(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
02 janvier 2025 (02.01.2025)

WIPO | PCT

(10) Numéro de publication internationale
WO 2025/003201 A1

(51) Classification internationale des brevets :
H04L 9/40 (2022.01)

(21) Numéro de la demande internationale :
PCT/EP2024/067921

(22) Date de dépôt international :
26 juin 2024 (26.06.2024)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
FR2306799 28 juin 2023 (28.06.2023) FR

(71) Déposant : **ORANGE** [FR/FR] ; 111, quai du Président Roosevelt, 92130 Issy-les-Moulineaux (FR).

(72) Inventeurs : **HAMON, Yoann** ; ORANGE - Intellectual Property and Licensing, Orange Gardens - 44 Avenue de la République, CS 50010, 92326 Chatillon (FR). **ESNAULT, Régis** ; ORANGE - Intellectual Property and Licensing, Orange Gardens - 44 Avenue de la République, CS 50010, 92326 Chatillon (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, CV, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IQ, IR, IS, IT, JM, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, MG, MK, MN, MU, 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, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW.

WO 2025/003201 A1

(54) **Title:** METHODS FOR THE PROTECTION OF A PIECE OF EQUIPMENT AND FOR THE TRANSMISSION OF DATA, AND CORRESPONDING ELECTRONIC DEVICES AND ELECTRONIC ASSEMBLY, COMPUTER PROGRAM PRODUCTS AND INFORMATION STORAGE MEDIA

(54) **Titre :** PROCÉDÉS DE PROTECTION D'UN ÉQUIPEMENT ET DE TRANSMISSION DE DONNÉES, DISPOSITIFS ET ENSEMBLE ÉLECTRONIQUES, PRODUITS PROGRAMMES D'ORDINATEUR ET SUPPORTS D'INFORMATION CORRESPONDANTS

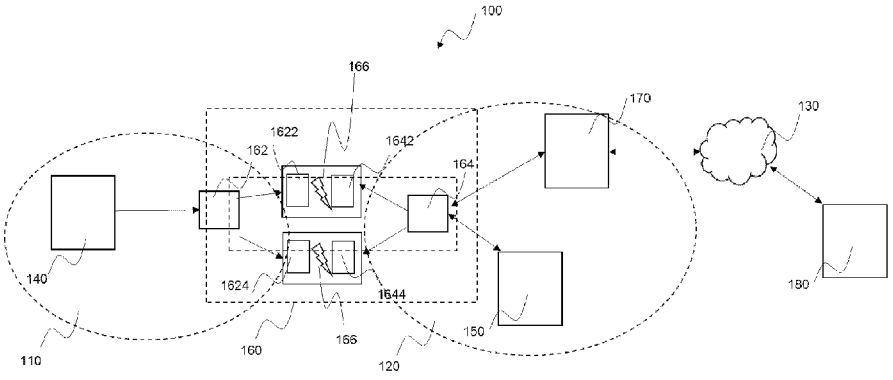

Fig 1

(57) **Abstract:** The invention relates to a method for protecting a piece of equipment in a communication network partitioned into a first portion and a second portion that is interconnected with the first portion via a first device in the first portion and a second device in the second portion, the method comprising: • transmitting, to the second device, an address of a piece of equipment in the first portion of the network; • transcoding data received from the second device into a structured data packet comprising an identifier for addressing the piece of equipment that is the recipient of the packet in the first portion; • transmitting the packet to the recipient piece of equipment. The invention also relates in particular to a transmission method implemented by a second electronic device in a second portion of the communication network, as well as to the corresponding electronic devices and electronic assembly, computer program products and information storage media.

(57) **Abrégé :** L'invention concerne un procédé de protection d' un équipement d'un réseau de communication partitionné en une première portion, et une seconde portion interconnectée avec la première portion via un premier dispositif de la première portion et un second dispositif de la seconde portion, le procédé comportant : • une transmission au second dispositif d'une adresse d'un équipement de la première portion du réseau; • un transcodage de données reçues du second dispositif en un paquet de données structuré comportant

[Suite sur la page suivante]

(84) **États désignés** *(sauf indication contraire, pour tout titre de protection régionale disponible)* : ARIPO (BW, CV, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SC, SD, SL, ST, SZ, TZ, UG, ZM, ZW), eurasien (AM, AZ, BY, KG, KZ, RU, TJ, TM), européen (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, ME, 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))*

— *en noir et blanc ; la demande internationale telle que déposée était en couleur ou en échelle de gris et est disponible sur PATENTSCOPE pour téléchargement.*

un identifiant d'adressage de l'équipement destinataire du paquet sur la première portion; • une transmission du paquet à l'équipement destinataire. Elle concerne également notamment un procédé de transmission, mis en œuvre par un second dispositif électronique d'une seconde portion du réseau de communication, ainsi que les dispositifs et ensemble électroniques, produits programme d'ordinateur et supports d'informations correspondants.

DESCRIPTION

Titre de l'invention : Procédés de protection d'un équipement et de transmission de données, dispositifs et ensemble électroniques, produits programmes d'ordinateur et supports d'information correspondants

Domaine technique

La présente application se rapporte au domaine de la sécurisation d'au moins une portion d'un réseau de communication.

Elle concerne notamment un procédé de protection d'au moins un équipement, mis en œuvre par un premier dispositif électronique d'une première portion d'un réseau de communication, et un procédé de transmission de donnée(s), mis en œuvre par un second dispositif électronique d'une seconde portion d'un réseau de communication, ainsi que les dispositifs et ensemble électroniques, produits programme d'ordinateur et supports d'informations correspondants.

1. Etat de la technique

La présente invention est relative à la protection d'au moins un équipement accessible via un réseau de communication. Il peut s'agir par exemple d'un équipement manipulant des données sensibles, ou effectuant des traitements sensibles, et pouvant donc être la cible d'attaque de tiers malveillants, soit pour accéder de façon indue à des données sensibles, soit pour perturber, voire empêcher, certains traitements via la propagation à l'équipement d'un virus informatique.

Cet équipement fait par exemple partie d'un réseau privé d'entreprise ou d'un réseau domestique, interconnecté à un réseau public tel qu'internet.

Des exemples de données sensibles incluent des données à caractère personnel (données médicales, bancaires etc..), des données industrielles (comme des plans d'objet manufacturés, des données relatives à la production de certaines machines industrielles comme des résultats de mesures, un nombre de pièces produites, etc..) des historiques de commandes reçues par des équipements industrielles, des alertes, etc.

Des tiers malveillants peuvent être par exemple être tentés de mettre hors d'état d'usage l'équipement, pour nuire à une entreprise ou obtenir une rançon. Des solutions de sécurisation de réseaux privés ont été développées pour protéger un équipement ou une pluralité d'équipements appartenant un même réseau privé de telles attaques. On peut citer par exemple des solutions à base de pares-feux (« firewalls » selon la terminologie anglaise) et/ou des systèmes de détection d'intrusion. On peut citer également l'utilisation de réseaux privés virtuels (RPV) (ou VPN pour Virtual Private Network selon la terminologie anglaise) isolant par cryptage, au sein d'un réseau étendu, les échanges entre les équipements du réseau étendu appartenant au réseau privé virtuel, De telles solutions permettent de limiter les communications avec les équipements extérieurs au réseau privé aux communications émises depuis le réseau privé vers ces équipements

« extérieurs », et empêchent ainsi les accès depuis l'extérieur du réseau à un équipement à protéger.

Cependant ces solutions, parfois appelés « diodes réseau », sont parfois inappropriées et très contraignantes pour protéger certains équipements électroniques comme des machines industrielles. En effet, de telles solutions permettent seulement les remontées d'informations à l'initiative de l'équipement protégé. Un logiciel s'exécutant sur un appareil électronique extérieur au réseau privé ne peut donc pas interroger un équipement protégé pour obtenir en retour une donnée. De telles solutions limitent fortement, voire empêchent, l'usage de certains protocoles de communication basés sur de telles requêtes et notamment de certains protocoles très répandus dans le domaine industriel (comme, dans le domaine industriel, les protocoles OPC-UA ou ModBus utilisés par de nombreuses machines-outils du marché). Elles ne sont donc pas adaptées à la protection de certains équipements du marché.

La présente demande a pour objet de proposer des améliorations à au moins certains des inconvénients de l'état de la technique.

2. Exposé de l'invention

La présente demande vise à améliorer la situation à l'aide d'un procédé de protection d'au moins un équipement d'un réseau de communication partitionné en une pluralité de portions comprenant au moins une première portion, comprenant ledit équipement, et au moins une seconde portion interconnectée avec ladite première portion via un premier dispositif de ladite première portion et un second dispositif de ladite seconde portion, ledit procédé comprenant :

- une transmission audit second dispositif d' au moins un identifiant d'adressage dudit équipement de ladite première portion dudit réseau de communication ;
- un transcodage de données reçues dudit second dispositif en au moins un paquet de données structuré comportant au moins un identifiant d'adressage d'un équipement destinataire dudit paquet sur ladite première portion ;
- une transmission dudit paquet audit équipement destinataire ;

au moins un desdits transcodage et/ou transmission étant effectué de façon conditionnelle en tenant compte d'au moins une règle de filtrage relative au contenu dudit paquet.

Dans certains modes de réalisation, ladite règle de filtrage tient compte d'au moins un élément contenu dans ledit paquet parmi les éléments suivants :

- une désignation d'un appareil émetteur dudit paquet ;
- une information d'adressage relative à au moins une donnée dudit équipement ;
- un type d'accès à effectuer sur ladite donnée ;
- une désignation d'un protocole de communication utilisé par ledit paque ;
- une combinaison d'au moins deux desdits éléments ci-avant.

Dans certains modes de réalisation, ledit filtrage est effectué avant ledit transcodage.

Dans certains modes de réalisation, ledit filtrage est effectué après ledit transcodage.

Dans certains modes de réalisation, lesdits premiers et second dispositifs communiquent entre eux via au moins deux chemins de communication, un premier chemin de communication unidirectionnel permettant au premier dispositif de recevoir des données dudit second dispositif, et un second chemin de communication, unidirectionnel, permettant au premier dispositif d'envoyer audit second dispositif une réponse audit paquet transmis audit équipement destinataire.

Dans certains modes de réalisation, ledit transcodage comprend une désérialisation desdites données.

La présente demande concerne également un procédé de transmission d'au moins une donnée destinée à au moins un équipement d'un réseau de communication partitionné en une pluralité de portions comprenant au moins une première portion, et au moins une seconde portion interconnectée avec ladite première portion via un premier dispositif de ladite première portion et un second dispositif de ladite seconde portion ; ledit procédé comprenant :

- une affectation audit second dispositif, comme identifiant d'adressage sur ladite seconde portion dudit réseau, d'au moins un identifiant d'adressage d'un équipement de ladite première portion
- sur réception d'un paquet structuré de données ayant comme adresse de destination ledit identifiant d'adressage, une sérialisation des données dudit paquet ; et
- une émission desdites données sérialisées vers ledit premier dispositif.

au moins une de ladite sérialisation et/ou ladite émission étant effectuée de façon conditionnelle en tenant compte d'au moins une règle de filtrage relative au contenu dudit paquet.

Dans certains modes de réalisation, ladite règle de filtrage tient compte d'au moins un élément contenu dans ledit paquet parmi les éléments suivants :

- une désignation d'un appareil émetteur dudit paquet ;
- une information d'adressage relative à au moins une donnée dudit équipement;
- un type d'accès à effectuer sur ladite donnée ;
- une désignation d'un protocole de communication utilisé par ledit paquet;
- une combinaison d'au moins deux desdits éléments ci-avant.

Dans certains modes de réalisation, le procédé de transmission comprend une obtention d'un descriptif relatif audit équipement de ladite première portion dudit réseau de communication comportant ledit au moins un identifiant d'adressage dudit au moins un équipement sur ladite première portion dudit réseau de communication.

Dans certains modes de réalisation, ledit filtrage est effectué sur les données sérialisées

Dans certains modes de réalisation, ledit filtrage est effectué avant ladite sérialisation.

Dans certains modes de réalisation, lesdits premiers et second dispositifs communiquent entre eux via au moins deux chemins de communication unidirectionnel, un premier chemin de communication unidirectionnel permettant au second dispositif de transmettre des données audit premier dispositif, et un second chemin de communication, unidirectionnel, permettant au second dispositif de recevoir du premier dispositif une réponse auxdites données transmises audit premier dispositif.

Les caractéristiques, présentées isolément dans la présente demande en lien avec certains modes de réalisation de l'un des procédés de la présente demande peuvent être combinées entre elles selon d'autres modes de réalisation de ce procédé.

Selon un autre aspect, la présente demande concerne également un dispositif électronique adapté à mettre en œuvre au moins un des procédés de la présente demande dans l'un quelconque de ses modes de réalisation.

La présente demande concerne ainsi un premier dispositif électronique d'un réseau de communication partitionné en une pluralité de portions comprenant au moins une première portion, comprenant au moins un équipement à protéger et ledit premier dispositif, et au moins une seconde portion interconnectée avec ladite première portion via le premier dispositif et un second dispositif de ladite seconde portion, ledit premier dispositif comprenant un moins un processeur configuré pour :

- une transmission audit second dispositif d'au moins un identifiant d'adressage duit équipement de ladite première portion dudit réseau de communication ;
- un transcodage de données reçues dudit second dispositif en au moins un paquet de données structuré comportant au moins un identifiant d'adressage d'un équipement destinataire dudit paquet sur ladite première portion ;
- une transmission dudit paquet audit équipement destinataire ;

au moins un desdits transcodage et/ou transmission étant effectuée de façon conditionnelle en tenant compte d'au moins une règle de filtrage.

La présente demande concerne aussi un second dispositif électronique d'un réseau de communication partitionné en une pluralité de portions comprenant au moins une première portion, comprenant au moins un équipement, et au moins une seconde portion comprenant ledit second dispositif, et interconnectée avec ladite première portion via un premier dispositif de ladite première portion et le second dispositif; ledit second dispositif comprenant un moins un processeur configuré pour :

- une affectation audit second dispositif, comme identifiant d'adressage sur ladite seconde portion dudit réseau, d'au moins un identifiant d'adressage d'un équipement de ladite première portion
- sur réception d'un paquet structuré de données ayant comme adresse de destination ledit identifiant d'adressage, une sérialisation des données dudit paquet et ;

- une émission desdites données sérialisées vers ledit premier dispositif.

au moins une de ladite sérialisation et/ou ladite émission étant effectuée de façon conditionnelle en tenant compte d'au moins une règle de filtrage relative au contenu dudit paquet.

Selon un autre aspect, la présente demande concerne également un ensemble électronique de protection d'au moins un équipement d'un réseau de communication partitionné en une pluralité de portions comprenant au moins une première portion, comprenant ledit équipement, et au moins une seconde portion interconnectée avec ladite première portion via au moins un premier dispositif dudit ensemble électronique, ledit premier dispositif appartenant à ladite première portion, et au moins un second dispositif dudit ensemble électronique, ledit second dispositif appartenant à ladite seconde portion,

- ledit au moins un premier dispositif électronique comprenant un moins un processeur configuré pour :
  - une transmission audit second dispositif d' au moins un identifiant d'adressage dudit équipement de ladite première portion dudit réseau de communication ;
  - un transcodage de données reçues dudit second dispositif en au moins un premier paquet de données structuré comportant au moins un identifiant d'adressage d'un équipement destinataire dudit premier paquet sur ladite première portion ;
  - une transmission dudit premier paquet audit équipement destinataire ;

  au moins un desdits transcodage et/ou transmission étant effectuée de façon conditionnelle en tenant compte d'au moins une première règle de filtrage relative au contenu dudit premier paquet.
- ledit au moins un second dispositif électronique comprenant un moins un processeur configuré pour :
  - une affectation audit second dispositif, comme identifiant d'adressage sur ladite seconde portion dudit réseau, d'au moins un identifiant d'adressage d'un équipement de ladite première portion
  - sur réception d'un second paquet structuré de données ayant comme adresse de destination ledit identifiant d'adressage, une sérialisation des données dudit second paquet et ;
  - une émission desdites données sérialisées vers ledit premier dispositif.

au moins une de ladite sérialisation et/ou ladite émission étant effectuée de façon conditionnelle en tenant compte d'au moins une seconde règle de filtrage relative au contenu dudit second paquet.

Selon un autre aspect, la présente demande concerne également un système comprenant au moins un équipement à protéger et au moins un ensemble électronique de protection dudit au

moins un équipement, dans un réseau de communication partitionné en une pluralité de portions comprenant au moins une première portion comprenant ledit équipement, et au moins une seconde portion interconnectée avec ladite première portion via au moins un premier dispositif dudit ensemble électronique, ledit premier dispositif appartenant à ladite première portion et au moins un second dispositif dudit ensemble électronique, ledit second dispositif appartenant à ladite seconde portion,:

- ledit au moins un premier dispositif électronique comprenant un moins un processeur configuré pour :
  - une transmission audit second dispositif d' au moins un identifiant d'adressage dudit équipement de ladite première portion dudit réseau de communication ;
  - un transcodage de données reçues dudit second dispositif en au moins un premier paquet de données structuré comportant au moins un identifiant d'adressage d'un équipement destinataire dudit premier paquet sur ladite première portion ;
  - une transmission dudit premier paquet audit équipement destinataire ;

  au moins un desdits transcodage et/ou transmission étant effectuée de façon conditionnelle en tenant compte d'au moins une première règle de filtrage relative au contenu dudit premier paquet
- ledit au moins un second dispositif électronique comprenant un moins un processeur configuré pour :
  - une affectation audit second dispositif, comme identifiant d'adressage sur ladite seconde portion dudit réseau, d'au moins un identifiant d'adressage d'un équipement de ladite première portion
  - sur réception d'un paquet structuré de données ayant comme adresse de destination ledit identifiant d'adressage, une sérialisation des données dudit second paquet et ;
  - une émission desdites données sérialisées vers ledit premier dispositif.

  au moins une de ladite sérialisation et/ou ladite émission étant effectuée de façon conditionnelle en tenant compte d'au moins une seconde règle de filtrage relative au contenu dudit second paquet.

La présente demande concerne aussi un programme d'ordinateur comprenant des instructions pour la mise en œuvre des divers modes de réalisation de l'un au moins des procédés ci-dessus, lorsque ledit programme est exécuté par un processeur, et un support d'informations lisible par un dispositif électronique et sur lequel est enregistré le programme d'ordinateur.

La présente demande concerne ainsi un programme d'ordinateur comprenant des instructions pour la mise en œuvre, lorsque le programme est exécuté par un processeur d'un premier dispositif électronique, d'un procédé de protection d'au moins un équipement d'un réseau de communication partitionné en une pluralité de portions comprenant au moins une première

portion, comprenant ledit équipement et ledit premier dispositif, et au moins une seconde portion interconnectée avec ladite première portion via le premier dispositif et un second dispositif de ladite seconde portion, ledit procédé comprenant :

- une transmission audit second dispositif d' au moins un identifiant d'adressage dudit équipement de ladite première portion dudit réseau de communication ;
- un transcodage de données reçues dudit second dispositif en au moins un paquet de données structuré comportant au moins un identifiant d'adressage d'un équipement destinataire dudit paquet sur ladite première portion ;
- une transmission dudit paquet audit équipement destinataire ;

au moins un desdits transcodage et/ou transmission étant effectuée de façon conditionnelle en tenant compte d'au moins une règle de filtrage relative au contenu dudit paquet.

Par ailleurs, la présente demande concerne un programme d'ordinateur comprenant des instructions pour la mise en œuvre, lorsque le programme est exécuté par un processeur d'un second dispositif électronique, d'un procédé de transmission d'au moins une donnée en provenance d'au moins un équipement d'un réseau de communication partitionné en une pluralité de portions comprenant au moins une première portion, et au moins une seconde portion, comprenant ledit second dispositif et interconnectée avec ladite première portion via un premier dispositif de ladite première portion et le second dispositif; ledit procédé comprenant :

- une affectation audit second dispositif, comme identifiant d'adressage sur ladite seconde portion dudit réseau, d'au moins un identifiant d'adressage d'un équipement de ladite première portion
- sur réception d'un paquet structuré de données ayant comme adresse de destination ledit identifiant d'adressage, une sérialisation des données dudit paquet et ;
- une émission desdites données sérialisées vers ledit premier dispositif.

au moins une de ladite sérialisation et/ou ladite émission étant effectuée de façon conditionnelle en tenant compte d'au moins une règle de filtrage relative au contenu dudit paquet.

La présente demande concerne aussi un support d'informations lisible par un processeur d'un premier dispositif électronique et sur lequel est enregistré un programme d'ordinateur comprenant des instructions pour la mise en œuvre, lorsque le programme est exécuté par le processeur, d'un procédé de protection d'au moins un équipement d'un réseau de communication partitionné en une pluralité de portions comprenant au moins une première portion, comprenant ledit équipement et ledit premier dispositif, et au moins une seconde portion interconnectée avec ladite première portion via le premier dispositif de ladite première portion et un second dispositif de ladite seconde portion, ledit procédé comprenant :

- une transmission audit second dispositif d' au moins un identifiant d'adressage dudit équipement de ladite première portion dudit réseau de communication ;

- un transcodage de données reçues dudit second dispositif en au moins un paquet de données structuré comportant au moins un identifiant d'adressage d'un équipement destinataire dudit paquet sur ladite première portion ;
- une transmission dudit paquet audit équipement destinataire ;

au moins un desdits transcodage et/ou transmission étant effectuée de façon conditionnelle en tenant compte d'au moins une règle de filtrage relative au contenu dudit paquet.

La présente demande concerne par ailleurs un support d'informations lisible par un processeur d'un second dispositif électronique et sur lequel est enregistré un programme d'ordinateur comprenant des instructions pour la mise en œuvre, lorsque le programme est exécuté par le processeur, d'un procédé de transmission d'au moins une donnée en provenance d'au moins un équipement d'un réseau de communication partitionné en une pluralité de portions comprenant au moins une première portion, et au moins une seconde portion comprenant ledit second dispositif et interconnectée avec ladite première portion via un premier dispositif de ladite première portion et le second dispositif de ladite seconde portion, ledit procédé comprenant :

- une affectation audit second dispositif, comme identifiant d'adressage sur ladite seconde portion dudit réseau, d'au moins un identifiant d'adressage d'un équipement de ladite première portion ;
- Sur réception d'un paquet structuré de données ayant comme adresse de destination ledit identifiant d'adressage, une sérialisation des données dudit paquet et ;
- Une émission desdites données sérialisées vers ledit premier dispositif.

au moins une de ladite sérialisation et/ou ladite émission étant effectuée de façon conditionnelle en tenant compte d'au moins une règle de filtrage relative au contenu dudit paquet.

Les programmes mentionnés ci-dessus peuvent utiliser n'importe quel langage de programmation, et être sous la forme de code source, code objet, ou de code intermédiaire entre code source et code objet, tel que dans une forme partiellement compilée, ou dans n'importe quelle autre forme souhaitable.

Les supports d'informations (ou d'enregistrement) mentionnés dans la présente demande peuvent être n'importe quelle entité ou dispositif capable de stocker le programme. Par exemple, un support d'informations peut comporter un moyen de stockage, tel qu'une ROM, par exemple un CD ROM ou une ROM de circuit microélectronique, ou encore un moyen d'enregistrement magnétique.

Un tel moyen de stockage peut par exemple être un disque dur, une mémoire flash, etc.

D'autre part, un support d'informations peut être un support d'informations transmissible tel qu'un signal électrique ou optique, qui peut être acheminé via un câble électrique ou optique, par radio ou par d'autres moyens. Un programme selon l'invention peut être en particulier téléchargé sur un réseau de type Internet.

Alternativement, un support d'informations peut être un circuit intégré dans lequel un

programme est incorporé, le circuit étant adapté pour exécuter ou pour être utilisé dans l'exécution de l'un quelconque des modes de réalisation d'au moins un des procédés objets de la présente demande de brevet.

De façon générale, par obtention d'un élément, on entend dans la présente demande par exemple une réception de cet élément depuis un réseau de communication, une acquisition de cet élément (via par exemple des éléments d'interface utilisateur , des capteurs, etc.), une création de cet élément par divers moyens de traitement tels que par copie, encodage, décodage, transformation etc et/ou un accès de cet élément depuis un support de stockage local ou distant accessible à au moins un appareil (comme le premier et/ou le second dispositif de l'ensemble) mettant en œuvre, au moins partiellement, cette obtention.

3. Brève description des dessins

D'autres caractéristiques et avantages de l'invention apparaîtront plus clairement à la lecture de la description suivante de modes de réalisation particuliers, donnés à titre de simples exemples illustratifs et non limitatifs, et des dessins annexés, parmi lesquels :

La [Fig 1] présente une vue simplifiée d'un système, cité à titre d'exemple, dans lequel au moins certains modes de réalisation des procédés de la présente demande peuvent être implémentés,

La [Fig 2] présente une vue simplifiée d'un dispositif adapté à mettre en œuvre au moins certains modes de réalisation d'au moins un des procédés de la présente demande,

La [Fig 3] présente un aperçu du procédé de protection de la présente demande, dans certains de ses modes de réalisation

La [Fig 4] présente un aperçu du procédé de transmission de données de la présente demande, dans certains de ses modes de réalisation

La [Fig 5] une vue simplifiée d'un système 500, cité à titre d'exemple, dans lequel au moins certains modes de réalisation du procédé de la présente demande peuvent être implémentés

4. Description des modes de réalisation

La présente demande vise à fournir une solution simple et efficace permettant à la fois de protéger un ou plusieurs équipements d'un réseau de communication contre des attaques informatiques, notamment externes à ce réseau de communication, tout en permettant à des appareils électroniques, situés par exemple dans une portion non protégée du réseau de communication ou à l'extérieur du réseau de communication, d'accéder (en lecture et en écriture) et de manière sécurisée, à au moins certaines données de ces équipements à protéger. Pour cela, la demande propose d'équiper le réseau de communication d'au moins deux dispositifs, ceux-ci réalisant une partition du réseau de communication en au moins deux portions.

Par partition, on entend ici un partage du réseau de communication en une pluralité de portions comprenant chacune au moins un appareil électronique, disjointes deux à deux (hormis certains

éléments d'interconnexion entre les au moins deux dispositifs comme précisé ci-après) et dont la réunion reconstitue le réseau de communication.

Au moins une première de ces portions est une portion (dite « protégée ») inaccessible directement depuis un appareil électronique situé à l'extérieur de cette première portion, cette première portion comprenant au moins un équipement à protéger. Au moins une seconde portion dite « exposée » (ie externe à cette première portion protégée) est accessible, directement et/ou via des équipements d'interconnexion, à des appareils extérieurs à la première portion (comme des appareils situés dans une autre « première » portion protégée que la première portion « protégée » où se situe l'équipement, et/ou des appareils de la seconde portion, et/ou des appareils extérieurs au réseau de communication).

Le ou les équipement(s) à protéger peuvent par exemple être des machines industrielles.

Selon la présente demande, les demandes d'accès à un équipement en provenance d'un appareil extérieur à la première portion sont filtrées par le premier et/ou le second dispositif, en application de règles de filtrage, de façon à ne conserver que les demandes d'accès jugées sûres. Par exemple, seules peuvent être conservées les demandes concernant des équipements non critiques de la première portion. Selon un autre exemple, seules peuvent être conservées les demandes de lecture de zone(s) mémoire d'un équipement de la première portion. Selon encore un autre exemple, seules peuvent être conservées les demandes d'écriture relatives à des zones mémoires « non critiques » d'un équipement de la première portion émises par certains appareils (comme un appareil d'un administrateur du réseau).

Des règles de filtrage différentes peuvent être appliquées par le premier et/ou le second dispositif. Par exemple, dans des topologies réseau où le premier dispositif est susceptible de recevoir des demandes de plusieurs seconds dispositifs interconnectant chacun la première portion (protégée) avec différentes secondes portions, exposées, la ou les règle(s) de filtrage appliquée(s) par le premier dispositif peut tenir compte du second dispositif de qui les demandes ont été reçues. En particulier, dans certains modes de réalisation, le premier dispositif peut recevoir des demandes provenant d'un « second dispositif » ne mettant en œuvre aucun filtrage.

Il peut s'agir aussi de règles identiques ou similaires. L'application d'une même règle au niveau du second dispositif puis du premier dispositif peut permettre, au niveau du second dispositif de supprimer plus tôt , dans la chaîne de traitement, certains paquets (conformément aux règles de filtrage), évitant ainsi des traitements inutiles. Au niveau du premier dispositif, elle peut permettre de se prémunir contre une éventuelle corruption du second dispositif (situé dans une portion « exposée » du réseau) et notamment de ses règles de filtrage.

Dans certains modes de réalisation, le premier dispositif et le second dispositif communiquent uniquement via des moyens de communication unidirectionnels. Ainsi, les demandes d'appareil tiers reçues par le second dispositif peuvent être transmises par le second dispositif (depuis la portion exposée) au premier dispositif via un premier chemin de communication unidirectionnel.

N'autoriser que des communications unidirectionnelles peut aider à un meilleur contrôle des échanges entre un appareil tiers et un équipement (via l'ensemble électronique) et donc à une meilleure prévention des attaques provenant d'appareils tiers.

On note que des messages, correspondant par exemple des messages « UDP » de l'équipement ou à des réponses éventuelles à des demandes, peuvent être transmis via un second chemin de communication unidirectionnel de la portion protégée vers la portion exposée. Des exemples de réponse incluent, lorsqu'il s'agit d'une demande de lecture, des valeurs de données de l'équipement destinataire de la demande et/ou dans le cas d'une demande d'écriture, une confirmation de réception de la demande ou une confirmation d'écriture. Dans certains modes de réalisation, comme illustré 1, les messages (comme des messages « UDP » ou des réponses) sont transmis du premier dispositif vers le second dispositif (via le second chemin de communication). En variante, elles peuvent être transmises de façon transparente au premier et second dispositif (via un second chemin de communication ne transitant pas par les premier et second dispositifs). Dans certaines modes de réalisations, où les messages transitent via le premier et le second dispositif, un filtrage des messages peut éventuellement être mis en œuvre par le premier dispositif et/ou le second dispositif (de façon à s'assurer par exemple qu'aucune donnée sensible ne puisse être communiquer à un appareil extérieur de la première portion). Ce filtrage peut s'appuyer sur des règles identiques ou similaires à celles utilisées lors du premier chemin de communication (par exemple elles peuvent porter sur les mêmes registres) ou sur des règles différentes.

Ainsi, selon la présente demande, il est possible de recevoir des requêtes d'un appareil tiers souhaitant obtenir des données en provenance de l'équipement à protéger, et de lui fournir en retour ces données, en toute sécurité pour l'équipement à protéger.

La présente demande peut en particulier aider à la fois à la protection d'une portion du réseau, tout en permettant le pilotage d'au moins certains équipements de cette première portion depuis l'extérieur du réseau.

L'ensemble logique comprenant les au moins un premier et second dispositifs et les moyens de communication (unidirectionnels par exemple) entre ces au moins deux dispositifs est également appelé dans la présente demande de brevet « ensemble électronique », « ensemble électronique de protection » ou « Diode intelligente » (ou Smart Diode selon la terminologie anglaise). Selon les modes de réalisation, il peut s'agir d'un ensemble virtuel, encapsulant virtuellement les premier et second dispositifs et des premiers moyens de communication unidirectionnels dans un premier sens de communication (du second dispositif vers le premier dispositif), et optionnellement des seconds moyens de communication unidirectionnels dans un second sens de communication, opposé au premier sens) ou d'un ensemble physique (comme un élément hardware), ayant par exemple un boîtier dans lequel sont installés les au moins un premier et second dispositifs et leurs moyens de communication mutuelle. Cet ensemble peut comprendre

selon les modes de réalisation, et la topologie du réseau (par exemple le nombre de portions à protéger) un nombre variable de « premier » dispositif et de « second » dispositif.

Un tel ensemble électronique offre l'avantage d'être facile à installer dans un réseau de communication, par exemple en « intermédiaire » entre un équipement (particulier) à protéger et le reste du réseau de communication., ou de façon à limiter les accès à cet équipement à protéger aux seuls accès effectués par le premier dispositif ou simplement pour limiter les accès à l'équipement à protéger aux appareils situés dans une portion (protégée) du réseau de communication, à laquelle appartient cet équipement. Un tel ensemble peut également aider à proposer un produit « clé en main » à un administrateur du réseau de communication.

Un tel ensemble électronique peut ainsi aider, au moins dans certains modes de réalisation, à sécuriser un équipement à protéger, sans nécessiter de modification et/ou de remplacement de cet équipement.

Par souci de clarté, on utilise dans la présente demande le terme « équipement électronique », ou « équipement », pour se référer à des équipements susceptibles d'être protégés par l'ensemble électronique. On utilisera le terme « dispositif électronique », ou « dispositif », pour se référer au premier ou au second dispositif électronique de l'ensemble électronique 160 introduits ci-avant. Le terme « appareil électronique » ou « appareil » est relatif à un appareil électronique quelconque (il peut s'agir parfois d'un équipement à protéger ou d'un dispositif de l'ensemble électronique).

On décrit à présent, en lien avec la figure 1, de façon plus détaillée la présente demande.

La figure 1 représente un système 100 dans lequel certains modes de réalisation de l'invention peuvent être mis en œuvre. Le système 100 comporte un ou plusieurs appareils électroniques, certains au moins pouvant communiquer entre eux via un ou plusieurs réseaux de communication 110, 120, 130 éventuellement partitionnés et/ou interconnectés. Dans l'exemple illustré, le système comprend ainsi un réseau privé partitionné en deux portions 110, 120. L'une des portions 120 est en outre interconnectée avec un autre réseau 130 (comme un réseau étendu et/ou public, permettant ainsi des communications, entre des appareils électroniques 150, 164, 170 de cette portion 120 et des appareils électroniques 180 n'appartenant pas au réseau privé.

Le réseau privé peut par exemple être un réseau privé d'entreprise ou domestique, par exemple un réseau privé local (ou LAN pour Local Area Network, selon la terminologie anglaise).

L'autre réseau 130 peut par exemple être un autre réseau local, ou un réseau « étendu » de couverture géographique importante, comme un réseau métropolitain (ou MAN, pour Metropolitan Area Network, selon la terminologie anglaise) ou un réseau dont la zone géographique couvre au moins une région d'un pays, ou un pays (ou WAN, pour Wide Area Network, selon la terminologie anglaise). Il peut s'agir par exemple d'un réseau WAN de type internet, ou cellulaire, GSM - Global System for Mobile Communications, UMTS - Universal Mobile Telecommunications System, Wifi - Wireless, etc.).

Comme illustré en figure 1, le système 100 peut également comprendre une portion 110 non interconnectée du réseau privé, dite protégée, comportant un ou plusieurs équipements électroniques 140. Il peut s'agir d'équipements comme un terminal (tel qu'un ordinateur portable, un smartphone, une tablette ou un objet connecté), un objet connecté (comme un robot, un dispositif mobile guidé automatiquement et/ou à distance, un compteur d'énergie, une machine-outil dans le cas d'un réseau privé industriel, et/ou un équipement électroménager dans le cas d'un réseau domestique), un serveur, par exemple un serveur d'applications, et/ou un dispositif de stockage.

Les équipements de la portion 100 non interconnectée peuvent utiliser des protocoles de communication différents selon les modes de réalisation, comme OPCUA (pour OPen Connectivity – Unified Architecture), MQTT (pour Message Queuing Telemetry Transport en anglais), ModBus TCP, Siemens S7, MTConnect, LabView. Ces protocoles peuvent différer selon les équipements de la portion non interconnectée.

Selon la présente demande, un appareil n'appartenant pas à une première portion protégée (comme un appareil n'appartenant pas au réseau de communication, ou appartenant à la seconde portion « exposée » du réseau de communication) émet un paquet de données (une demande de lecture ou d'écriture de/dans une zone mémoire par exemple) destiné à un équipement de la première portion. Le second dispositif intercepte ce paquet de données, décide optionnellement de conserver ou non ce paquet de données en fonction d'une règle de filtrage (appelée par la suite « seconde » règle de filtrage en référence au « second » dispositif) et le cas échéant (si le paquet est conforme à cette seconde règle de filtrage), transcode ce paquet en données sérialisées et les transmet au premier dispositif, situé dans la portion protégée, où ces données sont à nouveau filtrées par le premier dispositif avant d'être transcodées sous forme d'au moins un nouveau paquet de données (ayant, selon les modes de réalisation, une structure identique ou différente de celle du paquet émis par l'appareil tiers). Ce ou ces nouveau(x) paquets est/sont ensuite transmis à un équipement destinataire de la première portion. La réponse de l'équipement tiers peut ensuite être transmise via le premier et le second dispositif à l'appareil tiers ayant émis le paquet de données (par exemple en utilisant un mécanisme de sérialisation/désérialisation de données avec et/ou sans filtrage).

Ainsi, selon la présente demande, il est possible de recevoir des requêtes d'un appareil tiers souhaitant par exemple accéder, en lecture et/ou en écriture, à des données de l'équipement à protéger, et de lui fournir en retour ces données, en toute sécurité pour l'équipement à protéger.

Le système comprend au moins un ensemble électronique 160 tel qu'introduit ci-avant visant à protéger au moins certains équipements électroniques 140 du réseau privé 110. Le premier dispositif 162 de l'ensemble électronique 160 est situé dans une portion 110 dite « à protéger » du réseau privé comportant l'équipement 140 à protéger. Le premier dispositif 162 communique avec le second dispositif 164 (situé dans la portion interconnectée 120) via des moyens 1622,

1624, 1642, 1644 de communication unidirectionnels, comportant par exemple des premiers moyens 1622, 1642 de communication unidirectionnels dans un premier sens de communication, et des seconds moyens 1624, 1644 de communication unidirectionnels dans un second sens de communication, opposé au premier sens. De tels moyens de communication unidirectionnels peuvent varier selon les modes de réalisation (et notamment selon les capacités hardware du premier et/ou du second dispositif). Dans certains modes de réalisation, les moyens de communication unidirectionnels peuvent comprendre au moins un optocoupleur, et/ou encore des moyens de communication bidirectionnels ayant été limités à un seul sens de transmission, comme un câble Ethernet une liaison série et/ou ou une fibre optique et/ou au moins un isolateur digital (Digital isolator selon la terminologie anglaise) à isolation galvanique, capacitive, inductive et/ou optique.

Dans certains modes de réalisation, les premiers et second moyens de communication peuvent être différents. Par exemple, le second dispositif peut émettre des données vers le premier dispositif via une liaison Ethernet limitée à un sens de communication et le premier dispositif peut émettre des données vers le second dispositif via un optocoupleur. Dans d'autres modes de réalisation, les premiers et seconds moyens de communication peuvent être similaires. Par exemple, chacun des premiers et seconds moyens de communication unidirectionnels peut comprendre un optocoupleur 166.

La présence d'optocoupleur(s) permet de séparer les deux dispositifs de manière physique (aucun flux électrique n'est échangé, simplement de la lumière), et donc de renforcer la sécurité des échanges. L'isolation électrique des dispositifs entre eux peut aider par exemple à prévenir des attaques par injection de courant ou de signal électrique sur la seconde portion dudit réseau.

Le système peut également comprendre des éléments 164, 170 de gestion et/ou d'interconnexion réseau. Notamment (et même si non illustré en figure 1), dans certains modes de réalisation, l'ensemble électronique 160 peut comprendre au moins une passerelle d'interconnexion avec un autre réseau. Dans certains modes de réalisation, cette passerelle peut par exemple être connectée au deuxième dispositif de l'ensemble électronique (et donc permettre une interconnexion entre la portion « exposée » du réseau privé et l'autre réseau). Dans d'autres modes de réalisation, le deuxième dispositif peut jouer lui-même un rôle de passerelle d'interconnexion entre la portion « exposée » du réseau privé et l'autre réseau.

Le réseau privé peut par exemple utiliser des liaisons filaires comme au moins une liaison série et/ou une liaison Ethernet, ou des moyens de communication sans fil. Le réseau peut implémenter un protocole de communication comme ModBus Série, ou CAN (acronyme anglophone pour « *Controller Area Network* ») dans le cas d'une liaison série, ou comme ModBus TCP, OPC-UA, MQTT dans le cas d'une liaison Ethernet.

La figure 2 illustre une structure simplifiée d'un appareil électronique 200 du système 100, par exemple le premier dispositif 162, le premier dispositif 162, et/ou l'équipement à protéger 140 de

la figure 1. Selon les modes de réalisation, il peut s'agir d'un serveur, et/ou d'un terminal, ou encore d'un micro-ordinateur avec une interface homme-machine simple comme un RaspberryPi ©, un OrangePi © ou encore un NanoPI NEO.

L'appareil 200 comprend notamment au moins une mémoire M 210. L'appareil 200 peut notamment comprendre une mémoire tampon, une mémoire volatile, par exemple de type RAM (pour « Random Access Memory » selon la terminologie anglaise), et/ou une mémoire non volatile (par exemple de type ROM (pour « Read Only Memory » selon la terminologie anglaise). L'appareil 200 peut également comprendre une unité de traitement UT 220, équipée par exemple d'au moins un processeur P 222, et pilotée par un programme d'ordinateur PG 212 stocké en mémoire M 210. A l'initialisation, les instructions de code du programme d'ordinateur PG sont par exemple chargées dans une mémoire RAM avant d'être exécutées par le processeur P. Dans le cas où l'appareil est le premier dispositif 162 et/ou du second dispositif 164 de l'ensemble électronique, ledit au moins un processeur P 222 de l'unité de traitement UT 220 peut notamment mettre en œuvre, individuellement ou collectivement, l'un quelconque de modes de réalisation d'au moins un des procédés de la présente demande (décrits notamment en relation avec les figures 3 et 4), selon les instructions du programme d'ordinateur PG.

L'appareil peut également comporter, ou être couplé à, au moins un module d'entrée/ sortie I/O 230. L'au moins un module d'entrée/ sortie I/O 230 de l'appareil peut comprendre, dans certains modes de réalisation, au moins un module d'interfaçage avec un utilisateur de l'appareil (aussi appelé plus simplement dans cette demande « interface utilisateur »). Par interface utilisateur de l'appareil, on entend par exemple une interface intégrée à l'appareil 200, ou une partie d'un appareil tiers avec lequel il est couplé par des moyens de communication filaires ou sans fils. Par exemple, il peut s'agir d'un écran secondaire de l'appareil.

Une interface utilisateur peut notamment être une interface utilisateur, dite «de sortie », adaptée à un rendu (ou au contrôle d'un rendu) d'un élément de sortie d'une application informatique utilisée par l'appareil 200, par exemple une application s'exécutant au moins partiellement sur l'appareil 200 ou une application « en ligne » s'exécutant au moins partiellement à distance, par exemple sur un serveur. Des exemples d'interface utilisateur de sortie de l'appareil incluent un ou plusieurs écrans, notamment au moins un écran graphique (tactile par exemple), un ou plusieurs haut-parleurs, un objet connecté.

Par rendu, on entend ici une restitution (ou « output » selon la terminologie anglaise) sur au moins une interface utilisateur, sous une forme quelconque, par exemple comprenant des composantes textuelle, audio et/ou vidéo, ou une combinaison de telles composantes.

Par ailleurs, une interface utilisateur peut être une interface utilisateur, dite «d'entrée», adaptée à une acquisition d'une commande d'un utilisateur de l'appareil 200. Il peut s'agir notamment d'une action à effectuer en lien avec un item restitué, et/ou d'une commande à transmettre à une application informatique utilisée par l'appareil 200, par exemple une application s'exécutant au

moins partiellement sur l'appareil 200 ou une application « en ligne » s'exécutant au moins partiellement à distance, par exemple sur un serveur. Des exemples d'interface utilisateur d'entrée incluent un capteur, un moyen d'acquisition audio et/ou vidéo (microphone, caméra (webcam) par exemple), un clavier, une souris.

L'appareil peut également comporter, ou être couplé à, au moins un module d'entrée/ sortie I/O 230, tel qu'un module de communication, permettant à l'appareil 200 de communiquer avec au moins un autre appareil du système 100, via des interfaces de communication filaires ou sans fils. Par exemple, il peut s'agir d'au moins une interface de type Ethernet, et/ou de type Wifi, Bluetooth.

Dans le cas où l'appareil est le premier dispositif 162 ou le second dispositif 164 de l'ensemble électronique, les moyens de communication 1622, 1622, 1642, 1644 comportent par exemple des premiers moyens de communication unidirectionnels 1622, 1642 dans un premier sens de communication, et des seconds moyens de communication unidirectionnels 1624, 1644 dans un second sens de communication, opposé au premier sens, comme au moins une interface de type Ethernet, ou au moins une interface série avec un optocoupleur de l'ensemble électronique 160. Dans l'exemple de la figure 1, l'optocoupleur peut être connecté directement à l'interface série. Par exemple, le port de transmission du premier dispositif (portion protégée) peut être connecté à une broche de l'optocoupleur et le port de réception du second dispositif (portion exposée) peut être connecté à une autre broche de l'optocoupleur. Chaque côté de l'optocoupleur peut être alimenté en tension par le premier et le second dispositif respectivement (par exemple avec une tension de 3.3V).

Dans certains modes de réalisation, lorsque l'appareil 200 appartient à une première portion à protéger, les moyens de communication de l'appareil (hormis éventuellement les moyens de communication unidirectionnelle ci-dessus lorsque l'appareil est le premier dispositif) peuvent être uniquement des moyens de communication filaires, de façon à limiter physiquement les possibilités d'accès (directement ou via cet appareil) à un équipement à protéger situé dans la même portion à protéger du réseau (et donc les possibilités d'attaques de tiers) . Ainsi, au moins l'un des premier et second dispositifs 162, 164 peut être un micro-ordinateur de type « NanoPi NEO » ©, équipé uniquement d'un port Ethernet (et pas de Wifi).

Ledit au moins un microprocesseur du premier dispositif 162 peut notamment être adapté pour :

- une transmission audit second dispositif d' au moins un identifiant d'adressage dudit équipement de ladite première portion dudit réseau de communication ;
- un transcodage de données reçues dudit second dispositif en au moins un paquet de données structuré comportant au moins un identifiant d'adressage d'un équipement destinataire dudit paquet sur ladite première portion ;
- une transmission dudit paquet audit équipement destinataire ;

au moins un desdits transcodage et/ou transmission étant effectuée de façon conditionnelle en tenant compte d'au moins une règle de filtrage relative au contenu dudit paquet.

Ledit au moins un microprocesseur du second dispositif 164 peut notamment être adapté pour :

- une affectation audit second dispositif, comme identifiant d'adressage sur ladite seconde portion dudit réseau, d'au moins un identifiant d'adressage d'un équipement de ladite première portion
- sur réception d'un paquet structuré de données ayant comme adresse de destination ledit identifiant d'adressage, une sérialisation des données dudit paquet et ;
- une émission desdites données sérialisées vers ledit premier dispositif.

au moins une de ladite sérialisation et/ou ladite émission étant effectuée de façon conditionnelle en tenant compte d'au moins une règle de filtrage relative au contenu dudit paquet.

Certains des modules d'entrée -sorties ci-dessus sont optionnels et peuvent donc être absents de l'équipement à protéger, du premier dispositif et/ou du second dispositif dans certains modes de réalisation.

L'ensemble électronique introduit ci-dessus peut comprendre, dans certains modes de réalisation, un boîtier physique dans lequel sont logés le premier et le second dispositif et les moyens de communication bidirectionnels entre le premier dispositif et le second dispositif. Le boîtier peut par exemple limiter ou empêcher les accès physiques aux premier et second dispositifs et à leurs moyens de communication mutuelle. Il peut notamment s'agir d'un boîtier fermé par une bande de garantie non repositionnable, ou d'un boîtier scellé, de façon à rendre visible toute ouverture du boîtier, du fait de la détérioration d'un scellé ou de la bande de garantie, ou de rendre son ouverture difficile. Le boîtier peut par exemple laisser un accès physique à au moins certaines interfaces de communication du premier et/ou du second dispositif (autres que les moyens de communication mutuelle entre ces deux dispositifs par exemple) et/ou comporter des interfaces de communication reliées à au moins certaine(s) des interface(s) de communication du premier et du second dispositif.

Dans certains modes de réalisation, le boîtier peut ne donner accès qu'à certaines interfaces de communication filaires du premier dispositif. Par exemple, il peut s'agir de « forcer » ainsi l'usage de certaines interfaces de communication entre l'équipement et le premier dispositif offrant par exemple des avantages en termes de sécurité (par exemple du fait du protocole que mettent en jeu de tels interfaces) ou pour privilégier l'usage d'interfaces « filaires ». Dans certains modes de réalisation, le boîtier peut laisser libre l'accès à plusieurs interfaces de communication des premier et second dispositifs, de façon à proposer un ensemble adapté à différents environnements réseaux.

Dans certains modes de réalisation, par exemple lorsque l'ensemble électronique introduit ci-dessus n'empêche pas l'accès à certaines interfaces du premier dispositif, certaines de ces interfaces peuvent être désactivées de façon logicielle (par exemple ne fournir aucun service),

de façon à ce qu'un équipement tiers ne puisse pas accéder en lecture et/ou en écriture (via une connexion SHH dans le cas d'une liaison Ethernet par exemple) au descriptif du premier dispositif et à des données de l'équipement mémorisées par le premier dispositif.

Par le terme « module » ou le terme « composant » ou « élément » du dispositif, on entend ici un élément matériel, notamment câblé, ou un élément logiciel, ou une combinaison d'au moins un élément matériel et d'au moins un élément logiciel. Le procédé selon l'invention peut donc être mis en œuvre de diverses manières, notamment sous forme câblée et/ou sous forme logicielle.

La figure 3 illustre certains modes de réalisation du procédé 300 de protection de la présente demande (mis en œuvre par exemple par un premier dispositif d'un ensemble électronique selon l'invention) et la figure 4 illustre certains modes de réalisation du procédé 400 de fourniture de données de la présente demande (mis en œuvre par exemple par un second dispositif d'un ensemble électronique selon l'invention). On décrit à présent le procédé 400 (avant le procédé 300) pour respecter un ordre chronologique de traitement d'une demande (comme d'accès en lecture/écriture à un équipement) reçue d'un appareil tiers, et faciliter ainsi la lecture de la présente demande de brevet.

Le procédé 400 peut par exemple être mis en œuvre par un second dispositif situé dans une portion d'un réseau de communication totalement distincte d'une portion protégée de ce réseau, comme le second dispositif 164 de l'ensemble électronique 160 du système 100.

Selon les modes de réalisation, le procédé peut être mise en œuvre automatiquement au démarrage du second dispositif (via un script exécuté au démarrage (« boot ») du dispositif) ou plus tard, par exemple suite au lancement, manuel ou automatique (via une tâche de fond par exemple) d'un exécutable implémentant au moins un mode de réalisation du procédé 400. Le procédé peut notamment comprendre comme illustré en figure 4, une phase dite d'initialisation 410 (lors d'un démarrage du second dispositif par exemple ou ultérieurement, sur réception d'une commande utilisateur par exemple). Cette phase d'initialisation 410 comprend une mise en place 412 (initialisation et/ou établissement) de communications (par exemple unidirectionnelles) du second dispositif vers le premier dispositif. et optionnellement de communications unidirectionnelles du premier dispositif vers le second dispositif.

Cette phase d'initialisation 410 comprend aussi une obtention 414 d'un descriptif, pouvant prendre la forme d'un ou plusieurs fichiers au format YAML, XML ou JSON par exemple. Ce descriptif peut notamment comprendre des informations relatives aux demandes que va recevoir le second dispositif (format des paquets à recevoir par exemple) , et/ou des informations relatives à des règles de filtrage que doit appliquer le second dispositif, et/ou des informations relatives à un équipement à qui peut être destiné un paquet qui sera reçu par le second dispositif (comme un identifiant de cet équipement, une désignation d'au moins un protocole qu'il peut utiliser, etc..), des informations relatives aux données à transmettre au

premier dispositif (protocole à utiliser, format etc..). Dans certains modes de réalisation, le descriptif peut aussi comprendre des informations nécessaires à l'établissement d'une communication unidirectionnelle entre le second dispositif et le premier dispositif et vice-versa (comme une adresse du premier dispositif sur le réseau de communication, un format de données et/ou un protocole à utiliser pour communiquer avec le premier dispositif etc..).

Dans d'autres modes de réalisation, où le descriptif est par exemple au moins partiellement reçu du premier dispositif via les moyens de communication mutuelle, les informations nécessaires à l'établissement d'une communication unidirectionnelle entre le second dispositif et le premier dispositif peuvent être obtenues par le second dispositif (via des données de paramétrage localement accessibles au second dispositif ou distante par exemple) préalablement à la mise en place 412 des moyens de communication bidirectionnelle et à l'obtention 414 du descriptif.

Lorsque le descriptif est reçu par le second dispositif, l'obtention du descriptif peut comprendre une désérialisation des données (correspondant au descriptif) reçues (si le contenu du descriptif a été sérialisé avant sa transmission au second dispositif).

Le format de réception du descriptif peut différer selon les modes de réalisation. Par exemple il, peut s'agir d'un format XML ou JSON. Le pseudo-code ci-dessous illustre à titre d'exemple la transmission du descriptif de façon sérialisée dans le cas du protocole JSON :

{'m' : 'description', {JSON description}} où dans cet exemple

- *m* annonce le type des données transmises (ici annonce de données correspondant à un descriptif)
- *description* est un libellé textuel annonçant la transmission d'un descriptif *{JSON description}* en format JSON.

Comme expliqué plus haut, dans certains modes de réalisation, le descriptif peut être reçu du premier dispositif. Dans d'autres modes de réalisation, le descriptif peut être obtenu par accès à une zone de stockage accessible au second dispositif, comme une zone de stockage locale au second dispositif ou accessible depuis la seconde portion du réseau ou encore une zone de stockage amovible (telle une clé USB) couplée au second dispositif.

Concernant plus précisément les informations relatives aux paquets à recevoir, le descriptif obtenu 414 peut notamment comprendre des informations décrivant au moins un protocole (comme Ethernet) à utiliser pour recevoir ces paquets, une taille des paquets, un format (ou structure) des paquets, un débit de réception, etc…

Des exemples de protocoles incluent des protocoles hiérarchisés, utilisant des structures de données standardisées, comme les protocoles Open Platform Communications Unified Architecture (OPC-UA) et ModBus, ou des protocoles non hiérarchisés comme MQTT et Direct UDP (pour Direct Datagram Protocol en anglais).

Concernant les informations relatives à au moins une règle de filtrage que doit appliquer le second dispositif, elles peuvent comprendre par exemple :

- une désignation d'au moins un protocole accepté ou proscrit ;
- une désignation d'au moins un domaine réseau dont les demandes, lorsqu'elles sont émises depuis ce domaine, seront acceptées ou proscrites ;
- un identifiant d'au moins un appareil, émetteur d'une demande, accepté ou proscrit ;
- une désignation d'au moins une portion du réseau acceptée ou proscrite comme portion d'appartenance d'un destinataire d'une demande ;
- un identifiant d'au moins un équipement accepté ou proscrit comme destinataire d'une demande ;
- un type de demande d'accès (lecture, écriture, etc..) accepté ou proscrit ;
- une plage d'adresses acceptée ou proscrite comme paramètres d'une demande ;
- un paramètre accepté ou proscrit en lien avec un protocole particulier (comme un « topic » pour MQTT par exemple)
- une combinaison d'au moins deux desdites informations.

Certaines de ces informations peuvent être optionnelles dans certains modes de réalisation.

Concernant les informations relatives à un équipement à qui peut être destiné un paquet, elles peuvent notamment comprendre un identifiant d'adressage de cet équipement (par exemple selon les protocoles une adresse IP, une adresse MAC d'au moins un point d'accès, etc.), une désignation d'au moins un protocole qu'il accepte, un port de communication ouvert sur cet équipement.

Dans des modes de réalisation où l'ensemble électronique comprend des moyens de communication unidirectionnel du premier dispositif vers le second dispositif, le descriptif peut également comprendre des informations relatives à des données à recevoir du premier dispositif en réponse à un envoi par le second dispositif d'une demande provenant d'un appareil tiers. Il peut s'agir par exemple d'un protocole à utiliser pour recevoir ces données, et/ou d'une taille, d'un type et/ou d'un format de ces données, ou encore d'un protocole à utiliser pour transmettre ces données, et/ou un format de sortie de ces données à utiliser pour leur transmission à un appareil tiers.

Certaines des informations ci-avant peuvent être optionnelles dans le descriptif dans certains modes de réalisation.

Un exemple de descriptif est présenté ci-après.

Dans cet exemple, le descriptif concerne plusieurs équipements. Le terme « devices» annonce une liste des équipements à protéger (désignés par leurs adresses IP respectives), chacun accessible par un protocole différent dans cet exemple. On retrouve pour chacun les ports autorisés, les émetteurs (sources) autorisés (désignés par leurs adresses IP respectives), le type d'accès possible et les registres, les « namespaces » (pour OPC-UA), topic (pour MQTT), requêtes http (pour MTConnect) autorisés par type d'accès.

config_version : 1.0

```
config_date: 2023-05-15

diode:
  hostname: SmartDiode

devices:
  "192.168.0.5":
    type: modbus
    ports:
     - 9400
     - 502
    sources:
     - '192.168.0.1'
    read:
     - 0-105
     - 200-420
    write:
     - 1-12
     - 200-202
     - 400

  "192.168.0.11":
    type: opcua
    ports:
     - 48040
     - 4840
    read:
     - 'ns=1;s=UI-A@supervision|exports-4-0-4statistics-1:sigma2'
     - 'ns=2;i=1234'
    write:
     - 'ns=3;i=568'
     - 'ns=2;i=1234'

  "192.168.0.12":
    type: s7
    read:
     - '1:10-20' # DB=1, range 10 to 20
```

```
    write:
      - '10:50'
      - '10:60-70'

  "192.168.0.100":
    type: mqtt
    ports:
      - 1883
    read:
      - '#'
    write:
      - '/topic/whatever'

  "192.168.0.13":
    type: mtconnect
    read:
      - /probe # All devices
      - /M12345/probe # Specific device
      - /(M12345|M45678)/probe # Specific devices
      - /([a-zA-z0-9-]+)/probe # Any device
      - /current?path=//Axes(?:\/[^\.]+)*&at=(\d+) # //Axes and all its children
      - /current?path=//Rotary//DataItem[type="LOAD"](?:\/[^\.]+)*&at=(\d+)
      - /sample?path=//Axes(?:\/[^\.]+)*&from=(\d+)&count=(\d+)
    - /asset/([a-zA-z0-9;-]+)?type=(\w+)&count=(\d+)&device=([a-zA-z0-9-
]+)&removed=(true|false)
```

Dans certains modes de réalisation, le procédé 400 de transmission peut comprendre une mise à jour (optionnelle) du descriptif obtenu 414, soit automatiquement par le second dispositif, soit via une interface utilisateur du second dispositif, pour supprimer certaines informations du descriptif ou en ajouter des nouvelles (par exemple pour créer, supprimer et/ou modifier au moins une règle de filtrage).

Comme illustré en figure 4, le procédé peut comprendre un traitement 420 d'un paquet de données en provenance d'un appareil tiers situé à l'extérieur de la portion protégée. Il peut s'agir par exemple une demande d'accès en lecture ou en écriture à une zone mémoire d'un équipement de la première portion. Le paquet peut par exemple être obtenu 422 (ie ici reçu) par le second dispositif via la seconde portion du réseau de communication. Par exemple, lorsque le second dispositif est connecté à la seconde portion via une liaison Ethernet, le second dispositif

peut intercepter les paquets de données circulant sur la seconde portion du réseau et ayant une adresse de destination correspondant à un identifiant d'adressage contenu dans le descriptif.

Comme illustré en figure 4, le procédé peut comprendre un examen 430 des paquets reçus. tenant compte d'au moins une règle de filtrage (dite « seconde » règle de filtrage par référence au « second » dispositif) . L'au moins une seconde règle de filtrage peut par exemple être obtenue 432 à partir des informations présentes dans le descriptif (et détaillées ci-avant). Le procédé peut ainsi comprendre un filtrage 434 des paquets reçus pour ne conserver que celles cohérente avec l'au moins une « seconde » règle de filtrage obtenue.

Ainsi, selon un premier exemple, on peut conserver ou supprimer des paquets ayant pour protocole MQTT selon leur « topic ». Selon un second exemple, on peut conserver ou supprimer des paquets ayant pour protocole OPC-UA en fonction des nœuds désignés et d'un type de demande (accès en lecture ou en écriture) auquel correspond le paquet. Selon un troisième exemple, on peut conserver ou supprimer des paquets ayant pour protocole ModBus en fonction des registres désignés et d'un type de demande (accès en lecture ou en écriture) auquel correspond le paquet. On peut également tenir compte de l'équipement destinataire pour conserver ou supprimer des paquets.

Par exemple, en lien avec l'exemple de descriptif ci-avant, un paquet destiné à la machine « ModBus » seront conservées uniquement si elles ont comme port de destination le port 9400 et concernent les « registres » 0 à 105 des « coils » 0 à 1 dans le cas d'une demande d'accès en lecture. Par contre, seules les demandes d'accès en écriture aux registres 0-12 seront conservées. Ainsi, une demande d'écriture sur le registre 13, par exemple, sera éliminée.

Comme illustré, le procédé peut comprendre un transcodage 440 des paquets conservés. Ainsi, le procédé peut comprendre une extraction 442 des données contenues dans le paquet obtenu 422 en tenant compte de la structure du paquet et notamment du protocole utilisé dans l'encodage du paquet. Les données extraites peuvent par exemple comprendre, outre l'adresse du destinataire du paquet, au moins un port destinataire sur l'équipement destinataire, un type de demande à adresser à l'équipement, des données en lien avec la commande (plage d'adresses, valeurs de données etc..).

Par exemple, dans le cas d'un protocole MQTT, le pseudo code suivant peut être mis en œuvre lors de l'extraction:

```
# Extract destination IP
   destination_ip = packet[16:20]
# Extract destination port
   destination_port = packet[20:22]
# Extract MQTT topic
   topic_length = packet[30]
   topic = packet[31:31+topic_length]
```

```
# Extract MQTT payload
    payload_length = packet[31+topic_length+1]
    payload = packet[31+topic_length+2:31+topic_length+2+payload_length]
```

Dans l'exemple de la figure 4, le procédé peut comprendre une sérialisation des données extraites. Cette sérialisation peut par exemple tenir compte du descriptif obtenu 414 (notamment d'une désignation, dans le descriptif ; d'un protocole à utiliser pour la sérialisation, comme XML ou JSON).

Par exemple, les données sérialisées peuvent comprenant en entête une annonce d'un type des données (protocole employé ou annonce de données correspondant à un descriptif, etc.), un libellé identifiant ce type de données, ainsi que d'éventuel libellés textuels ou code numérique annonçant la signification des éléments qui les suivent. Ces annonces peuvent être optionnelle dispositif décrit plus loin comportes dans certains modes de réalisation, notamment lorsque le descriptif du second dispositif (et celui du premier dispositif) ne prévoit qu'un unique protocole.

Comme illustré en figure 4, le procédé peuvent comprendre une transmission 450 au premier dispositif des données transcodées (via un des chemins de communication unidirectionnels mis en place par exemple)

En variante, le filtrage peut être effectué sur les données extraites / sérialisées (et non sur les paquets reçus).

Un filtrage effectué sur des paquets (plutôt que sur des données sérialisées) permet de s'appuyer sur la structure des paquets (et donc sur la sémantique des champs de ces paquets) pour effectuer le filtrage. De plus, il évite d'effectuer des traitements inutiles de sérialisation de données qui ne seront pas conservées.

De façon optionnelle, le procédé peut comprendre un traitement 460 d'un message de l'équipement (comme un message UDP ou une réponse à la demande envoyée vers le premier dispositif (et transmise par celui-ci à l'équipement)). Sur réception 462 d'un message, le procédé peut comprendre une transmission 464 de la réponse à l'appareil tiers auquel elle est destinée. Il peut s'agir notamment dans certains modes de réalisation d'une simple réémission d'un paquet reçu. Le traitement peut éventuellement comprendre un filtrage des paquets reçus (similairement à ce qui a déjà été décrit ci-dessus, mais éventuellement avec des règles de filtrage différentes (par exemple pour interdire la communication du contenu de certains registres), ou pour filtrer les destinataires des messages).

Selon les modes de réalisation, la façon dont le second dispositif obtient un paquet destiné à un équipement de la première portion peut varier. Par exemple, dans certains modes de réalisation où le second dispositif est connecté à la seconde portion du réseau de communication via une liaison Ethernet, le second dispositif peut intercepter les paquets de données circulant sur la seconde portion du réseau lorsque leur adresse de destination correspondant à celle de l'équipement. Dans d'autres modes de réalisation, le second dispositif peut utiliser, comme son

propre identifiant d'adressage sur la seconde portion, un identifiant d'adressage d'au moins un équipement sur la première portion. L'identifiant d'adressage de l'équipement sur la première portion peut par exemple être obtenu par lecture du descriptif ou reçu du premier dispositif et le procédé peut comprendre une définition ou modification de son propre identifiant d'adressage pour être égal à l'identifiant d'adressage de l'équipement sur la première portion. Il peut s'agir aussi d'un ajout de l'identifiant d'adressage de l'équipement sur la première portion à son/ses identifiant(s) d'adressage sur la seconde portion.

De tels modes de réalisation peuvent permettre au second dispositif de « se faire passer » pour l'équipement, vis-à-vis d'appareils de la seconde portion ou externes au réseau de communication

De tels modes de réalisation peuvent ainsi aider un administrateur du réseau de communication à disposer d'une solution « plug and play ». Ainsi, l'insertion de l'ensemble électronique dans le réseau, pour la protection d'un équipement, peut-être transparente aux autres appareils déjà présents dans le réseau et peut ne pas nécessiter de modifier un plan de routage (ou d'adressage) de l'ensemble du réseau ou de modifier le logiciel de l'un des appareils tiers souhaitant obtenir des données provenant de l'équipement.

En particulier, lorsque le second dispositif fait partie d'un ensemble électronique protégeant plusieurs équipements, le second dispositif peut s'affecter plusieurs adresses (IP par exemple) sur la seconde portion (via des « subnets » par exemple) identique chacune à l'un des identifiants d'adressages d'un équipement à protéger sur la première portion.

Par exemple, dans certains modes de réalisation, l'ensemble électronique peut être installé dans un réseau existant comportant un équipement qu'il s'agit (nouvellement) de protéger. Lorsque l'ensemble électronique est installé de façon à pouvoir communiquer (par exemple via une liaison filaire) avec l'équipement à protéger, constituant ainsi une première portion du réseau (comprenant au moins l'équipement et le premier dispositif), un opérateur du réseau peut n'avoir aucune action à effectuer (hormis cette installation). Les demandes destinées à l'équipement étant reçues par le second dispositif et les éventuelles réponses de l'équipement étant transmises par le second dispositif, les appareils et logiciels extérieurs à la portion protégée du réseau peuvent continuer à effectuer des requêtes vers l'équipement, sans modification de la routine d'accès qu'ils utilisaient avant l'installation de l'ensemble électronique pour protéger l'équipement. L'insertion de l'ensemble électronique dans le réseau peut donc être transparente à ces appareils et logiciels.

On décrit à présent le procédé 300 illustré en figure 3, et mis en œuvre par exemple par un premier dispositif situé dans une portion protégée d'un réseau de communication comme le premier dispositif 162 de l'ensemble électronique 160 du système 100.

Similairement à ce qui a été décrit ci-avant pour le procédé 400 mis en œuvre par le second dispositif, le procédé 300 peut être mis en œuvre, selon les modes de réalisation, lors du démarrage du premier dispositif, ou plus tard, et peut comprendre, comme illustré en figure 3,

une phase dite d'initialisation 310 (lors d'un démarrage du premier dispositif par exemple ou ultérieurement, sur réception d'une commande utilisateur par exemple). Cette phase d'initialisation peut comprendre une obtention 312 d'un descriptif pouvant prendre la forme d'un ou plusieurs fichiers par exemple et pouvant notamment comprendre des informations relatives à la mise en place d'une communication bidirectionnelle entre le premier dispositif et le second dispositif (comme une adresse du second dispositif sur le réseau de communication, un protocole à utiliser etc..) et/ou des informations relatives aux données que va recevoir le premier dispositif en provenance du second dispositif (protocole à utiliser, format etc..), et/ou des informations relatives à des règles de filtrage de ces données que doit appliquer le premier dispositif, et/ou des informations relatives à au moins un équipement à qui peuvent être destinées ces données (comme un identifiant de cet équipement, une désignation d'au moins un protocole qu'il peut utiliser, etc..), et/ou des informations relatives à la structuration de ces données en paquet(s) de données avant leur transmission à un équipement, et des informations relatives à une communication à établir avec un équipement pour la transmission d'au moins un tel paquet (comme un mot de passe, ou une clé publique ou privée nécessaire à une connexion à l'équipement).

Les informations relatives à la mise en place d'une communication bidirectionnelle entre le premier dispositif et le second dispositif, les informations relatives aux données que va recevoir le premier dispositif en provenance du second dispositif (protocole à utiliser, format etc..), et et/ou les informations relatives à la structuration de ces données en paquet(s) peuvent être similaires à celles décrites en liaison avec le procédé 400 de transmission (le format des paquets reçus par le second dispositif pouvant être différent du format des paquets émis par le premier dispositif).

Les informations relatives à des règles de filtrage peuvent être similaires à celles décrites en liaison avec le procédé 400 de transmission. Dans certains modes de réalisation, les règles de filtrage peuvent différer des règles de filtrage appliquées par le second dispositif. Par exemple, les règles de filtrage à appliquer par le premier dispositif peuvent tenir compte du second dispositif de qui sont reçues les données (lorsque le premier dispositif peut recevoir des données de plusieurs « seconds » dispositifs) de façon par exemple à éliminer certaines données correspondant à des demandes d'écriture en provenance d'une seconde portion interconnectée avec un réseau public comme internet.

Les informations nécessaires à l'identification d'un équipement à protéger peuvent comprendre au moins une des informations d'identification suivantes :

- un libellé textuel ;
- une adresse (ou identifiant d'adressage) de l'équipement sur la première portion (par exemple selon les protocoles une adresse IP, une adresse MAC d'au moins un point d'accès de l'équipement etc..) ;

- une référence constructeur de l'équipement ;
- un numéro de série de l'équipement ;
- une combinaison d'au moins deux des informations d'identification ci-dessus.

Les informations nécessaires à l'établissement d'une communication entre le premier dispositif et l'équipement (en complément aux informations d'identification) peuvent comprendre notamment au moins une des informations, dites de communication, suivantes :

- une information désignant un protocole utilisable pour dialoguer avec l'équipement ;
- un port de l'équipement utilisable pour dialoguer avec l'équipement selon ledit protocole ;
- au moins un élément de sécurisation de connexion (comme un identifiant d'accès, un mot de passe, une clé publique ou privée etc..) ;
- des paramètres complémentaires spécifiques à certain(s) protocoles(s) (comme un « topic » dans le cas du protocole MQTT).
- une combinaison d'au moins deux des informations de communication ci-dessus.

Des exemples de protocoles pour communiquer avec l'équipement incluent des protocoles hiérarchisés, utilisant des structures de données standardisées, comme les protocoles Open Platform Communications Unified Architecture (OPC-UA) ModBus, ou des protocoles non hiérarchisés comme MQTT ou Direct UDP.

Certaines des informations du descriptif peuvent être optionnelles dans certains modes de réalisation. Par exemple, des informations de communication comme des éléments de sécurisation de connexion peuvent être absents lorsque l'accès à l'équipement n'est pas restreint à l'intérieur de la première portion. De plus, certaines des informations descriptives de données peuvent dépendre du ou des protocole(s) désigné(s) dans les informations de communication.

Dans certains modes de réalisation, le descriptif peut par exemple être obtenu par accès à une zone de stockage accessible au premier dispositif (comme une zone de stockage locale au premier dispositif ou située dans la première portion du réseau ou encore une zone de stockage amovible (telle une clé USB) couplée au premier dispositif ou accessible via une connexion série sur un port micro-USB du premier dispositif. Il peut s'agir notamment d'un port micro-USB inaccessible à un tiers lorsque le boîtier de l'ensemble électronique comportant le premier dispositif est fermé.

Dans certains modes de réalisation (par exemple certains modes de réalisation où le descriptif est obtenu par lecture d'une zone de stockage accessible au premier dispositif), le procédé 300 peut comprendre une transmission 316 d'au moins une portion du descriptif obtenu 312 au second dispositif.

Dans certains modes de réalisation, le descriptif peut être créé, ou complété, dynamiquement (et au moins partiellement automatiquement) par le premier dispositif lui-même.

Dans un tel mode de réalisation, le procédé peut comprendre une scrutation (ou exploration) (ou scan ARP (pour Address Resolution Protocol selon la terminologie anglaise) de la première portion, pour découvrir les appareils présents dans la première portion, puis au moins une tentative de connexion à ces appareils en utilisant un ou plusieurs protocole(s) candidat(s) (selon les modes de réalisation), permettant, quand une tentative de connexion réussit, de détecter au moins un protocole utilisé par l'équipement. Les tentatives de connexion peuvent éventuellement utiliser des éléments complémentaires (comme au moins une valeur de port (pour découvrir au moins un port ouvert sur l'appareil concerné) et/ou des paramètres complémentaires en cohérence avec ce (ou ces) protocole candidat). Par exemple, le procédé peut comprendre, pour chaque appareil découvert de la première portion, une tentative de connexion avec un ensemble de protocoles candidats définis par configuration (manuelle ou automatique) du dispositif.

Lorsqu'au moins une tentative de connexion a été menée avec succès pour au moins un appareil découvert, le procédé peut comprendre un enregistrement de l'adresse de l'appareil découvert en association avec les protocoles ayant permis la connexion, et les éventuels éléments complémentaires dans ledit descriptif.

Un tel mode de réalisation peut permettre, non seulement de créer un descriptif, mais également de mettre à jour automatiquement un descriptif existant. Il peut s'agir ainsi d'ajouter des informations ayant trait à un équipement nouvellement découvert ou de modifier des informations du descriptif relatives à un équipement, par exemple pour ajouter des informations relatives à un nouveau protocole accepté par cet équipement (suite à une mise à jour logicielle de l'équipement par exemple), ou pour supprimer la désignation d'un port devenu inaccessible (défectueux par exemple).

Dans certains modes de réalisation, le procédé peut comprendre de plus une mise à jour (optionnelle) du descriptif obtenu par le premier dispositif. Ainsi, une mise à jour automatique peut comprendre par exemple un ajout d'informations de filtrage par défaut, applicables pour les demandes d'accès à un équipement nouvellement découvert (et enregistré dans le descriptif), comme une conservation uniquement des demandes d'accès en lecture, ou un ajout d'une information de filtrage interdisant l'usage, quel que soit l'équipement concerné d'un protocole peu sécurisé par exemple) ou interdisant l'usage d'un port défectueux.

Une mise à jour peut aussi être effectuée manuellement par un opérateur, via une interface utilisateur du premier dispositif, notamment pour créer et/ou supprimer et/ou modifier des informations de filtrage. Il peut s'agir par exemple compléter manuellement un fichier descriptif créé automatiquement par le premier dispositif.

Dans certains modes de réalisation, le descriptif obtenu 312 peut être identique au descriptif décrit en liaison avec le procédé 400 mis en œuvre dans le premier dispositif. Par exemple, les deux descriptifs peuvent être obtenus par copie d'un même support de stockage amovible, ou le

second dispositif peut recevoir du premier dispositif l'intégralité du descriptif qu'a précédemment lui-même obtenu 312 le premier dispositif (ou vice-versa). Dans de tels modes de réalisation, le descriptif du second dispositif peut alors contenir certaines informations non utiles au second dispositif (comme un mot de passe, ou une clé publique ou privée nécessaire à une connexion à l'équipement dont proviennent les données). Un tel mode de réalisation peut offrir des avantages en termes de simplicité de traitement (pour l'un des premier et second dispositif) et /ou de simplicité de configuration, donc de gain de temps, côté second dispositif, puisqu'il n'est pas nécessaire de prévoir un « descriptif » particulier au second dispositif.

Dans d'autres modes de réalisation, les descriptifs peuvent être différents. En particulier, certaines informations contenues dans le descriptif obtenu par le premier dispositif et relatives à l'équipement à protéger et/ou aux communications avec cet équipement (comme un mot de passe par exemple) peuvent être omises dans le descriptif obtenu par le second dispositif. De plus, dans certaines modes de réalisation où le format des paquets à créer par le premier dispositif et le format des paquets reçus par le second dispositif sont différents, des informations contenues dans les descriptifs et relatives aux formats des paquets à recevoir ou à créer seront différentes.

La phase d'initialisation 310 peut comprendre une mise en place 314 des moyens de communication bidirectionnels avec le second dispositif et, optionnellement, une transmission 316 d'au moins une portion du descriptif obtenu 310 au second dispositif.

La transmission 316 peut notamment comprendre la transmission d'au moins une information d'identification de l'équipement comme une adresse de l'équipement sur la première portion (par exemple selon les protocoles une adresse IP, une adresse MAC, etc..). (aussi appelée identifiant d'adressage sur la première portion dans la présente demande).

Elle peut également comprendre au moins certaines informations de communication avec l'équipement (par exemple des informations relatives à un protocole et/ou un port de communication).

En particulier dans certains modes de réalisation, la portion du descriptive transmise peut comprendre des informations du descriptif susceptibles d'aider le second dispositif de « se faire passer » pour l'équipement, vis-à-vis d'appareils de la seconde portion ou externes au réseau de communication.

Le procédé peut comprendre une obtention 320 de données, correspondant à une demande issue d'un appareil tiers, reçues (obtenues) du second dispositif, via les moyens de communication bidirectionnels. Le procédé peut comprendre en outre un transcodage, par exemple une désérialisation (ou structuration) 330 de ces données pour obtenir un paquet de données de données structuré. La structuration des données peut tenir compte d'informations présentes dans le descriptif désignant un protocole utilisé par l'équipement.

Par exemple, en reprenant l'exemple du pseudo-code d'extraction de données cité précédemment en liaison avec le procédé 400 de transmission, le pseudo -code permettant la désérialisation de ces données en un paquet structuré, selon le protocole MQTT pourrait être le suivant :

```
mqtt_packet = bytearray()
mqtt_packet += bytes(packet['destination_ip'])
mqtt_packet += bytes(packet['destination_port'])
mqtt_packet += b'\x00\x00'
mqtt_packet += bytes([len(packet['topic'])])
mqtt_packet += packet['topic']
mqtt_packet += packet['payload']
```

Le procédé peut comprendre un examen 340 des données extraites tenant compte d'au moins une règle de filtrage (dite « première » règle de filtrage par référence au « premier » dispositif). L'au moins une « première » règle de filtrage peut par exemple être obtenue 342 à partir des informations présentes dans le descriptif du premier dispositif (et détaillées ci-avant). Le procédé peut ainsi comprendre un filtrage 344 des données reçues, ou en variante un filtrage des paquets formés à partir des données reçues, pour ne conserver que celles (ou ceux) en cohérence avec l'au moins une « première » règle de filtrage obtenue.

En variante, le filtrage peut être effectué sur les données extraites, de façon à ne structurer en paquets que les données à conserver. Comme expliqué ci-avant, effectuer un filtrage sur les données structurées en paquets permet de s'appuyer sur la structure des paquets pour l'application des règles de filtrage.

Comme illustré en figure 3, le procédé comprend une émission 350 du paquet obtenu sur la première portion du réseau, vers un équipement destinataire de ce paquet.

Suite à l'émission d'au moins un paquet qui correspond à une demande d'un appareil tiers (destinée à l'équipement), le premier dispositif peut optionnellement traiter une réponse de l'équipement , plus précisément le premier dispositif peut recevoir un message 362 de l'équipement et transmettre 364 ce message (après une sérialisation et/ou un filtrage avant ou après cette sérialisation éventuels) au second dispositif.

Dans certains modes de réalisation détaillées en lien avec les figures 3 et 4, le premier dispositif et le second dispositif peuvent être adaptés à communiquer selon plusieurs protocoles avec, respectivement, au moins un équipement à protéger et au moins un appareil tiers.

Dans une variante, le premier dispositif et le second dispositif peuvent communiquer avec un équipement à protéger et un appareil tiers avec un seul protocole. Par exemple, le réseau peut comporter plusieurs ensembles électroniques de protection, chacun protégeant un ou plusieurs équipements ayant un même protocole. De tels modes de réalisation peuvent permettre des

descriptifs plus simples. En particulier, dans certains modes de réalisation l'ensemble électronique peut être dédié à un protocole particulier et programmé pour ce seul protocole.

Dans une variante, lors de l'initialisation, plusieurs second dispositifs peuvent communiquer avec le premier dispositif pour transmettre respectivement des demandes d'appareils tiers utilisant des protocoles différents.

Dans une autre variante, un même second dispositif peut communiquer avec plusieurs «premiers dispositifs », ce second dispositif pouvant par exemple disposer de plusieurs adresses différentes, choisies chacune pour correspondre à celle d'un équipement protégé par un des premiers dispositifs et aiguillant les demandes reçues vers le « premier » dispositif adéquat.

La présente demande propose un ensemble électronique constituant, au moins dans certains de ses modes de réalisation, une solution simple et efficace pour demander des données de manière sécurisée à une machine industrielle connectée à un réseau public comme Internet. En particulier, dans au moins certains modes de réalisation, la configuration d'au moins un des premier et second dispositifs de l'ensemble électronique peut être facile (notamment lorsqu'elle est automatique) et l'un ou l'autre des dispositifs de l'ensemble électronique peut être utilisable avec plusieurs protocoles différents, ce qui peut donc permettre d'offrir une solution adaptable à différents environnements industriels.

La solution présentée dans la présente demande peut trouver des applications dans de nombreux domaines, et notamment dans des domaines cibles privilégiées d'attaques informatiques. Ainsi, dans l'industrie manufacturière, la solution objet de la présente demande peut aider à protéger des machines industrielles (pour empêcher leur corruption par exemple), en empêchant les accès à certaines données sensibles de ces machines comme des données relatives aux processus industriels mis en œuvre, tout en rendant d'autres données (comme des données de production) disponibles à des applications de surveillance et de contrôle. Dans l'exemple de la figure 5, l'ensemble électronique de protection 160 est mise en œuvre en œuvre pour permettre une interrogation sécurisée à distance d'une machine industrielle (l'équipement 140) par un appareil tiers de télégestion de type SCADA (Pour Supervisory Control and Data Acquisition) depuis une portion non sécurisée du réseau de communication.

Un autre exemple de mise en œuvre concerne le domaine de la distribution. La solution objet de la présente demande peut en effet être utilisée pour aider à protéger des équipements électroniques de points de vente, en limitant les possibilités d'accès à des données stockées sur ces équipements, comme des données de vente et/ou à des informations sensibles sur des clients.

Encore un autre exemple de mise en œuvre concerne le domaine de la finance (banque, service financiers) et notamment les informations financières et personnelles sensibles manipulées, que la solution objet de la présente demande peut aider à protéger d'attaques (tout en offrant des possibilités d'accès à d'autres données, moins sensibles par exemple).

La solution objet de la présente demande peut également trouver des applications dans le domaine de la santé, pour protéger les données médicales sensibles de patients tout en laissant des possibilités d'accès à au moins certaines de ces données à des professionnels de la santé.

REVENDICATIONS

1. Procédé de protection d'au moins un équipement d'un réseau de communication partitionné en une pluralité de portions comprenant au moins une première portion, comprenant ledit équipement, et au moins une seconde portion interconnectée avec ladite première portion via un premier dispositif de ladite première portion et un second dispositif de ladite seconde portion, ledit procédé comprenant :
   - une transmission audit second dispositif d'au moins un identifiant d'adressage dudit équipement de ladite première portion dudit réseau de communication ;
   - un transcodage de données reçues dudit second dispositif en au moins un paquet de données structuré comportant au moins un identifiant d'adressage d'un équipement destinataire dudit paquet sur ladite première portion ;
   - une transmission dudit paquet audit équipement destinataire ;

   au moins un desdits transcodage et/ou transmission étant effectuée de façon conditionnelle en tenant compte d'au moins une règle de filtrage relative au contenu dudit paquet.
2. Procédé de protection selon la revendication 1 où ladite règle de filtrage tient compte d'au moins un élément contenu dans ledit paquet parmi les éléments suivants :
   -une désignation d'un appareil émetteur dudit paquet ;
   -une information d'adressage relative à au moins une donnée dudit équipement ;
   - un type d'accès à effectuer sur ladite donnée ;
   -une désignation d'un protocole de communication utilisé par ledit paquet;
   - une combinaison d'au moins deux desdits éléments ci-avant ;
3. Procédé de protection selon la revendication 1 ou 2 où ledit filtrage est effectué avant ledit transcodage.
4. Procédé de protection selon la revendication 1 ou 2 où ledit filtrage est effectué après ledit transcodage.
5. Procédé de protection selon l'une des revendications 1 à 4 où lesdits premiers et second dispositifs communiquent entre eux via au moins deux chemins de communication, un premier chemin de communication unidirectionnel permettant au premier dispositif de recevoir des données dudit second dispositif, et un second chemin de communication, unidirectionnel, permettant au premier dispositif d'envoyer audit second dispositif une réponse audit paquet transmis audit équipement destinataire.
6. Procédé de protection selon l'une quelconque des revendications 1 à 5 où le procédé ledit transcodage comprend une désérialisation desdites données.
7. Procédé de transmission de données destinées à au moins un équipement d'un réseau de communication partitionné en une pluralité de portions comprenant au moins une première portion, et au moins une seconde portion interconnectée avec ladite première

portion via un premier dispositif de ladite première portion et un second dispositif de ladite seconde portion, ledit procédé comprenant :

- Une affectation audit second dispositif, comme identifiant d'adressage sur ladite seconde portion dudit réseau, d'au moins un identifiant d'adressage d'un équipement de ladite première portion ;
- Sur réception d'un paquet structuré de données ayant comme adresse de destination ledit identifiant d'adressage, une sérialisation des données dudit paquet ; et
- une émission desdites données sérialisées vers ledit premier dispositif.

au moins une de ladite sérialisation et/ou ladite émission étant effectuée de façon conditionnelle en tenant compte d'au moins une règle de filtrage relative au contenu dudit paquet.

8. Procédé de transmission selon la revendication 7 où ladite règle de filtrage tient compte d'au moins un élément contenu dans ledit paquet parmi les éléments suivants :
   -une désignation d'un appareil émetteur dudit paquet ;
   -une information d'adressage relative à au moins une donnée dudit équipement ;
   - un type d'accès à effectuer sur ladite donnée ;
   -une désignation d'un protocole de communication utilisé par ledit paquet;
   - une combinaison d'au moins deux desdits éléments ci-avant ;
9. Procédé de transmission selon la revendication 7 ou 8 comprenant une obtention d'un descriptif relatif audit équipement de ladite première portion dudit réseau de communication comportant ledit au moins un identifiant d'adressage dudit au moins un équipement sur ladite première portion dudit réseau de communication.
10. Procédé de transmission selon l'une des revendications 7 à 9 où ledit filtrage est effectué sur les données sérialisées
11. Procédé de transmission selon l'une des revendications 7 à 10 où ledit filtrage est effectué avant ladite sérialisation.
12. Procédé de transmission selon l'une des revendications 7 à 11 où lesdits premiers second dispositifs communiquent entre eux via au moins deux chemins de communication unidirectionnel, un premier chemin de communication unidirectionnel permettant au second dispositif de transmettre des données audit premier dispositif, et un second chemin de communication, unidirectionnel, permettant au second dispositif de recevoir du premier dispositif une réponse auxdites données transmises audit premier dispositif.
13. Premier dispositif électronique d'un réseau de communication partitionné en une pluralité de portions comprenant au moins une première portion, comprenant au moins un équipement à protéger et ledit premier dispositif, et au moins une seconde portion interconnectée avec ladite première portion via le premier dispositif et un second

dispositif de ladite seconde portion, ledit premier dispositif comprenant un moins un processeur configuré pour :

- une transmission audit second dispositif d'au moins un identifiant d'adressage duit équipement de ladite première portion dudit réseau de communication ;
- un transcodage de données reçues dudit second dispositif en au moins un paquet de données structuré comportant au moins un identifiant d'adressage d'un équipement destinataire dudit paquet sur ladite première portion ;
- une transmission dudit paquet audit équipement destinataire ;

au moins un desdits transcodage et/ou transmission étant effectuée de façon conditionnelle en tenant compte d'au moins une règle de filtrage.

14. Second dispositif électronique d'un réseau de communication partitionné en une pluralité de portions comprenant au moins une première portion, comprenant au moins un équipement, et au moins une seconde portion comprenant ledit second dispositif, et interconnectée avec ladite première portion via un premier dispositif de ladite première portion et le second dispositif; ledit second dispositif comprenant un moins un processeur configuré pour :

- une affectation audit second dispositif, comme identifiant d'adressage sur ladite seconde portion dudit réseau, d'au moins un identifiant d'adressage d'un équipement de ladite première portion
- sur réception d'un paquet structuré de données ayant comme adresse de destination ledit identifiant d'adressage, une sérialisation des données dudit paquet et ;
- une émission desdites données sérialisées vers ledit premier dispositif ;

au moins une de ladite sérialisation et/ou ladite émission étant effectuée de façon conditionnelle en tenant compte d'au moins une règle de filtrage relative au contenu dudit paquet.

15. Ensemble électronique de protection d'au moins un équipement d'un réseau de communication partitionné en une pluralité de portions comprenant au moins une première portion, comprenant ledit équipement, et au moins une seconde portion interconnectée avec ladite première portion via au moins un premier dispositif dudit ensemble électronique, ledit premier dispositif appartenant à ladite première portion, et au moins un second dispositif dudit ensemble électronique, ledit second dispositif appartenant à ladite seconde portion,

- ledit au moins un premier dispositif électronique comprenant un moins un processeur configuré pour :
  - une transmission audit second dispositif d'au moins un identifiant d'adressage dudit équipement de ladite première portion dudit réseau de communication ;

- un transcodage de données reçues dudit second dispositif en au moins un premier paquet de données structuré comportant au moins un identifiant d'adressage d'un équipement destinataire dudit premier paquet sur ladite première portion ;
- une transmission dudit premier paquet audit équipement destinataire ;

au moins un desdits transcodage et/ou transmission étant effectuée de façon conditionnelle en tenant compte d'au moins une première règle de filtrage relative au contenu dudit premier paquet.

- ledit au moins un second dispositif électronique comprenant un moins un processeur configuré pour :
  - une affectation audit second dispositif, comme identifiant d'adressage sur ladite seconde portion dudit réseau, d'au moins un identifiant d'adressage d'un équipement de ladite première portion
  - sur réception d'un second paquet structuré de données ayant comme adresse de destination ledit identifiant d'adressage, une sérialisation des données dudit second paquet et ;
  - une émission desdites données sérialisées vers ledit premier dispositif.

au moins une de ladite sérialisation et/ou ladite émission étant effectuée de façon conditionnelle en tenant compte d'au moins une seconde règle de filtrage relative au contenu dudit second paquet.

16. Programme d'ordinateur comprenant des instructions pour la mise en œuvre d'un procédé de protection selon l'une des revendications 1 à 6, et/ou d'un procédé de transmission selon l'une des revendications 7 à 12, lorsque ledit programme est exécuté par un processeur.

17. Support d'informations lisible par un dispositif électronique et sur lequel est enregistré un programme d'ordinateur comprenant des instructions pour la mise en œuvre d'un procédé de protection selon l'une au moins des revendications 1 à 6, et/ou d'un procédé de transmission selon l'une au moins des revendications 7 à 12.

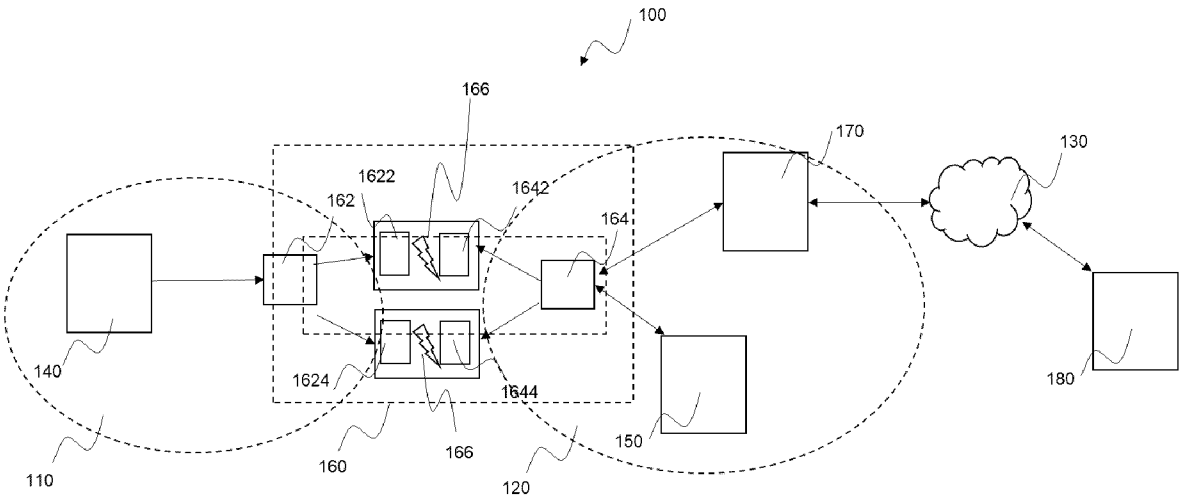
100
166
170
130
1622
162
1642
164
140
1624
1644
150
180
110
160
166
120

Fig 1

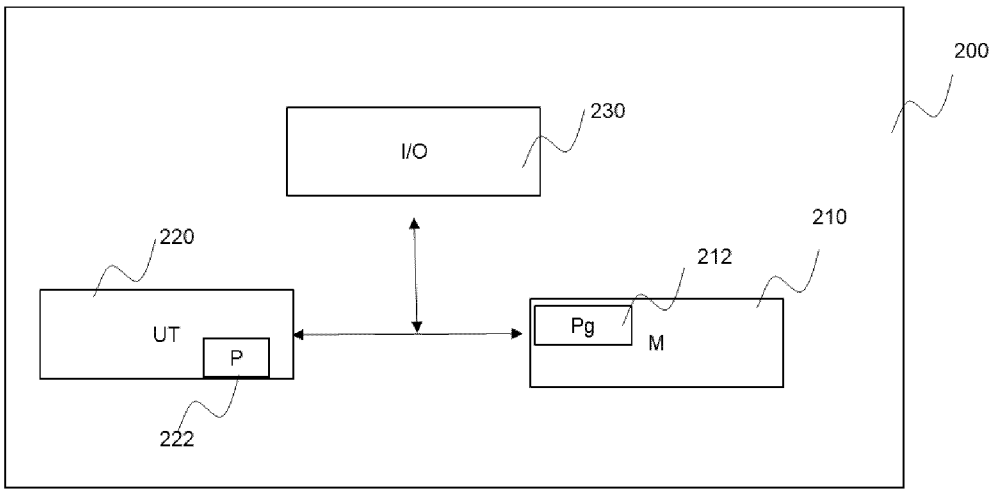
200
230
I/O
210
220
212
UT
P
Pg
M
222

Fig 2

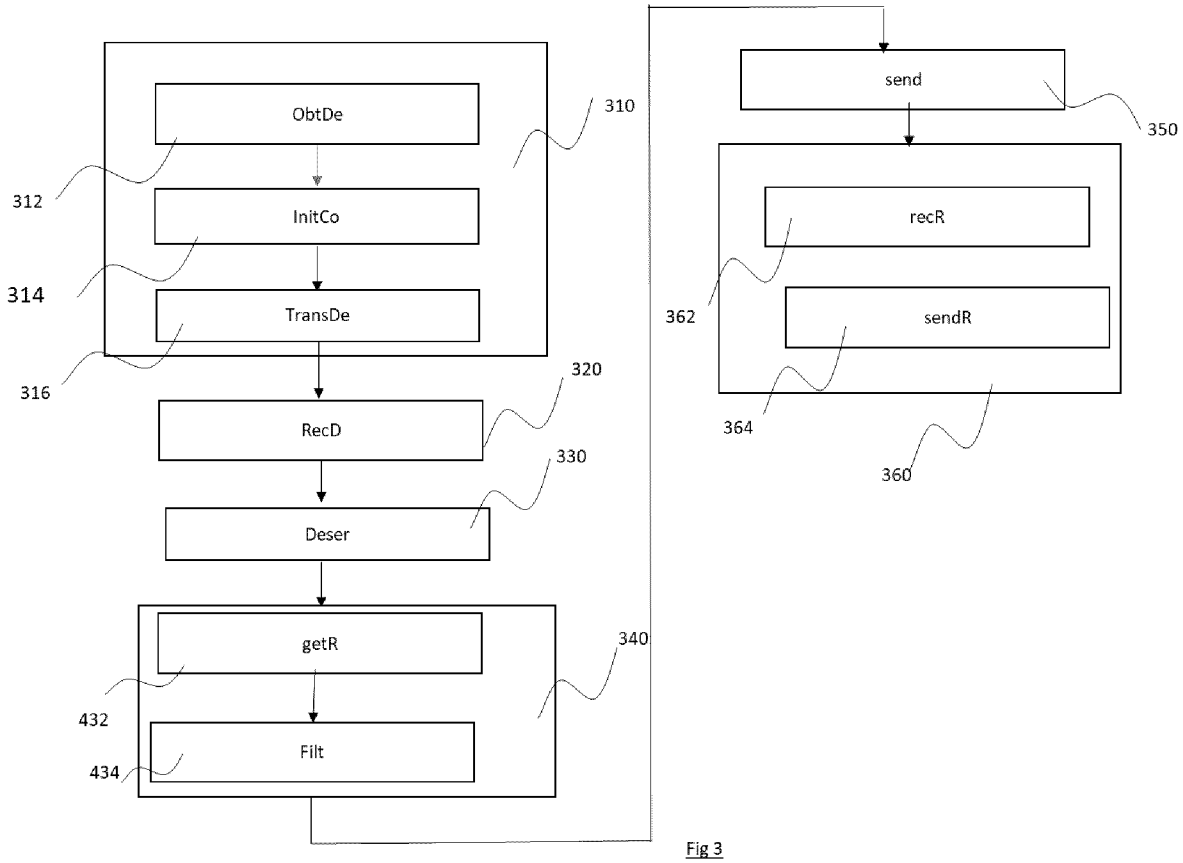
ObtDe
InitCo
TransDe
RecD
Deser
getR
Filt
310
312
314
316
320
330
340
432
434
send
recR
sendR
350
362
364
360

Fig 3

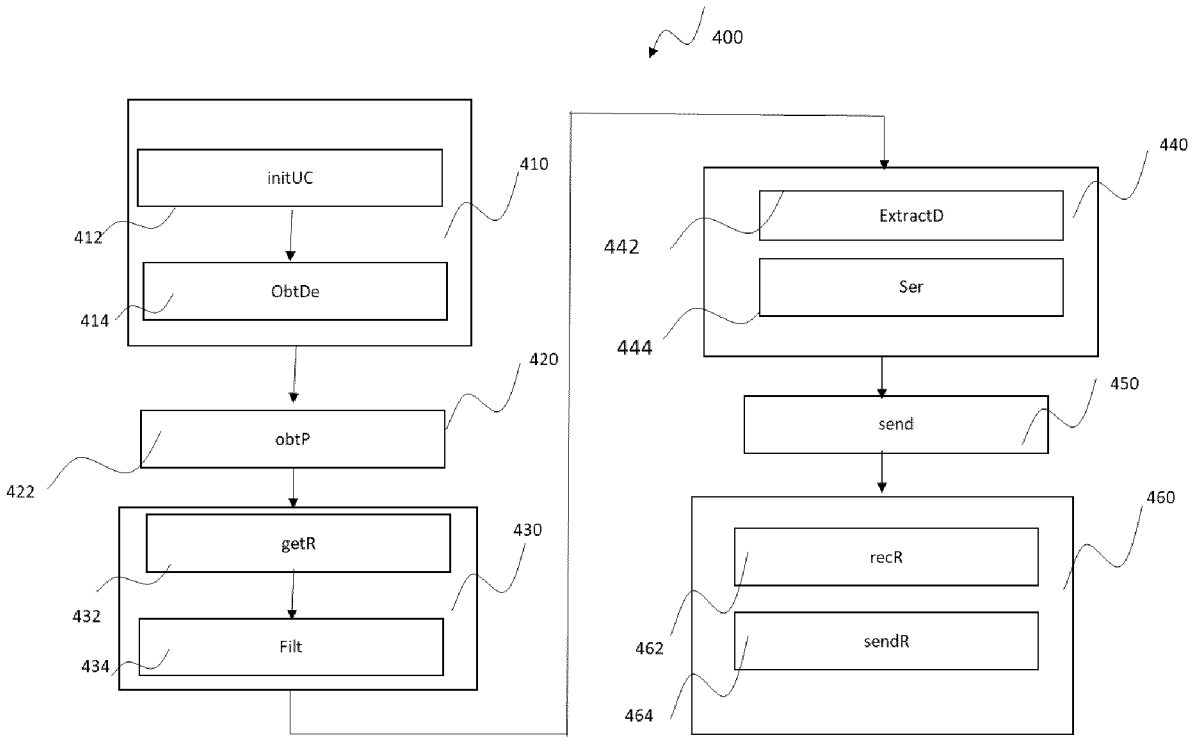
400
initUC
ObtDe
obtP
getR
Filt
410
412
414
420
422
430
432
434
ExtractD
Ser
send
recR
sendR
440
442
444
450
460
462
464

Fig 4

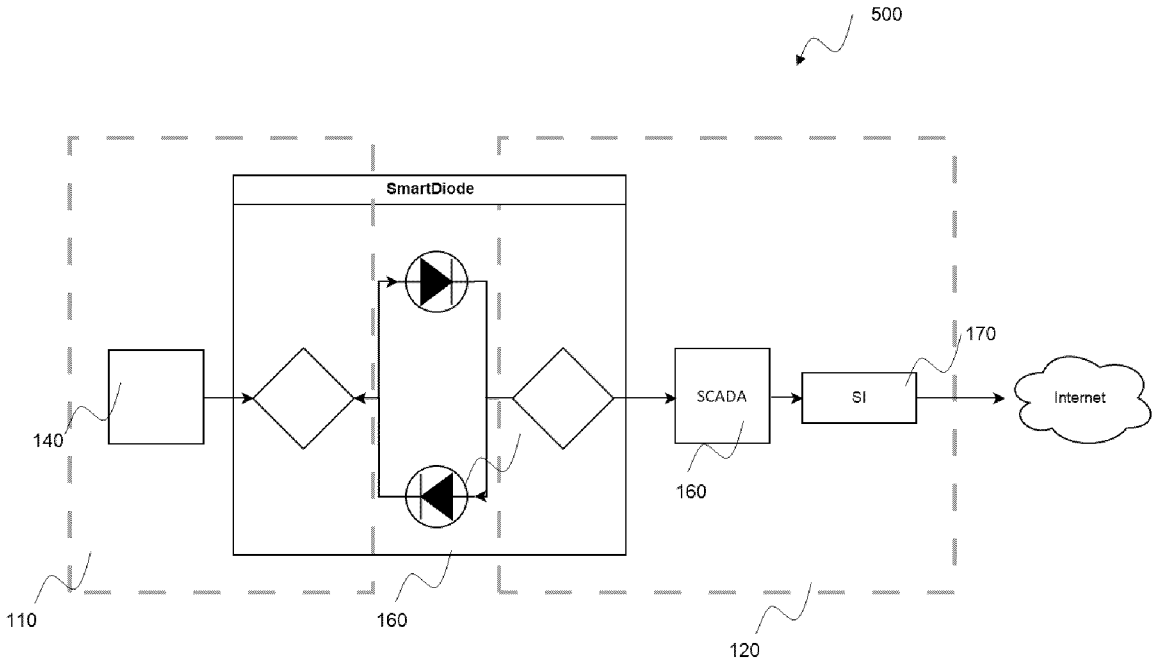

Fig 5

INTERNATIONAL SEARCH REPORT

International application No.
PCT/EP2024/067921

A. CLASSIFICATION OF SUBJECT MATTER

H04L 9/40(2022.01)i

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

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.
X	US 2020036732 A1 (GRUBEL BRIAN C [US] ET AL) 30 January 2020 (2020-01-30) abstract paragraph [0005] - paragraph [0008] paragraph [0018] - paragraph [0020]; figure 1 paragraph [0021] - paragraph [0048]; figure 2 paragraph [0049] - paragraph [0051]; figure 3 paragraph [0052] - paragraph [0057]; figure 4	1-17
A	US 2020106742 A1 (MOORE SEAN [US] ET AL) 02 April 2020 (2020-04-02) abstract paragraph [0002] - paragraph [0046]	1-17
A	EP 3729773 B1 (FEND INCORPORATED [US]) 03 November 2021 (2021-11-03) abstract paragraph [0003] - paragraph [0022] paragraph [0039] - paragraph [0064]	1-17

☐ Further documents are listed in the continuation of Box C. ☑ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
28 August 2024	**13 September 2024**

Name and mailing address of the ISA/EP	Authorized officer
European Patent Office **p.b. 5818, Patentlaan 2, 2280 HV Rijswijk** **Netherlands (Kingdom of the)** Telephone No. **(+31-70)340-2040** Facsimile No. **(+31-70)340-3016**	**Jakob, Gregor** Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/EP2024/067921

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
US 2020036732 A1	30 January 2020	CN 110784438 A	11 February 2020
		EP 3599566 A1	29 January 2020
		US 2020036732 A1	30 January 2020
US 2020106742 A1	02 April 2020	CN 112602301 A	02 April 2021
		CN 118018282 A	10 May 2024
		EP 3821580 A1	19 May 2021
		US 10333898 B1	25 June 2019
		US 2020106742 A1	02 April 2020
		US 2022210125 A1	30 June 2022
		WO 2020014134 A1	16 January 2020
EP 3729773 B1	03 November 2021	CA 3086589 A1	27 June 2019
		EP 3729773 A1	28 October 2020
		US 2019197002 A1	27 June 2019
		WO 2019126237 A1	27 June 2019

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale n°
PCT/EP2024/067921

A. CLASSEMENT DE L'OBJET DE LA DEMANDE

INV. H04L9/40
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)
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
X	US 2020/036732 A1 (GRUBEL BRIAN C [US] ET AL) 30 janvier 2020 (2020-01-30) abrégé alinéa [0005] - alinéa [0008] alinéa [0018] - alinéa [0020]; figure 1 alinéa [0021] - alinéa [0048]; figure 2 alinéa [0049] - alinéa [0051]; figure 3 alinéa [0052] - alinéa [0057]; figure 4	1-17
A	US 2020/106742 A1 (MOORE SEAN [US] ET AL) 2 avril 2020 (2020-04-02) abrégé alinéa [0002] - alinéa [0046]	1-17
A	EP 3 729 773 B1 (FEND INCORPORATED [US]) 3 novembre 2021 (2021-11-03) abrégé alinéa [0003] - alinéa [0022] alinéa [0039] - alinéa [0064]	1-17

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

☒ Les documents de familles de brevets sont indiqués en annexe

* Catégories spéciales de documents cités:

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

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
28 août 2024	13/09/2024

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

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Demande internationale n°
PCT/EP2024/067921

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
US 2020036732 A1	30-01-2020	CN 110784438 A	11-02-2020
		EP 3599566 A1	29-01-2020
		US 2020036732 A1	30-01-2020
US 2020106742 A1	02-04-2020	CN 112602301 A	02-04-2021
		CN 118018282 A	10-05-2024
		EP 3821580 A1	19-05-2021
		US 10333898 B1	25-06-2019
		US 2020106742 A1	02-04-2020
		US 2022210125 A1	30-06-2022
		WO 2020014134 A1	16-01-2020
EP 3729773 B1	03-11-2021	CA 3086589 A1	27-06-2019
		EP 3729773 A1	28-10-2020
		US 2019197002 A1	27-06-2019
		WO 2019126237 A1	27-06-2019