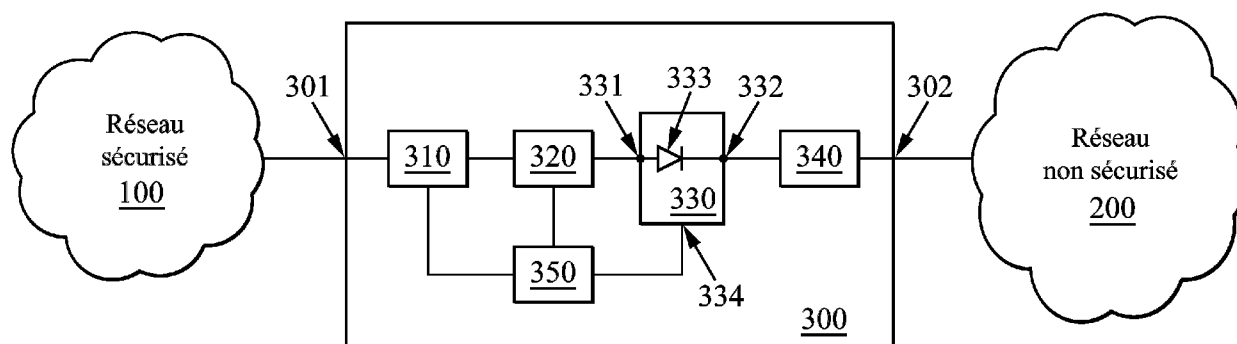


FIG. 1

100 Secure network

200 Not secure network

(57) Abstract: The invention relates to a unidirectional communication system. This invention provides a solution enabling the sending of alerts and notification to remote operators while overcoming the problem of protecting a secure network against cyber attacks when the secure network is caused to communicate information from the secure network to a public network. In practice, the solution is based on the use of a data diode (also known as a network diode) in order to enable the unidirectional transmission of information from the secure network to a public network, which makes a computer attack on the secure network from the public network impossible. In addition, by using a controlled data diode, it is also ensured that no sensitive information can leak from the secure network via the system according to the invention. Indeed, the transmission of the message is only performed after the message to be sent has been cleaned of sensitive information and then encrypted.

(57) Abrégé : L'invention propose un système de communication unidirectionnel. Cette invention apporte une solution permettant l'émission d'alertes et de notification à des opérateurs distants tout en palliant au problème de la protection d'un réseau sécurisé contre

[Suite sur la page suivante]

EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, 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, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, 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), eurasién (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))

des cyberattaques lorsque le réseau sécurisé est amené à communiquer des informations depuis le réseau sécurisé vers un réseau public. En pratique, la solution est basée sur l'utilisation d'une diode de données (aussi connue sous le nom de diode réseau ou "data diode" en anglais) pour permettre la transmission unidirectionnelle des informations du réseau sécurisé vers un réseau public, ce qui rend impossible une attaque informatique du réseau sécurisé depuis le réseau public. En outre, grâce à une diode de données commandée, il est également garanti qu'aucune information sensible ne puisse fuir du réseau sécurisé via le système selon l'invention. En effet, la transmission du message n'est effectuée qu'après que le message à émettre ait été nettoyé des informations sensibles, puis chiffré.

Titre: Système et procédé de communication unidirectionnel**Description**Domaine technique

- [001] La présente invention concerne un système de communication depuis un réseau sécurisé vers un réseau de confiance moindre.

Technique antérieure

- [002] La norme ISO 22301 définit la continuité d'activité d'un système d'information en exploitation comme sa capacité à poursuivre la fourniture de produits ou la prestation de services à des niveaux acceptables et préalablement définit après un incident perturbateur. Également connue sous le sigle MCO pour maintien en condition opérationnelle, la continuité d'activité d'un système d'information en exploitation vise à définir l'ensemble des moyens et procédures nécessaires pour que le système d'information reste, au long de sa durée d'utilisation, apte à l'emploi qui lui est assigné.
- [003] Dans les systèmes d'information dits critiques, le MCO représente un coût d'exploitation important car il nécessite souvent la présence sur place d'au moins un technicien de maintenance qui doit se tenir prêt à intervenir à tout moment, dès la détection d'un incident perturbateur. Cette configuration est notamment dictée par le besoin de confidentialité des informations associées au fonctionnement de ces systèmes.
- [004] Afin de réduire le coût d'exploitation du MCO, les opérateurs de systèmes d'information critiques envisagent de plus en plus l'utilisation de la télésurveillance comme c'est souvent le cas pour les systèmes d'information non critiques. En pratique, lorsqu'un événement perturbateur se produit, un message d'avertissement est automatiquement transmis au technicien de maintenance d'astreinte, par exemple, via SMS, courriel ou appel vocal sur téléphonie fixe ou cellulaire.
- [005] Cependant, l'adoption de la télésurveillance des systèmes d'information critique via un réseau public n'inspire pas confiance aux opérateurs concernés. En effet, les dispositifs utilisés actuellement pour émettre les appels d'astreinte ne garantissent pas une sécurisation suffisante de l'interconnexion entre le système d'information et le réseau public, de sorte qu'il existe des risques d'intrusion informatiques et/ou de perte d'informations sensibles.
- [006] Il est donc important de proposer une solution permettant de résoudre ces problèmes car de tels défauts de sécurité peuvent permettre la réalisation d'attaques informatique provoquant, par exemple, la modification du comportement du système d'information, son indisponibilité par saturation de ses ressources ou permettre, par exemple, de récupérer des informations sensibles du système d'information.

Résumé de l'invention

- [007] À cet effet, un premier objet de l'invention concerne un système de communication pour la transmission d'au moins un message depuis un premier réseau d'un premier système d'information vers un second réseau d'un second système d'information, le premier réseau ayant une classification de sécurité supérieure à celle du second réseau. En pratique, le système comprend :
- une entrée de système apte à être connectée au premier réseau, et prévue pour recevoir le message, le message comprenant au moins une première métadonnée associée au fonctionnement du premier système d'information;
 - une sortie de système apte à être connectée au second réseau ;
 - une unité d'analyse et de filtrage d'information couplée à l'entrée de système, et prévue pour générer un message filtré en filtrant le message en fonction d'un signal de filtrage de sorte qu'au moins une information sensible associée à la au moins une première métadonnée est masquée;
 - une unité de chiffrement d'information couplée à l'unité d'analyse et de filtrage d'information, et prévue pour générer un message chiffré en chiffrant le message filtré en fonction d'un signal de chiffrement ;
 - un circuit à diode de données couplé à l'unité de chiffrement d'information, et comprenant une entrée de circuit et une sortie de circuit, le circuit à diode de données étant prévu pour transférer unidirectionnellement le message chiffré entre l'entrée de circuit et la sortie de circuit, le circuit à diode de données comprenant en outre une entrée de commande et des moyens d'activation pour empêcher ou permettre le passage du message chiffré entre l'entrée de circuit et la sortie de circuit en fonction d'un signal de commande reçu au niveau de l'entrée de commande;
 - une unité d'émission de message couplée entre la sortie de circuit et la sortie de système, et prévue pour émettre un message d'appel comprenant le message chiffré ; et,
 - un processeur couplé à l'unité d'analyse et de filtrage d'information, à l'unité de chiffrement d'information et au circuit, et prévu pour générer le signal de filtrage, le signal de chiffrement et le signal de commande.
- [008] Dans une première mise en œuvre, le circuit à diode de données comprend en outre un élément de diode de données ayant une unité de transmission prévue pour transmettre unidirectionnellement le message chiffré, les moyens d'activation étant prévus pour être actionnables entre une première position dans laquelle les moyens d'activation sont agencés de manière à interrompre l'alimentation de l'unité de transmission et dans une deuxième position dans laquelle les moyens d'activation sont agencés de manière à activer l'alimentation de l'unité de transmission.
- [009] Dans une deuxième mise en œuvre, l'unité d'analyse et de filtrage d'information est en outre prévue pour générer un premier signal de terminaison d'opération indicatif de

l'achèvement des opérations de l'unité d'analyse et de filtrage d'information. En outre, l'unité de chiffrement d'information est en outre prévue pour générer un second signal de terminaison d'opération indicatif de l'achèvement des opérations de l'unité de chiffrement d'information. Enfin, le processeur est en outre prévu pour générer le signal de commande en réponse à la génération successive du premier signal de terminaison d'opération et du second signal de terminaison d'opération.

- [0010] Dans une troisième mise en œuvre, le système comprend en outre,
- un port de mémoire couplé au processeur, et prévu pour recevoir une mémoire portable ;
 - et,
 - une mémoire portable apte à être reçue dans le port de mémoire et configurée pour mémoriser des données de filtrage et de données de chiffrement.
- Dans ce cas, le processeur est en outre prévu pour configurer le signal de filtrage et le signal de chiffrement, à partir des données de filtrage et de données de chiffrement, respectivement.
- [0011] Selon un exemple de la troisième mise en œuvre,
- la mémoire portable est en outre configurée pour mémoriser au moins une liste de contact comprenant au moins un numéro d'appel d'un dispositif mobile à contacter, chaque numéro d'appel étant associé à au moins une deuxième métadonnée relative au fonctionnement du premier système d'information,
 - le processeur est en outre prévu pour inclure la liste de contact dans le signal de filtrage,
 - l'unité d'analyse et de filtrage d'information est en outre prévue pour générer un message d'association associant le message filtré à au moins un numéro d'appel dont la au moins une deuxième métadonnée coïncide avec la première métadonnée,
 - l'unité de chiffrement d'information est en outre prévue pour associer le message d'association à le message chiffré ; et,
 - l'unité d'émission de message est en outre prévue pour émettre le message d'appel en fonction du message d'association.
- [0012] Dans ce cas, de préférence, l'unité d'émission de message est en outre prévue pour générer et émettre un message de pulsation périodique pendant l'attente d'un message d'appel.
- [0013] Avantageusement, l'unité d'émission de message est en outre prévue pour détruire le message d'appel suite à l'émission du message d'appel.
- [0014] Dans un arrangement particulier, l'unité d'émission de message est configurée pour émettre le message d'appel en utilisant un protocole de messagerie choisi parmi au moins l'un des protocoles suivants : SMS, MMS, XMPP et SMTP.
- [0015] Dans un autre arrangement particulier,
- l'unité d'analyse et de filtrage d'information, l'unité de chiffrement d'information et le processeur sont compris dans une première enceinte,
 - le circuit à diode de données est compris dans une deuxième enceinte; et,
 - l'unité d'émission de message est compris dans une troisième enceinte.

Dans ce cas, la première enceinte, la deuxième enceinte et la troisième enceinte sont géographiquement distinctes les unes des autres de sorte qu'aucun rayonnement électromagnétique ne puisse être capté d'une enceinte à une autre.

- [0016] De manière avantageuse,
- l'unité d'analyse et de filtrage d'information, l'unité de chiffrement d'information, le processeur et l'unité d'émission de message sont compris dans une première enceinte ; et,
 - le circuit à diode de données est compris dans une deuxième enceinte.

Dans ce cas, la première enceinte et la deuxième enceinte sont géographiquement distinctes les unes des autres de sorte qu'aucun rayonnement électromagnétique ne puisse être capté d'une enceinte à une autre.

- [0017] Enfin, un deuxième objet de l'invention concerne un procédé de transmission d'au moins un message depuis un premier réseau d'un premier système d'information vers un second réseau d'un second système d'information, le premier réseau ayant une classification de sécurité supérieure à celle du second réseau, le message comprenant au moins une première métadonnée associée au fonctionnement du premier système d'information. En pratique, le procédé comprend les étapes suivantes :
- générer un message filtré en filtrant le message en fonction d'un signal de filtrage de sorte qu'au moins une information sensible associée à la au moins une première métadonnée est masquée;
 - générer un message chiffré en chiffrant le message filtré en fonction d'un signal de chiffrement ;
 - transférer unidirectionnellement le message chiffré du réseau sécurisé vers le réseau non sécurisé en fonction d'un signal de commande, seulement lorsque le filtrage et le chiffrement ont été réalisés.

Brève description des dessins

- [0018] Les caractéristiques et avantages de l'invention seront mieux compris à la lecture de la description qui va suivre et en référence aux dessins annexés, donnés à titre illustratif et nullement limitatif.
- [0019] La figure 1 représente un exemple de mise en œuvre du système selon l'invention.
- [0020] La figure 2 représente une mise en œuvre du circuit à diode de données selon l'invention.
- [0021] La figure 3 représente un organigramme d'un procédé selon l'invention.

Description des modes de réalisation

- [0022] Dans le cadre de cette description, on entend par système d'information l'ensemble des moyens matériels, des moyens logiciels, des bases de données et des réseaux de communication pouvant être agencés pour fournir des produits ou des prestations de services dans un domaine dit critique.
- [0023] En outre, on entend par domaine critique les systèmes d'information pour lesquels une panne peut avoir des conséquences dramatiques, comme la mort, les blessures graves,

les dégâts matériels/économiques importants, ou des conséquences graves pour l'environnement. Ainsi, cette définition couvre, par exemple, les systèmes d'information de transport (par ex. pour le pilotage d'un avion, d'un train, d'une voiture, d'un bateau), les systèmes d'information d'énergie (par ex. pour le contrôle d'une centrale nucléaire), les systèmes d'information de santé (par ex. un dispositif médical) ou encore les systèmes d'information de télécommunication (par ex. un système de communication au sol d'un système de communication par satellite). Toutefois, n'importe quel système d'information conforme à la définition ci-dessus est aussi envisagé dans cette description.

- [0024] Dans la description, on entend également par incident perturbateur, l'ensemble des événements liés à l'état en opération d'un système d'information tel que : la défaillance d'un composant de stockage, le défaut d'alimentation d'un moteur d'un dispositif, la chute de tension de commande d'une machine, la chute de la puissance (hydraulique, électrique, etc....) reçue par une machine, défaillance mécanique. Toutefois, on notera que l'invention ne porte pas sur la détection et le diagnostic d'un incident perturbateur. Dans le reste de la description, on considérera qu'un incident au niveau d'un système d'information a été détecté et diagnostiqué comme étant perturbateur. L'incident perturbateur est ensuite inclus dans un message à transmettre à un technicien de maintenance ou un expert technique.
- [0025] Dans l'invention, une solution est proposée au problème de la protection d'un réseau sécurisé contre des cyberattaques lorsque le réseau sécurisé est amené à communiquer des informations depuis le réseau sécurisé vers un réseau public, par exemple par l'émission d'alertes et de notification à des opérateurs distants. En pratique, la solution est basée sur l'utilisation d'une diode de données (aussi connue sous le nom de diode réseau ou "data diode" en anglais) pour permettre la transmission unidirectionnelle des informations du réseau sécurisé vers un réseau public. Ceci a pour effet de rendre impossible une attaque informatique du réseau sécurisé depuis le réseau public. Ainsi, cet agencement garantit une séparation physique entre le réseau sécurisé et le réseau public.
- [0026] La figure 1 représente un système 300 selon l'invention. Dans l'exemple de la figure 1 le système 300 est disposé entre un réseau sécurisé 100 et un réseau non sécurisé 200. Le réseau sécurisé 100 est associé à un premier système d'information tandis que le réseau non sécurisé 200 est associé à un second système d'information différent du premier système d'information. De manière générale, le réseau sécurisé 100 est considéré comme plus sécurisé que le réseau non sécurisé 200 car il possède une classification de sécurité supérieure à celle du réseau non sécurisé 200.
- [0027] Structuellement, le système 300 comprend une entrée de système 301 et une sortie de système 302. En outre, le système 300 comprend une unité d'analyse et de filtrage d'information 310, une unité de chiffrement d'information 320, un circuit à diode de données 330, une unité d'émission de message 340 et un processeur 350.
- [0028] Dans l'exemple de la figure 1, l'entrée de système 301 est configurée pour être connectée au réseau sécurisé 100 tandis que la sortie de système 302 est configurée pour être

connectée au réseau non sécurisé 200. Lorsque le système 300 est en opération, l'entrée de système 301 est prévue pour recevoir un message comprenant au moins une métadonnée associée au fonctionnement du premier système d'information.

- [0029] On entend par message, un ensemble de signaux numériques mis sous une forme déterminée. Par exemple, le message reçu à l'entrée de système 301 peut être un message textuel selon le standard RFC5424 ou tout autre standard normalisé ou pas. Le message peut comprendre des éléments d'identification du message, d'horodatage de génération du message, d'identification de la source du message ou encore d'identification de l'événement ayant provoqué la génération du message. Toutefois, d'autres éléments peuvent être ajoutés au message à transmettre.
- [0030] On entend ici par métadonnée toute information descriptive du fonctionnement du premier système d'information. Par exemple, dans le domaine du transport, il peut s'agir de données relatives à la défaillance d'un composant de stockage, à l'état de santé des moteurs ou encore la température d'une pièce ou d'un composant.
- [0031] De retour à la figure 1, l'unité d'analyse et de filtrage d'information 310 est couplée à l'entrée de système 301. En opération, l'unité d'analyse et de filtrage d'information 310 est configurée pour générer un message filtré en filtrant le message reçu en fonction d'un signal de filtrage. Le signal de filtrage contient toutes les informations permettant à l'unité d'analyse et de filtrage d'information 310 de déterminer l'étendue des informations à filtrer. En pratique, l'unité d'analyse et de filtrage d'information 310 filtre la métadonnée du message reçue de l'entrée de système 301 de sorte qu'au moins une information sensible associée à la métadonnée est masquée. Ceci a pour effet d'empêcher la fuite d'informations sensibles du réseau sécurisé 100.
- [0032] On entend par information sensible, une information ou une connaissance obtenue directement ou indirectement, qui si elle est révélée au public, nuirait au système d'information sur laquelle elle porte. En d'autres termes, il s'agit d'une information dont la divulgation, l'utilisation à mauvais escient, la modification ou l'accès non autorisé peut affecter défavorablement la sécurité du système d'information concerné. Par exemple, il peut s'agir d'une information associée à l'identification des serveurs informatiques du système d'information tel que les adresses IP, les noms des serveurs ou encore la taille des serveurs informatiques. En effet, de telles informations peuvent, par exemple, informer sur les capacités d'attaque ou de défense du système d'information. Dans ce cas, si l'information sensible tombe entre de mauvaises mains, cela pourrait affecter défavorablement la sécurité d'une organisation.
- [0033] Dans une première en œuvre particulière de l'unité d'analyse et de filtrage d'information 310, le masquage est réalisé par la suppression de l'information sensible de la métadonnée. Par exemple, l'adresse IP d'un serveur ayant subi un incident perturbateur peut être supprimée de la métadonnée.
- [0034] Dans une deuxième mise en œuvre de l'unité d'analyse et de filtrage d'information 310, le masquage est réalisé par le remplacement de l'information sensible de la métadonnée par

une ou plusieurs informations non sensibles. Par exemple, le nom d'un serveur ayant subi un incident perturbateur peut être remplacé par un autre nom ou un sigle différent du véritable nom du serveur. Dans ce cas, le où les mots de remplacement doivent être connus de l'opérateur qui recevra le message. Une autre possibilité du même ordre peut consister à remplacer l'information sensible par une offuscation pour un encodage de l'information sensible.

- [0035] Dans une troisième mise en œuvre de l'unité d'analyse et de filtrage d'information 310, le masquage est réalisé par une combinaison de suppression et de remplacement de l'information sensible. Ainsi, si une métadonnée comprend l'adresse IP et le nom d'un serveur ayant subi un incident perturbateur, les solutions de la première mise en œuvre et de la deuxième mise en œuvre peuvent être utilisées conjointement. Par exemple, l'adresse IP peut être remplacée par un sigle et le nom du serveur peut être supprimé de la métadonnée.
- [0036] Toujours dans la figure 1, l'unité de chiffrement d'information 320 est couplée à l'unité d'analyse et de filtrage d'information 310. En opération, l'unité de chiffrement d'information 320 est configurée pour générer un message chiffré en chiffrant le message filtré en fonction d'un signal de chiffrement. Le signal de chiffrement contient toutes les informations permettant à l'unité de chiffrement d'information 320 de chiffrer l'information filtrée. En pratique, le chiffrement peut se faire à l'aide de tous moyens de chiffrement connu de l'homme de l'art, notamment par l'utilisation d'un algorithme symétrique ou asymétrique. Ceci a pour effet d'empêcher l'interception des messages de notification émis depuis le réseau sécurisé 100.
- [0037] De nouveau dans la figure 1, le circuit à diode de données 330 est couplé à l'unité de chiffrement d'information 320. Le circuit à diode de données 330 comprend une entrée de circuit 331, une sortie de circuit 332 est un élément de diode de données 333. En opération, l'élément de diode de données 333 est configuré pour transférer unidirectionnellement le message chiffré entre l'entrée de circuit 331 et la sortie de circuit 332. En effet, l'élément de diode de données 333 qui est également connu sous le nom de diode réseau est un système qui permet d'interconnecter deux réseaux informatiques en autorisant le transfert de données dans un seul sens. Ce type de système est généralement employé pour relier un réseau nécessitant un niveau de sécurité élevée à un réseau de confiance moindre (par exemple Internet). Dans ce cas, seule la remontée d'information du réseau de confiance moindre est autorisée afin de garantir la confidentialité du réseau sécurisé en évitant les fuites d'informations sensibles. Toutefois, dans le cadre de l'invention il est envisagé d'utiliser l'élément de diode de données 333 dans le sens inverse de sorte que seule la remontée d'information du réseau sécurisé est possible. Ceci a pour effet qu'il est impossible de mettre en œuvre des attaques informatiques depuis l'extérieur du réseau sécurisé, car il n'y a qu'une seule voie de communication depuis le réseau sécurisé vers le réseau de confiance moindre et pas dans l'autre sens.

- [0038] En outre dans la figure 1, le circuit à diode de données 330 comprend une entrée de commande 335 et des moyens d'activation 334 pour empêcher ou permettre le passage du message chiffré entre l'entrée de circuit 331 et la sortie de circuit 332 en fonction d'un signal de commande reçu au niveau de l'entrée de commande 335. Les moyens d'activation 334 sont prévus pour être actionnables entre une première position dans laquelle les moyens d'activation 334 empêchent le passage du message chiffré, et une deuxième position dans laquelle les moyens d'activation 334 permettent le passage de l'information. Enfin, les moyens d'activation 334 sont normalement actionnés dans la première position.
- [0039] Dans la figure 2, il est représenté une mise en œuvre particulière du circuit à diode de données 330 selon l'invention. Dans l'exemple de la figure 2, l'élément de diode de données 333 du circuit à diode de données 330 comprend un élément de transmission TX et un élément de réception RX, tous deux prévus en combinaison pour transmettre unidirectionnellement le message chiffré entre l'élément de transmission TX et l'élément de réception RX. Dans un exemple, l'élément de diode de données 333 est réalisé sur la base d'une fibre optique ne comprenant qu'un seul brin. Dans ce cas, l'élément de transmission TX peut être une source de lumière prévue pour émettre un flux de lumière dans la fibre optique et l'élément de réception RX peut être un photo-récepteur prévu pour recevoir le flux de lumière. Toutefois d'autres mises en œuvre de liaison réseau unidirectionnelle peuvent également être utilisées avec l'invention. Par exemple, il est également envisagé l'utilisation d'une liaison série RS-232 partielle ou encore une liaison Ethernet RJ45 partielle avec des éléments de transmission et réception correspondant.
- [0040] Dans une mise en œuvre particulière de la figure 2, les moyens d'activation 334 sont actionnés dans la première position en commandant l'interruption de l'alimentation de l'élément de transmission TX tandis que les moyens d'activation 334 sont actionnés dans la deuxième position en commandant l'activation de l'alimentation de l'élément de transmission TX. Pour cela, les moyens d'activation 334 peuvent être directement connectés à l'alimentation de l'élément de transmission TX.
- [0041] De retour à la figure 1, l'unité d'émission de message 340 est couplée entre la sortie de circuit 332 et la sortie de système 302. En opération, l'unité d'émission de message 340 est configurée pour émettre un message d'appel comprenant le message chiffré. Dans une mise en œuvre particulière, l'unité d'émission de message 340 est configurée pour émettre le message d'appel en utilisant un protocole de messagerie choisie parmi au moins l'un des protocoles suivants : SMS, E-mail, MMS, XMPP Ainsi, pour une meilleure sécurité, aucune copie du message émis n'est conservée au niveau du système 300.
- [0042] Dans une mise en œuvre particulière, l'unité d'émission de message 340 est prévue pour détruire le message d'appel suite à l'émission du message d'appel.
- [0043] Dans un exemple de la mise en œuvre précédente, l'unité d'émission de message 340 est prévue pour recevoir un message d'acquiescement en réponse à l'émission du message

d'appel et pour détruire le message d'appel en réponse à la réception du message d'acquiescement.

- [0044] Dans une autre mise en œuvre particulière, l'unité d'émission de message 340 est en outre prévue pour générer et émettre un message de pulsation périodique (en anglais, "heartbeat message" ou "keep alive message") pendant l'attente d'un message d'appel. Le message de pulsation est prévu pour indiquer au destinataire du message que le système 300 est encore en cours d'exécution. En d'autres termes, le message de pulsation périodique permet d'indiquer au destinataire du message que le système 300 est toujours en activité. Dans un exemple, la période de génération et d'émission du message de pulsation peut être fixée à toutes les minutes, toutes les demi-heures ou toutes les heures. Dans une mise en œuvre particulière, le message de pulsation périodique est chiffré et agencé de sorte qu'il n'est pas possible de l'intercepter et ainsi de pouvoir simuler la présence du système 300 en jouant une séquence de transmission du message de pulsation périodique déjà utilisée.
- [0045] Enfin, dans la figure 1, le processeur 350 est couplé à l'unité d'analyse et de filtrage d'information 310, à l'unité de chiffrement d'information 320 et au circuit à diode de données 330. En opération, le processeur 350 est configuré pour générer le signal de filtrage, le signal de chiffrement et le signal de commande.
- [0046] Dans une première mise en œuvre du processeur 350, l'ensemble des informations permettant de configurer le signal de filtrage, le signal de chiffrement et le signal de commande sont compris dans une mémoire du processeur 350. Dans ce cas, c'est le processeur 350 qui ordonnance la génération des signaux de filtrage de chiffrement et de commande. Dans le cadre de cette mise en œuvre particulière, il est entendu que le signal de filtrage est généré avant le signal de chiffrement de sorte à générer le signal de commande actionnant les moyens d'activation 334 dans la deuxième position que lorsque les opérations de masquage et de filtrage ont été réalisées. Par exemple, le processeur 350 peut générer le signal de chiffrement, d'une part, et le signal de commande d'autre part, après une temporisation prédéterminée suivant la génération du signal de filtrage, d'une part, et du signal de chiffrement d'autre part. De cette manière, il peut être garanti que l'information transmise a été préalablement filtrée de toute information sensible et chiffrée.
- [0047] Dans une deuxième mise en œuvre du processeur 350, la génération du signal de commande est conditionnée par l'exécution des opérations de l'unité d'analyse et de filtrage d'information 310 puis de l'unité de chiffrement d'information 320. En pratique, l'unité d'analyse et de filtrage d'information 310 est en outre prévue pour générer un premier signal de terminaison d'opération indicatif de l'achèvement des opérations de l'unité d'analyse et de filtrage d'information 310. Il en est de même pour l'unité de chiffrement d'information 320 qui est également prévue pour générer un second signal de terminaison d'opération indicatif de l'achèvement des opérations de l'unité de chiffrement d'information 320. Enfin, le processeur 350 est en outre prévu pour générer le signal de

commande en réponse à la génération du premier signal de terminaison d'opération et du second signal de terminaison d'opération. Dans le cadre de cette mise en œuvre particulière, il est entendu que le premier signal de terminaison d'opération est généré avant le second signal de terminaison d'opération de sorte à générer le signal de commande actionnant les moyens d'activation 334 dans la deuxième position que lorsque les opérations de masquage et de filtrage ont été réalisées. De cette manière, il peut être garanti que l'information transmise a été préalablement filtrée de toute information sensible et chiffrée.

- [0048] Dans une autre mise en œuvre particulière du système 300, on incorpore un port de mémoire et une mémoire portable. Dans cette mise en œuvre, le port de mémoire est couplé au processeur 350 et configuré pour recevoir la mémoire portable. En outre, la mémoire portable est configurée pour mémoriser des données de filtrage et des données de chiffrement. Enfin, le processeur 350 est adapté pour configurer, respectivement, le signal de filtrage et le signal de chiffrement à partir des données de filtrage et de données de chiffrement. Ainsi, dans cette mise en œuvre particulière, les données permettant de configurer le signal de filtrage, le signal de chiffrement sont obtenues à partir de la mémoire portable. Ceci offre la possibilité aux propriétaires du système d'information sécurisée 100 de déterminer la manière dont le filtrage et le chiffrement doivent être réalisés.
- [0049] Dans un exemple de cette mise en œuvre particulière du système 300, la mémoire portable peut également être configurée pour mémoriser des données de commande utilisable par le processeur 350 pour configurer le signal de commande.
- [0050] Dans un exemple de la mise en œuvre précédente, la mémoire portable est en outre configurée pour mémoriser au moins une liste de contact comprenant au moins numéro d'appel d'un dispositif mobile ou fixe à contacter. Dans cet exemple, chaque numéro d'appel est associé à au moins une deuxième métadonnée relative au fonctionnement du réseau sécurisé 100. En outre, le processeur 350 est également prévu pour inclure la liste de contact dans le signal de filtrage. Par ailleurs, l'unité d'analyse et de filtrage d'information 310 est également configurée pour générer un message d'association associant le message filtré à au moins un numéro d'appel dont la deuxième métadonnée coïncident avec la première métadonnée. Cet agencement a pour effet de permettre la notification de l'occurrence d'un incident à un ou plusieurs techniciens les plus appropriés pour résoudre l'incident.
- [0051] On dira que la première métadonnée et la deuxième métadonnée coïncident lorsqu'elles comprennent toutes deux une information relative au même incident perturbateur du réseau sécurisé 100. Par exemple, si la première métadonnée peut comprendre une information indiquant qu'une défaillance d'un composant de stockage a lieu, alors une deuxième métadonnée qui coïncide avec la première métadonnée comprend également une information relative à la défaillance d'un composant de stockage. En pratique, comme chaque numéro d'appel est associé à un technicien spécialiste d'un ou de plusieurs

incidents perturbateur du réseau sécurisé 100, alors, la mise en coïncidence selon l'invention a pour objectif de limiter la liste d'appel aux seuls numéros associés aux techniciens spécialistes de l'incident perturbateur qui s'est produit.

[0052] Dans une mise en œuvre particulière, on pourra envisager la mise en place d'une table de coïncidence permettant d'associer une spécialité technique à un incident perturbateur. Par exemple, toutes les défaillances du premier système d'information qui sont liées à la mécanique peuvent être mises en coïncidence avec la spécialité technique d'un mécanicien. Ainsi, grâce à la table de coïncidence et la liste de contact, l'unité d'analyse et de filtrage d'information 310 est capable de déterminer le ou les numéros d'appel pertinents qui sont associés à l'occurrence d'un incident perturbateur particulier en faisant coïncider le l'incident perturbateur à une spécialité technique particulière. En pratique, on peut envisager de stocker la table de coïncidence dans une mémoire de l'unité d'analyse et de filtrage d'information 310 ou encore dans le processeur 350.

[0053] Dans un autre exemple de la mise en œuvre précédente, on peut envisager d'externaliser la fonctionnalité permettant de déterminer le ou les numéros d'appel pertinents qui sont associés à l'occurrence d'un incident perturbateur particulier, dans une unité distincte de l'unité d'analyse et de filtrage d'information 310. Par exemple, une unité de routage couplée à l'unité d'analyse peut être utilisée. Dans ce cas, l'unité de routage peut comprendre une mémoire ainsi qu'un processeur. La mémoire peut alors comprendre inclure la liste de contact et la table de coïncidence, tous deux mentionnés ci-dessus. Dans cet exemple particulier, l'unité d'analyse et de filtrage d'information 310 est configurée pour fournir la deuxième métadonnée relative au fonctionnement du réseau sécurisé 100 à l'unité de routage. Par la suite, l'unité de routage est configurée pour déterminer et retourner à l'unité d'analyse et de filtrage d'information 310, au moins un numéro d'appel dont la deuxième métadonnée coïncident avec la première métadonnée. En outre, l'unité de routage est également configurée pour déterminer et retourner à l'unité d'analyse et de filtrage d'information 310, le ou les numéros d'appel pertinents qui sont associés à l'occurrence d'un incident perturbateur particulier en faisant coïncider le l'incident perturbateur à une spécialité technique particulière.

[0054] Par la suite, l'unité de chiffrement d'information 320 est également configurée pour associer le message d'association au message chiffré. Enfin, l'unité d'émission de message 340 est également configurée pour émettre le message d'appel en fonction du message d'association. Dans un autre exemple de cette mise en œuvre, on peut envisager d'inclure la liste de contact dans une mémoire du processeur 350.

[0055] Dans une mise œuvre de l'invention, on peut envisager d'agencer physiquement les différents éléments du système 300 selon plusieurs arrangements.

[0056] Par exemple, dans un premier arrangement, on regroupe dans une première enceinte l'unité d'analyse et de filtrage d'information 310, l'unité de chiffrement d'information 320 et le processeur 350. Ensuite, on inclut le circuit à diode de données dans une deuxième enceinte distincte de la première enceinte. Enfin, on positionne l'unité d'émission de

message 340 dans une troisième enceinte distincte de la première enceinte et de la deuxième enceinte. Dans cet arrangement, la première enceinte, la deuxième enceinte et la troisième enceinte peuvent être géographiquement distinctes les unes de autres de sorte qu'aucun rayonnement électromagnétique ne puisse être capté d'une enceinte à une autre.

[0057] Dans un second arrangement on regroupe dans une première enceinte l'unité d'analyse et de filtrage d'information 310, l'unité de chiffrement d'information 320, le processeur 350 est l'unité d'émission de message 340. Ensuite, on positionne le circuit à diode de données 330 dans une deuxième enceinte distincte de la première enceinte. Dans cet arrangement, la première enceinte et la deuxième enceinte sont géographiquement distinctes les unes des autres de sorte qu'aucun rayonnement électromagnétique ne puisse être capté d'une enceinte à une autre.

[0058] Dans la description, il a été considéré que les informations transmises du réseau sécurisé 100 vers le réseau sécurisé 200 étaient liées à un dysfonctionnement du premier système d'information. Ceci a pour effet de permettre la mise en place de la maintenance corrective sous astreinte à distance du premier système d'information via un réseau public. Toutefois, grâce à l'invention, des informations qui ne sont pas nécessairement liées à un dysfonctionnement du premier système d'information peuvent également être transmises à l'extérieur de ce système. Dans ce cas, l'unité d'analyse et de filtrage d'information 310 devra être configurée pour laisser passer les informations correspondantes. Ceci aura pour effet de permettre la mise en place d'une supervision à distance du premier système d'information.

[0059] L'invention concerne également un émetteur (non représenté) d'un système de communication de type filaire ou sans fil comprenant le système 300 tel que décrit plus haut. Un tel émetteur permet l'établissement d'une communication unidirectionnelle cryptée à travers un réseau de communication quelconque, et notamment un réseau public.

[0060] L'invention concerne aussi un procédé 400 pour la transmission d'au moins une première métadonnée depuis le réseau sécurisé 100 vers le réseau non sécurisé 200 selon les aspects techniques décrits ci-dessus. Dans la figure 3, le procédé 400 comprend les étapes suivantes consistant à :

- générer un message filtré 410 en filtrant la première métadonnée en fonction du signal de filtrage tel que décrit plus haut, de sorte qu'au moins une information sensible associée à la première métadonnée est masquée;
- générer un message chiffré 420 en chiffrant le message filtré en fonction du signal de chiffrement tel que décrit plus haut ;
- transférer unidirectionnellement 430 le message chiffré du réseau sécurisé 100 vers le réseau non sécurisé 200, de manière conditionnelle, en commandant le passage du message chiffré en fonction du signal de commande tel que décrit plus haut.

[0061] L'invention décrite apporte une solution au problème de la protection d'un réseau sécurisé contre des cyberattaques lorsque le réseau sécurisé est amené à communiquer des informations depuis le réseau sécurisé vers un réseau public. En effet, dans son ensemble, le système selon l'invention peut difficilement être compromis par une cyberattaque. Plus précisément, seule l'unité d'émission de message est susceptible d'être compromise ou endommagée par une telle attaque. Toutefois, comme cette unité se trouve positionnée en aval de la limite de sécurité physique du système (c-à-d après le circuit à diode de données), alors sa perte n'a pas d'impact sur la sécurité globale du réseau sécurisé. Ainsi, l'adjonction d'un système selon l'invention à un système d'information existant ne fournit pas d'opportunité pour la mise en œuvre de cyberattaque à l'encontre du réseau de ce système d'information. En outre, grâce à l'utilisation d'un circuit à diode de données commandée, il est également garanti qu'aucune information sensible ne puisse fuir du réseau sécurisé via le système selon l'invention. On peut également utiliser la notion de "thyristor de données". En effet, comme un thyristor permet la conduction unidirectionnelle du courant grâce au commandement d'une gâchette, le "thyristor de données" permet la transmission unidirectionnelle d'un message après que le message à émettre ait été nettoyé des informations sensibles, puis chiffré. Dans ce cas, le message fait office de courant, tandis que l'information de confirmation du nettoyage et le chiffrement du message font offices de gâchette du thyristor.

Revendications

1. Système de communication (300) pour la transmission d'au moins un message depuis un premier réseau (100) d'un premier système d'information vers un second réseau (200) d'un second système d'information, le premier réseau (100) ayant une classification de sécurité supérieure à celle du second réseau, le système (300) comprenant :
 - une entrée de système (301) apte à être connectée au premier réseau, et prévue pour recevoir le message, le message comprenant au moins une première métadonnée associée au fonctionnement du premier système d'information;
 - une sortie de système (302) apte à être connectée au second réseau ;
 - une unité d'analyse et de filtrage d'information (310) couplée à l'entrée de système, et prévue pour générer un message filtré en filtrant le message en fonction d'un signal de filtrage de sorte qu'au moins une information sensible associée à la au moins une première métadonnée est masquée;
 - une unité de chiffrement d'information (320) couplée à l'unité d'analyse et de filtrage d'information, et prévue pour générer un message chiffré en chiffrant le message filtré en fonction d'un signal de chiffrement ;
 - un circuit à diode de données (330) couplé à l'unité de chiffrement d'information (320), et comprenant une entrée de circuit (331) et une sortie de circuit (332), le circuit à diode de données (330) étant prévu pour transférer unidirectionnellement le message chiffré entre l'entrée de circuit (331) et la sortie de circuit (332), le circuit à diode de données comprenant en outre une entrée de commande (335) et des moyens d'activation (334) pour empêcher ou permettre le passage du message chiffré entre l'entrée de circuit (331) et la sortie de circuit (332) en fonction d'un signal de commande reçu au niveau de l'entrée de commande (335);
 - une unité d'émission de message (340) couplée entre la sortie de circuit (332) et la sortie de système (302), et prévue pour émettre un message d'appel comprenant le message chiffré ;et,
 - un processeur (350) couplé à l'unité d'analyse et de filtrage d'information (310), à l'unité de chiffrement d'information (320) et au circuit (330), et prévu pour générer le signal de filtrage, le signal de chiffrement et le signal de commande.
2. Système selon la revendication 1 dans lequel, le circuit à diode de données comprend en outre un élément de diode de données (333) ayant une unité de transmission prévue pour transmettre unidirectionnellement le message chiffré, les moyens d'activation (334) étant prévus pour être actionnables entre une première position dans laquelle les moyens d'activation (334) sont agencés de manière à interrompre l'alimentation de l'unité de transmission et dans une deuxième position dans laquelle les moyens d'activation (334) sont agencés de manière à activer l'alimentation de l'unité de transmission.
3. Système selon l'une quelconque des revendications 1 ou 2 dans lequel,
 - l'unité d'analyse et de filtrage d'information (310) est en outre prévue pour générer un

premier signal de terminaison d'opération indicatif de l'achèvement des opérations de l'unité d'analyse et de filtrage d'information (310) ;

- l'unité de chiffrement d'information (320) est en outre prévue pour générer un second signal de terminaison d'opération indicatif de l'achèvement des opérations de l'unité de chiffrement d'information (320) ; et,

- le processeur (350) est en outre prévu pour générer le signal de commande en réponse à la génération successive du premier signal de terminaison d'opération et du second signal de terminaison d'opération.

4. Système selon l'une quelconque des revendications 1, 2 ou 3 comprenant en outre,

- un port de mémoire couplé au processeur, et prévu pour recevoir une mémoire portable ; et,
- une mémoire portable apte à être reçue dans le port de mémoire et configurée pour mémoriser des données de filtrage et de données de chiffrement ;

dans lequel le processeur est en outre prévu pour configurer le signal de filtrage et le signal de chiffrement, à partir des données de filtrage et de données de chiffrement, respectivement.

5. Système selon la revendication 4 dans lequel,

- la mémoire portable est en outre configurée pour mémoriser au moins une liste de contact comprenant au moins un numéro d'appel d'un dispositif mobile à contacter, chaque numéro d'appel étant associé à au moins une deuxième métadonnée relative au fonctionnement du premier système d'information,

- le processeur est en outre prévu pour inclure la liste de contact dans le signal de filtrage,

- l'unité d'analyse et de filtrage d'information est en outre prévue pour générer un message d'association associant le message filtré à au moins un numéro d'appel dont la au moins une deuxième métadonnée coïncide avec la première métadonnée,

- l'unité de chiffrement d'information est en outre prévue pour associer le message d'association à le message chiffré ; et,

- l'unité d'émission de message est en outre prévue pour émettre le message d'appel en fonction du message d'association.

6. Système selon la revendication 5 dans lequel l'unité d'émission de message est en outre prévue pour générer et émettre un message de pulsation périodique pendant l'attente d'un message d'appel.

7. Système selon l'une quelconque des revendications 1, 2, 3, 4, 5 ou 6 dans lequel l'unité d'émission de message est en outre prévue pour détruire le message d'appel suite à l'émission du message d'appel.

8. Système selon l'une quelconque des revendications 1, 2, 3, 4, 5, 6 ou 7 dans lequel l'unité d'émission de message est configurée pour émettre le message d'appel en utilisant un protocole de messagerie choisi parmi au moins l'un des protocoles suivants : SMS, MMS, XMPP et SMTP.

9. Système selon l'une quelconque des revendications 1, 2, 3, 4, 5, 6, 7 ou 8 dans lequel,

- l'unité d'analyse et de filtrage d'information, l'unité de chiffrement d'information et le processeur sont compris dans une première enceinte,

- le circuit à diode de données est compris dans une deuxième enceinte; et,
- l'unité d'émission de message est comprise dans une troisième enceinte;

dans lequel, la première enceinte, la deuxième enceinte et la troisième enceinte sont géographiquement distinctes les unes des autres de sorte qu'aucun rayonnement électromagnétique ne puisse être capté d'une enceinte à une autre.

10. Système selon l'une quelconque des revendications 1, 2, 3, 4, 5, 6, 7, 8 ou 9 dans lequel,

- l'unité d'analyse et de filtrage d'information, l'unité de chiffrement d'information, le processeur et l'unité d'émission de message sont compris dans une première enceinte ; et,
- le circuit à diode de données est compris dans une deuxième enceinte ;

dans lequel, la première enceinte et la deuxième enceinte sont géographiquement distinctes les unes des autres de sorte qu'aucun rayonnement électromagnétique ne puisse être capté d'une enceinte à une autre.

11. Procédé (400) de transmission d'au moins un message depuis un premier réseau (100) d'un premier système d'information vers un second réseau (200) d'un second système d'information, le premier réseau (100) ayant une classification de sécurité supérieure à celle du second réseau, le message comprenant au moins une première métadonnée associée au fonctionnement du premier système d'information, le procédé comprenant les étapes suivantes :

- générer (410) un message filtré en filtrant le message en fonction d'un signal de filtrage de sorte qu'au moins une information sensible associée à la au moins une première métadonnée est masquée;
- générer (420) un message chiffré en chiffrant le message filtré en fonction d'un signal de chiffrement ;
- transférer unidirectionnellement (430) le message chiffré du réseau sécurisé (100) vers le réseau non sécurisé (200) en fonction d'un signal de commande, seulement lorsque le filtrage et le chiffrement ont été réalisés.

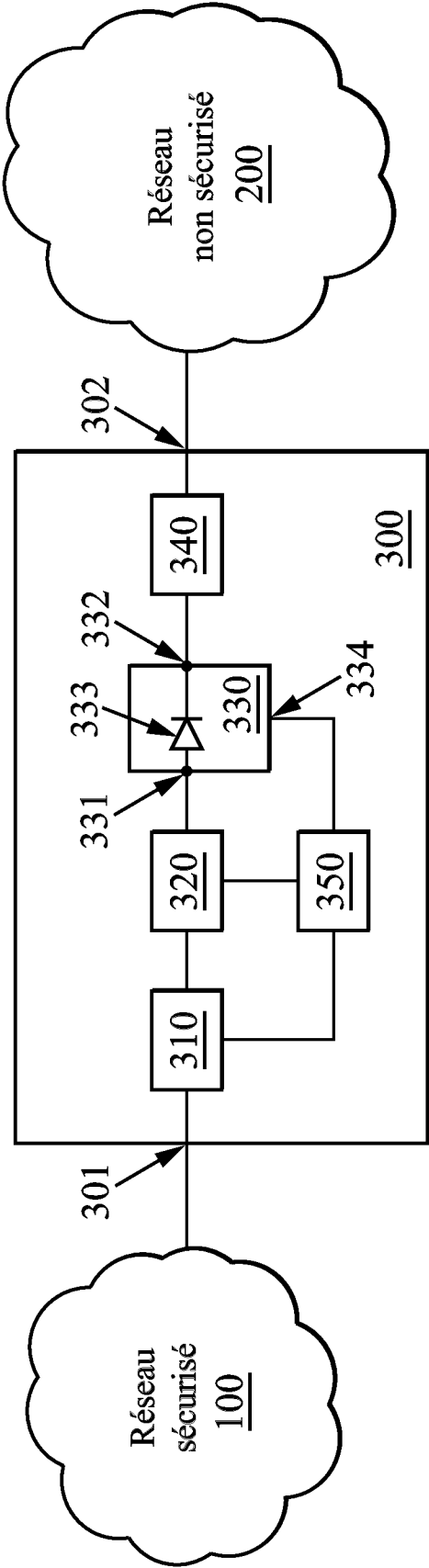


FIG. 1

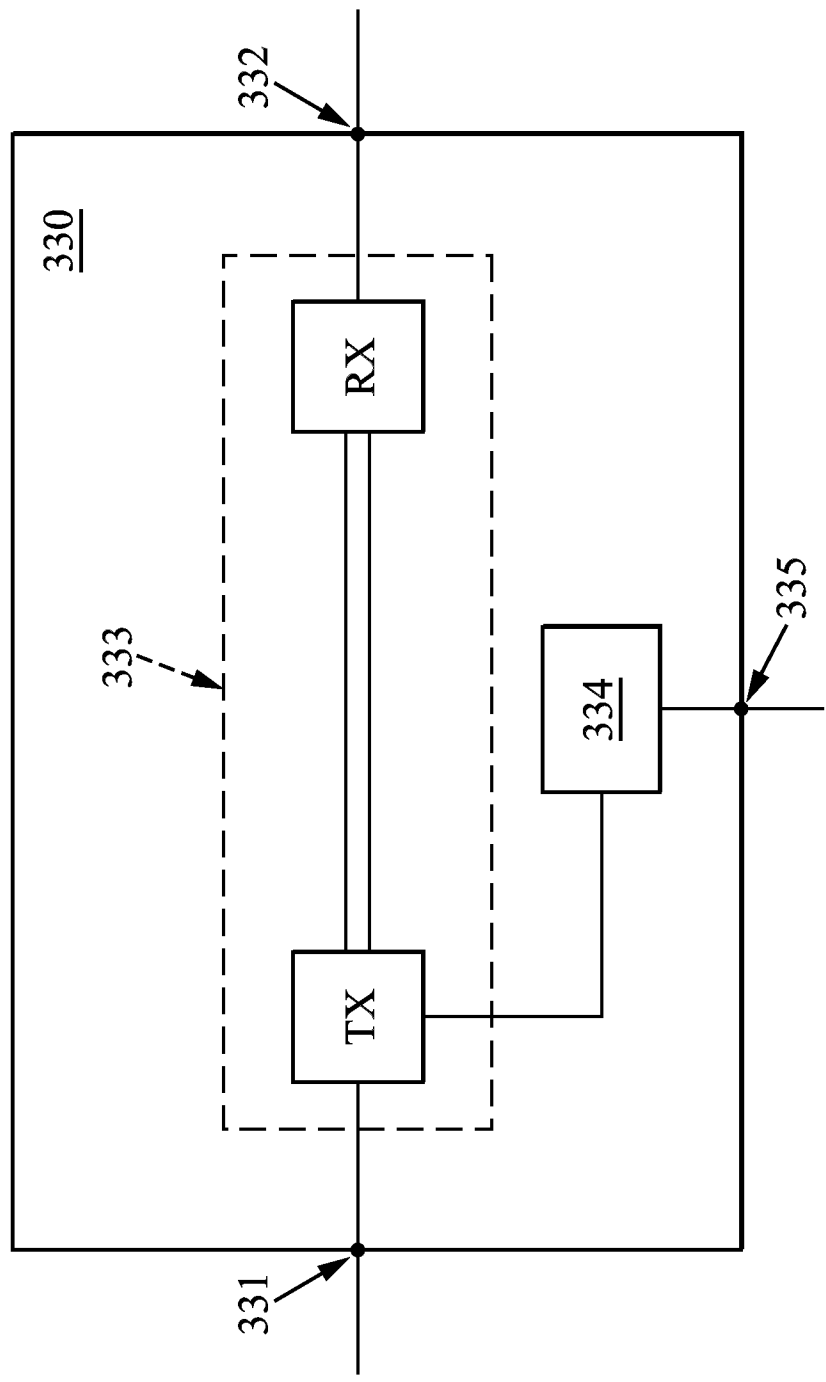


FIG. 2

3/3

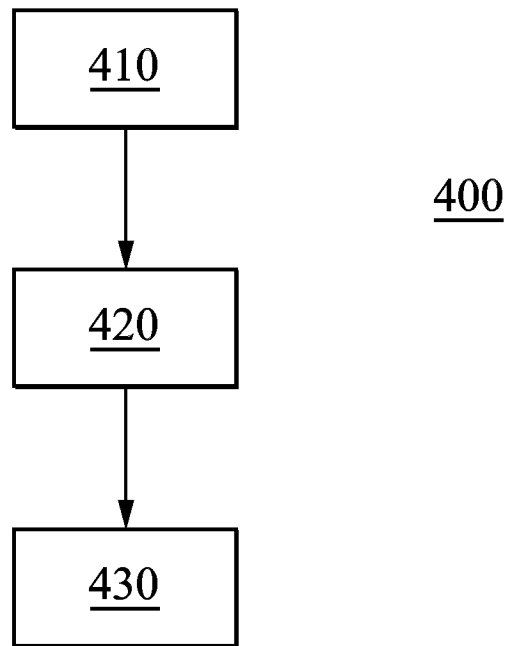


FIG. 3

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2017/084232

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06F21/60 H04L29/06
ADD.

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)
G06F H04L

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.
Y	"Chapter 7: Establishing Secure Enclaves; Chapter 8: Exception, Anomaly, and Threat Detection; Chapter 9: Monitoring Enclaves ED - Eric D Knapp", 1 January 2011 (2011-01-01), INDUSTRIAL NETWORK SECURITY. SECURING CRITICAL INFRASTRUCTURE NETWORKS FOR SMART GRID, SCADA, AND OTHER INDURSTIAL CONTROL SYSTEMS, SYNGRESS, PAGE(S) 147 - 247, XP002687973, ISBN: 978-1-59749-645-2 page 157 page 163 pages 166-167 page 181 pages 215-218 pages 234-236 ----- -/-	1-11



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

31 January 2018

Date of mailing of the international search report

07/02/2018

Name and mailing address of the ISA/

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040,
Fax: (+31-70) 340-3016

Authorized officer

Erdene-Ochir, O

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2017/084232

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2015/161397 A1 (COOK STEPHEN J [GB] ET AL) 11 June 2015 (2015-06-11) paragraphs [0001] - [0005] paragraphs [0030] - [0035] paragraphs [0040] - [0043] figures 4-6 -----	1-11
A	Austin Scott ET AL: "Tactical Data Diodes in Industrial Automation and Control Systems", 18 May 2015 (2015-05-18), pages 1-32, XP055290300, GIAC directory of certified professionals Retrieved from the Internet: URL: http://www.giac.org/paper/gicsp/242/tactical-data-diodes-industrial-automation-control-systems/142041 [retrieved on 2016-07-21] pages 2-3 pages 7-10 pages 13-15 page 29 -----	1-11
A	US 2016/063269 A1 (LIDEN LARS H [US] ET AL) 3 March 2016 (2016-03-03) paragraphs [0001] - [0004] paragraphs [0031] - [0033] paragraphs [0046] - [0050] paragraphs [0115] - [0117] figure 1 -----	1-11

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/EP2017/084232

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2015161397 A1	11-06-2015	CN 105814580 A	27-07-2016
		EP 3077953 A1	12-10-2016
		US 2015161397 A1	11-06-2015
		WO 2015084689 A1	11-06-2015

US 2016063269 A1	03-03-2016	CN 106663175 A	10-05-2017
		JP 2017530460 A	12-10-2017
		US 2016063269 A1	03-03-2016
		WO 2016036628 A1	10-03-2016

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale n°

PCT/EP2017/084232

A. CLASSEMENT DE L'OBJET DE LA DEMANDE INV. G06F21/60 H04L29/06 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) G06F H04L		
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
Y	"Chapter 7: Establishing Secure Enclaves; Chapter 8: Exception, Anomaly, and Threat Detection; Chapter 9: Monitoring Enclaves ED - Eric D Knapp", 1 janvier 2011 (2011-01-01), INDUSTRIAL NETWORK SECURITY. SECURING CRITICAL INFRASTRUCTURE NETWORKS FOR SMART GRID, SCADA, AND OTHER INDURSTIAL CONTROL SYSTEMS, SYNGRESS, PAGE(S) 147 - 247, XP002687973, ISBN: 978-1-59749-645-2 page 157 page 163 pages 166-167 page 181 pages 215-218 pages 234-236 ----- -/-	1-11
☒ 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 31 janvier 2018		Date d'expédition du présent rapport de recherche internationale 07/02/2018
Nom et adresse postale de l'administration chargée de la recherche internationale Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016		Fonctionnaire autorisé Erdene-Ochir, O

C(suite). DOCUMENTS CONSIDERES COMME PERTINENTS		
Catégorie*	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
Y	US 2015/161397 A1 (COOK STEPHEN J [GB] ET AL) 11 juin 2015 (2015-06-11) alinéas [0001] - [0005] alinéas [0030] - [0035] alinéas [0040] - [0043] figures 4-6 -----	1-11
A	Austin Scott ET AL: "Tactical Data Diodes in Industrial Automation and Control Systems", 18 mai 2015 (2015-05-18), pages 1-32, XP055290300, GIAC directory of certified professionals Extrait de l'Internet: URL: http://www.giac.org/paper/gicsp/242/tactical-data-diodes-industrial-automation-control-systems/142041 [extrait le 2016-07-21] pages 2-3 pages 7-10 pages 13-15 page 29 -----	1-11
A	US 2016/063269 A1 (LIDEN LARS H [US] ET AL) 3 mars 2016 (2016-03-03) alinéas [0001] - [0004] alinéas [0031] - [0033] alinéas [0046] - [0050] alinéas [0115] - [0117] figure 1 -----	1-11

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Demande internationale n°

PCT/EP2017/084232

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
US 2015161397 A1	11-06-2015	CN 105814580 A	27-07-2016
		EP 3077953 A1	12-10-2016
		US 2015161397 A1	11-06-2015
		WO 2015084689 A1	11-06-2015

US 2016063269 A1	03-03-2016	CN 106663175 A	10-05-2017
		JP 2017530460 A	12-10-2017
		US 2016063269 A1	03-03-2016
		WO 2016036628 A1	10-03-2016
