Synthèse sur les protocoles de communication pour l'Internet des objets de l'industrie 4.0

Alexis Bitaillou, Benoît Parrein, Guillaume Andrieux

Synthèse sur les protocoles de communication pour l'Internet des objets de l'industrie 4.0

Janvier 2019

Rédigé par : Alexis BITAILLOU, doctorant

Sous la direction de : Benoît PARREIN, maitre de conférences
Guillaume ANDRIEUX, maitre de conférences

Dans le cadre du projet de recherche COWIN,

financé par les RFI WISE et Atlanstic2020,

labellisé par les pôles EMC2 et Images & Réseaux.

Laboratoires LS2N (UMR 6004) - IETR (UMR 6164)

Table des matières

Introduction

Cette synthèse est un extrait de l'état de l'art de la thèse « Réseaux cognitifs sans fil pour des applications industrielles 4.0 ». Cette thèse est encadrée par Benoît PARREIN (LS2N - UMR 6004) et Guillaume ANDRIEUX (IETR - UMR 6164). Elle est financée dans le cadre du projet COWIN par le RFI WISE et le RFI Atlanstic 2020. L'objectif de cette thèse est de valider le concept de réseaux sans fil cognitifs qui consiste à estimer de manière automatique les paramètres protocolaires de la pile OSI afin de satisfaire les critères de qualité de service (QoS) et d'usage (QoE). Le contexte applicatif de cette thèse est celui de l'Industrie du Futur. Dans notre cas, nous nous attacherons à l'industrie 4.0. Ce document s'articule en 3 sections. La première partie définit le cadre de l'utilisation de l'Internet des objets industriel (IIoT). Ensuite, nous proposons de définir l'Internet des objets industriel. Enfin, nous aborderons les différentes technologies réseaux présentes dans l'industrie permettant de relier les éléments industriels à l'IoT.

Alexis Bitaillou est ingénieur en Informatique diplômé de Polytech Nantes. Depuis 2018, il est doctorant dans l'équipe de recherche RIO (Réseaux pour l'Internet des Objets) au sein du Laboratoire des Sciences du Numérique de Nantes (LS2N). Ses centres d'intérêt portent sur les réseaux cognitifs et la sécurité informatique. Contact : alexis.bitaillou@ls2n.fr

Benoît Parrein est Maître de Conférences à l'Université de Nantes (Polytech Nantes). Il est titulaire de l'Habilitation à Diriger des Recherches (HDR) depuis 2015. Ses centres d'intérêt portent sur les réseaux pour l'Internet des Objets, les réseaux auto-organisés et les réseaux de robots. Il est co-auteur de plus de 50 publications nationales et internationales. Depuis 2017, il est responsable de l'équipe de recherche RIO (Réseaux pour l'Internet des Objets) au sein du Laboratoire des Sciences du Numérique de Nantes (LS2N). Contact : benoit.parrein@ls2n.fr

Guillaume Andrieux est Maître de Conférences à l'Université de Nantes (IUT de La Roche-sur-Yon). Il a obtenu un doctorat en électronique et télécommunications en 2004 puis l'Habilitation à Diriger des Recherches (HDR) en 2018. Il effectue sa recherche dans l'équipe SYSCOM (SYStems, COMmunication) du laboratoire IETR (Institut d'Electronique et de Télécommunications de Rennes). Ses centres d'intérêt portent actuellement sur les communications numériques, le traitement d'antennes et l'efficacité énergétique dans les réseaux sans fil.

1 Industrie 4.0

Nous allons brièvement rappeler l'évolution de l'industrie, puis nous présenterons l'industrie 4.0, son contexte et ses ambitions.

1.1 Introduction

L'industrie commença notamment grâce à l'invention de la machine à vapeur au XVIIIe siècle. La révolution industrielle permit d'augmenter la productivité et de diminuer les coûts de certains biens manufacturés. Les secteurs du textile et de la sidérurgie sont les plus impactés. Cette première révolution industrielle est caractérisée par la mécanisation.

La deuxième révolution industrielle fut portée par l'électrisation. L'électricité remplaça le charbon et rendit la machine à vapeur obsolète dans l'industrie. Les équipements électriques sont plus sûrs à l'utilisation ainsi que plus efficient que la machine à vapeur. La deuxième révolution industrielle a permis la production de masse notamment grâce à la réorganisation du travail et à la chaîne d'assemblage.

Avec le perfectionnement de l'électronique et le développement des nouvelles technologies de l'information et de la communication (NTIC) à la fin du XXe siècle, l'industrie entra dans une nouvelle ère. L'industrie 3.0 commence juste après les deux premiers chocs pétroliers. L'électricité devient donc l'énergie prépondérante. L'industrie 3.0 introduit l'automatisation et l'informatique dans l'industrie. L'automatisation peut prendre la forme de robotisation, par exemple. L'objectif est que les ouvriers n'ont plus à faire les tâches simples et répétitives. Cela implique une réduction de la masse salariale non qualifiée, mais aussi l'emploi de personnel qualifié pour la maintenance des équipements. L'informatique dans l'entreprise permet une meilleure gestion des ressources. Par exemple, les entreprises s'équipent de progiciel de gestion intégré[1], ce qui permet la centralisation des informations et de la planification. Les communications sont facilitées par le déploiement de réseaux câblés, notamment l'Internet.

L'industrie 4.0 possède quelques prérequis techniques. Avant de passer à l'industrie 4.0, il faut déjà avoir la maîtrise de l'industrie 3.0 [Chr17]. Comme il était indispensable d'avoir l'électrisation pour utiliser la robotique, il est indispensable d'utiliser l'automatisation et les NTIC pour commencer à mettre en œuvre l'industrie 4.0. L'autre prérequis concerne l'Internet des Objets (IoT). L'IoT est un domaine qui est apparu cette dernière décennie. Il repose surtout sur les capteurs et les terminaux de faible puissance connectés à Internet. Un système cyber-physique (CPS) est un système où des éléments informatiques contrôlent les éléments physiques. Par exemple, un distributeur de billet de banque est un système cyber-physique. L'IoT adapté à l'industrie (Industrial Internet of Things) et les systèmes cyber-physiques sont considérés comme des éléments fondamentaux de l'industrie 4.0 [ZLZ15].

Il existe une initiative française nommée « Nouvelle France Industrielle » (NFI) depuis 2015. Elle s'appuie aussi sur l'industrie du futur. Elle définit neuf secteurs clés : l'économie des données, les objets intelligents, la confiance numérique, l'alimentation intelligente, les nouvelles ressources, la ville durable, la mobilité écologique, les transports de demain et la médecine du futur. Enfin, le projet Nouvelle France Industrielle précise 47 technologies clés dont l'Internet des objets, l'intelligence artificielle, la robotique autonome et les réseaux électriques intelligents.

1. ERP pour le sigle en anglais.

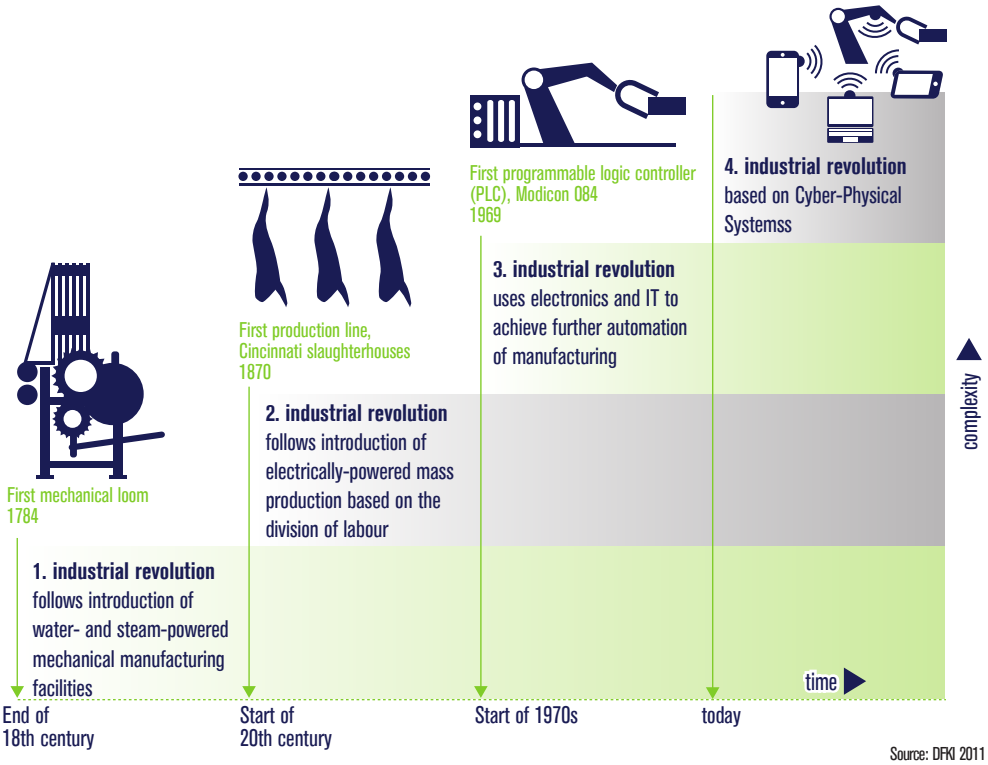

FIG. 1 : De la première révolution industrielle à l'industrie 4.0, *extrait du site du Deutsches Forschungszentrum für Künstliche Intelligenz (DFKI)*

1.2 Les origines de l'industrie 4.0

Les origines de l'industrie 4.0 sont relativement simples. Le concept d'industrie 4.0 est développé dans une étude sponsorisée par le ministère fédéral allemand de l'enseignement et de la recherche. Il demande à un comité composé de chercheurs académiques et industriels de se pencher sur la question « comment sécuriser l'avenir de l'industrie manufacturière allemande » [Kag13]. La réponse de ce comité est un rapport d'environ 80 pages publié en 2013. *Recommendations for implementing the strategic initiative INDUSTRIE 4.0* fait rapidement un « état des lieux » de l'industrie au niveau mondial et propose un ensemble de recommandations pour mettre en place l'industrie 4.0. L'industrie allemande fait partie des leaders mondiaux. Néanmoins, elle est menacée par l'industrie chinoise et étasunienne. Par exemple, l'industrie chinoise a des coûts salariaux moindres. De plus, combiné avec sa capacité de production, il est possible de produire un bien en grande quantité et à faible coût. Les coûts salariaux en Allemagne sont relativement élevés. Il n'est donc pas possible de produire en masse et à faible coût en Allemagne. L'industrie allemande doit donc trouver un moyen de rester compétitif, voire se démarquer des autres industries. Un autre élément vient handicaper l'industrie allemande. Le nombre de personnes hautement qualifié est insuffisant pour satisfaire la demande. Pire, le déficit tend même à se creuser dans les prochaines années. A défaut de pouvoir recruter, l'industrie allemande doit soit garder ses employés plus longtemps actifs, soit les faire évoluer en interne.

1.3 Les ambitions de l'industrie 4.0

L'objectif principal de l'industrie 4.0 est de créer de la valeur ajoutée dans l'industrie manufacturière, indépendamment des coûts salariaux [Kag13]. Il est possible de découper cet objectif en plusieurs sous-objectifs.

1.3.1 Une optimisation des moyens et des ressources

Le premier point est d'optimiser le processus de fabrication. Pour cela, il faut que les équipements de production soient le plus polyvalent possible. L'objectif est de pouvoir remplacer une machine par une autre en cas de besoin. Par exemple, en cas de maintenance ou en cas de changement de bien à produire, l'usine ne doit pas être dépendante d'une machine. De plus, la chaîne de production doit être flexible. Elle doit pouvoir s'adapter rapidement au processus de production.

Une chaîne de production capable de s'adapter rapidement permet d'éviter les temps morts. Ce n'est qu'un élément pour optimiser les coûts. D'autres éléments comme la gestion des matières premières sont aussi importants. La nouveauté de l'industrie 4.0 est la possibilité de simuler le niveau des stocks, le transport et la logistique. Cela permettra de mieux anticiper les approvisionnements par exemple. La gestion de l'énergie peut être améliorée notamment pendant les week-ends et les périodes de vacances. L'idée de Siemens repris dans [Kag13] est de pouvoir passer l'usine en « mode veille ». L'efficacité et l'efficience des ressources utilisées est un point clé pour réduire le coût des produits.

1.3.2 Vers plus de flexibilité

La flexibilité des processus de fabrication est un élément clé de l'industrie 4.0. L'industrie 4.0 permet la création de valeur par la personnalisation du bien par le client. L'objectif est que chaque client puisse demander un produit sur-mesure. Pour cela, il faut donc pouvoir adapter le processus de fabrication en fonction des besoins. Les équipements doivent être reconfigurables « à la volée ». Selon Grier [Gri17], l'idée est que les usines deviennent reconfigurables rapidement et à très faible coût à la manière du *cloud computing*. Ce qui implique le développement de solutions équivalentes à celles présentes dans le cloud computing. Par exemple avec des solutions comme les réseaux logiciels (ou *Software-Defined Network*, SDN) en réseaux informatiques, un contrôleur peut (re)configurer un ensemble d'équipements (semi-)automatiquement et très rapidement. Nous retrouvons ce lien avec le cloud computing dans le nom de certains modèles. Par exemple, un modèle d'implémentation de l'industrie 4.0 porte le nom de *cloud manufacturing*. Comme le cloud computing, l'industrie 4.0 doit supporter l'intégration de bout en bout de la chaîne de valeur. Elle doit aussi permettre l'intégration verticale. L'intégration verticale est la capacité à augmenter les capacités en augmentant la capacité des éléments existants. L'intégration verticale d'une usine consiste à pouvoir ajouter une ligne de production sans construire une autre usine, par exemple. L'intégration horizontale consisterait à construire une usine supplémentaire de capacité comparable. Par analogie avec le stockage de données, l'intégration verticale consisterait à augmenter la capacité de stockage d'un/des serveur(s). En intégration horizontale, un serveur supplémentaire serait ajouté au groupe de serveur.

1.3.3 Des technologies standardisées et ouvertes

Une recommandation pour l'industrie 4.0 est de reposer sur un unique ensemble de standards ouverts. L'exemple cité dans [Kag13] est l'ensemble des normes IEEE (Institute of Electrical and Electronics Engineers) et IETF (Internet Engineering Task Force). Cette recommandation est importante car elle permettrait aux entreprises de ne pas être dépendant technologiquement. Par

exemple, des solutions commerciales comme Sercos ou PROFINET se tournent vers des standards IEEE (Ethernet notamment) et IETF pour assurer leur pérennité. Une partie des technologies, notamment réseaux, destinées aux entreprises sont propriétaires. L'autre avantage est que les entreprises puissent pouvoir communiquer, que leurs systèmes soient interopérables. L'un des points bloquants est pour le moment la gestion du temps réel. Par exemple, Ethernet n'est pas particulièrement adapté au temps réel. Des solutions propriétaires comme les deux premières versions de Sercos ou PROFIBUS permettent une gestion « native » du temps réel et de la latence.

1.3.4 Sûreté de fonctionnement

La sûreté est un élément des plus importants dans l'industrie. Il est nécessaire de protéger les biens et les personnes des éventuels risques. L'industrie 4.0 réaffirme cette priorité et l'étend à l'environnement au sens large. Les problèmes de sûreté sont apparus dès le début de l'industrie. Les accidents sont potentiellement plus graves avec des machines. La plupart d'entre eux ont heureusement été résolus notamment ceux liés aux protections des équipements. L'industrie 3.0 a introduit de nouveaux défis techniques. Un problème majeur apparu lors de l'industrie 3.0 est celui de la sécurité informatique.

1.3.5 Sécurité informatique

Aux débuts de l'intégration des NTIC, la sécurité n'est pas une priorité. Les fonctionnalités ont été préférées à la sécurité. Les premiers virus comme le ver Morris [Orm03] ont montré que la sécurité ne devait plus être négligée. Ces menaces s'attaquent principalement aux systèmes informatiques des entreprises. Le but est soit de voler des données stratégiques, soit de paralyser l'entreprise. WannaCry [Ehr17] est un exemple du second cas. Ce rançongiciel est capable de paralyser l'intégralité d'un réseau informatique jusqu'à paiement d'une rançon. Le système de santé britannique NHS et différentes entreprises comme Saint-Gobain et Renault ont vu leurs parcs informatiques bloqués pendant plusieurs jours suites aux infections de rançongiciels. Autre exemple, Petya et ses variantes auraient coûté plus d'un milliard d'euros aux entreprises selon une estimation du Monde [Ute17]. Stuxnet est un exemple d'attaque contre des équipements industriels [CA11 ; Kus13]. Stuxnet est un virus étatique destiné à freiner le programme nucléaire iranien. Il a commencé par infecter un grand nombre d'ordinateurs. Une fois sur le réseau de contrôle des équipements de la centrale nucléaire, le virus a pris possession du système de contrôle et d'acquisition de données (SCADA). Enfin, il a faussé les informations et a fait fonctionner les centrifugeuses anormalement jusqu'à destruction. Stuxnet a démontré qu'il était possible de détruire des équipements physiques connectés à un système informatique. Dans un cadre industriel, les cybermenaces peuvent bloquer le fonctionnement d'une entreprise et détruire des équipements, d'après ces exemples. Dans l'industrie 4.0, la sécurité est donc considérée comme cruciale, au même titre que la sûreté. Pour les systèmes cyber-physiques, la sécurité doit être intégrée dès la conception (*security by design*).

1.3.6 L'humain dans l'industrie 4.0

Les objectifs de l'industrie 4.0 ne sont pas uniquement financiers et techniques. Le rapport met en avant la nécessité de former les employés tout au long de leur carrière. La formation doit pouvoir faciliter les reconversions en interne, par exemple. Concrètement, il s'agit de permettre de faire évoluer les employés, afin qu'ils gagnent en responsabilités, qu'ils puissent participer à l'organisation du travail et qu'ils puissent avoir une longue carrière au sein de l'entreprise.

1.4 Mise en œuvre de l'industrie 4.0

Nous avons vu les objectifs de l'industrie 4.0. Ils sont certes ambitieux mais reste dans la continuité de l'industrie 3.0. Nous retrouvons les prémices de l'industrie 4.0 dans des concepts des années 2000 [MFD00 ; Fan+05]. En 2003, Lee [Lee03] propose le concept d'*E-manufacturing*. On retrouve certains éléments de l'industrie 4.0 comme le lien entre les systèmes de productions et le système d'information et de planification, la surveillance des équipements, les outils de prédiction de maintenance ainsi que les outils d'optimisation de la production.

Le dernier modèle avant la présentation de l'industrie est le cloud manufacturing [Li+10 ; Xu12]. Ce modèle s'inspire du cloud computing. Il considère l'usine comme un ensemble de ressources, compétences et capacités utilisables comme des services. Tao *et al.* [Tao+11] évoquent la possibilité d'utiliser les périphériques IoT pour automatiquement gérer et contrôler certains équipements. Le cloud manufacturing est un modèle proche techniquement des attentes de l'industrie 4.0.

D'après le rapport « Recommendations for implementing the strategic initiative INDUSTRIE 4.0 » [Kag13], les industriels allemands estiment qu'il faudra attendre 2025 pour que l'industrie 4.0 soit pleinement établie et opérationnelle. Dans l'article [Alm16], Almada-Lobo évoque la difficulté à mettre en œuvre l'industrie 4.0. Par exemple, il met en avant deux interprétations distinctes sur la décentralisation des équipements. Il cite l'exemple de la répartition de la puissance de calcul. La question posée est : est-ce que la puissance de calcul doit être physiquement décentralisée ou seulement logiquement décentralisée ?

Des équipes de recherche commencent à réfléchir à l'organisation de l'usine dans le cadre de l'industrie du futur. La contrainte majeure est que l'usine soit reconfigurable à la demande. Son agencement n'est plus laissé au hasard. Wang *et al.* [Wan+16b] proposent par exemple un modèle supportant l'intégration verticale.

Comme le montre les articles [Lu17 ; Tra+17], de nombreux travaux ont publié sur l'industrie 4.0. Nous retrouvons le choix des technologies comme un des questionnements majeurs. Comme la recommandation est de choisir un unique ensemble technologique [Kag13], le choix devient crucial. Nous pouvons citer comme critères la standardisation, la pérennité, le coût d'intégration. Par exemple, concernant les choix des périphériques IoT, les Raspberry Pi semblent privilégiés. Par leur conception ouverte, ils respectent la recommandation sur les technologies ouvertes. Concernant la partie réseau, nous nous orientons pour les réseaux câblés vers Ethernet. En effet, des solutions commerciales comme Sercos et PROFINET ont adoptées Ethernet. Ethernet a été choisi pour sa pérennité.

2 L'Internet des objets industriel

Nous allons commencer par faire un historique de l'internet des objets (Internet of Things, IoT). Puis nous verrons comment l'internet des objets peut intervenir dans un cadre industriel. Enfin, nous terminerons par les limites et challenges liés à l'internet des objets.

2.1 Introduction

Dans cette introduction, nous allons remonter aux origines de l'Internet des objets et poser sa définition. Ensuite, nous verrons quelques domaines d'applications.

2.1.1 Les origines de l'Internet des objets

Les origines de l'expression « Internet of Things » sont assez obscures [MBR15]. Le nom est né du domaine de la RFID (Radio Frequency IDentification). D'après [MBR15], « Internet of Things »

serait apparu dans un document de l'Union internationale des télécommunications en 1997. Au début des années 2000, l'Auto-ID Center utilisa le terme « Internet of Things ». Il associe IoT au système Electronic Product Code (EPC) et à la possibilité de récupérer des informations d'un tag RFID depuis Internet [Bro01a ; SBE01 ; TM06]. Finalement, l'origine du nom « Internet of Things » est revendiquée par Ashton en 2009 [Ash09]. Il affirme avoir commencé à l'utiliser à partir de 1999. Il définit l'IoT comme des objets uniquement identifiables et interopérables connectés par RFID [LXZ15].

2.1.2 Au départ, plusieurs initiatives, un IoT finalement

Nous avons vu que le terme « Internet of Things » venait très probablement du « domaine RFID ». D'autres articles mettent en avant la technologie RFID comme technologie principale de communication [TM06 ; DM08 ; Wel+09]. En 2005, l'Union internationale des télécommunications (UIT ou ITU) produit un premier rapport sur l'IoT [SU05]. Elle met aussi en avant la technologie RFID mais pas exclusivement. L'UIT évoque les technologies liées aux capteurs, les objets intelligents et les nanotechnologies.

Le terme *Internet of Things* apparaît pour la première dans la littérature scientifique en 2004 [GKC04]. Cet article prend d'abord l'exemple de la domotique et les bâtiments intelligents. Il pose le concept d'internet des objets, un réseau d'objets du quotidien. « Même quelque chose d'aussi simple qu'une ampoule pourrait être connectée directement à l'Internet, si elle est convenablement équipée avec un système capable d'envoyer des signaux via un câble ». Surtout, il fixe quelques « règles » concernant les objets connectés. La simplicité d'installation et d'utilisation est la première des règles. Par exemple, l'installation d'une ampoule connectée ne doit pas nécessiter l'emploi d'un ingénieur « réseaux ». Un autre point est la diminution des coûts et de la complexité de l'installation et de la configuration de l'objet dans le réseau. Concernant le réseau, pour eux, l'Internet n'est pas adapté aux besoins des objets connectés. Par exemple, le nombre d'adresses Ethernet MAC (Media Access Control) disponible est insuffisant. Il propose donc un système d'adressage automatique avec des adresses sur 128 bits. Les auteurs optent pour IP comme protocole commun. Cet ensemble de propositions constitue l'Internet 0, un des ancêtres de l'Internet des objets tel que nous le connaissons [KG04 ; Kri04].

L'Internet 0 n'est qu'une initiative qui participera à la création de l'IoT. D'autres projets comme IPSO (IP for Smart Objects) [DV08] et Web of Things [GT09] ont aussi apportés leurs contributions. Par exemple, IPSO insiste pour qu'IP soit un élément clé de la communication IoT. Les technologies fermées et/ou propriétaires sont vues comme une crainte. Web of Things met en avant la nécessité d'intégrer les technologies Web au monde des objets communicants [ZGC11]. Par exemple, Web of Things propose de remplacer HTTP par CoAP (Constrained Application Protocol, RFC 7252), un protocole similaire mais adapté aux terminaux dotés de faible ressource. Comme il n'y a pas encore de définition formelle de l'Internet des objets, d'autres visions de l'IoT se développent. La figure 2 montre l'IoT finalement comme une convergence de plusieurs visions.

2.1.3 La définition de l'UIT-T

En 2012, UIT-T s'empare de l'Internet des Objets. Il propose la recommandation Y.2060, *Présentation générale de l'Internet des objets* [TEL12]. UIT-T propose la définition suivante de l'Internet des objets : « infrastructure mondiale pour la société de l'information, qui permet de disposer de services évolués en interconnectant des objets (physiques ou virtuels) grâce aux technologies de l'information et de la communication interopérables existantes ou en évolution. » Il fournit aussi les caractéristiques fondamentales de l'IoT. Dans l'IoT, un objet peut se connecter à l'Internet. La

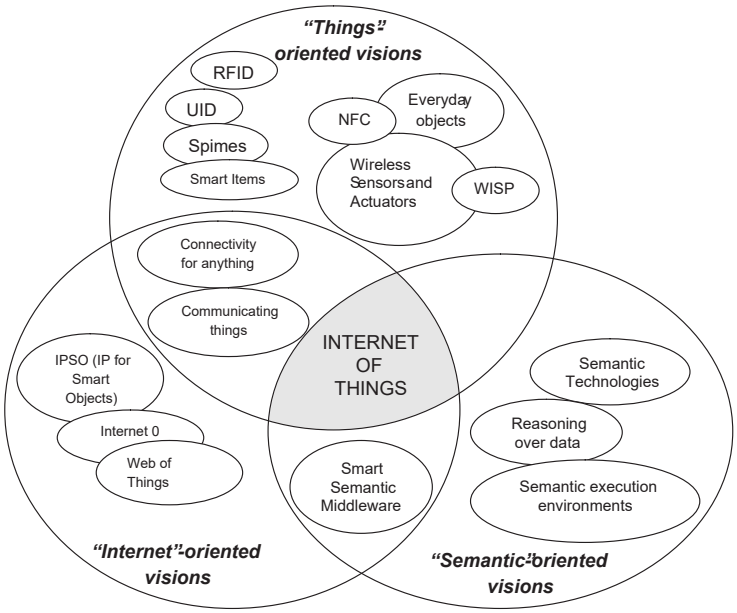

FIG. 2 : L'Internet des objets comme convergence de différentes visions, *[AIM10]*

notion d'hétérogénéité est une caractéristique fondamentale. Les objets n'ont pas nécessairement la même plate-forme matérielle, ni les même fonctionnalités réseaux. Enfin, l'IoT doit pouvoir supporter un très grand nombre de terminaux. IUT-T estime ce nombre à au moins dix fois plus que le nombre de terminaux reliés à Internet en 2012. La recommandation précise des « exigences de niveau ». Ces exigences sont proches de ce qu'offre l'Internet actuel. Comme l'objet peut se connecter à l'IoT, il lui faut un identificateur. Ainsi, il sera possible de le « retrouver » dans le réseau. L'infrastructure doit supporter l'auto-configuration, l'autogestion, l'auto-optimisation et d'autres mécanismes déjà présents dans l'Internet. Cela implique aussi l'interopérabilité des équipements. Bien sûr, l'IoT doit supporter les mécanismes de sécurité élémentaire : l'authentification, le contrôle d'intégrité, le chiffrement. Enfin IUT-T définit un modèle de références en 4 couches : application, prise en charge des services et application, réseau et dispositif. L'UIT-T n'est pas le seul organisme à avoir proposé une définition de l'Internet des objets, l'article [MBR15] propose un récapitulatif des autres définitions.

2.1.4 Le développement de l'IoT

L'Internet des objets se développe relativement vite. La figure 3 montre les perspectives de croissance de l'Internet des objets. En 2011, Cisco estimait que le nombre d'objets connectés pourrait atteindre les 50 milliards de terminaux en 2020 [Eva11]. De nouvelles études se montrent plus tempérées. L'étude [Lun+14] estimait en 2014 que le nombre de terminaux IoT serait proche des 28 milliards en 2020. L'estimation du nombre de terminaux est déjà relativement compliquée. En 2016, cette estimation se situait entre 6 et 18 milliards de terminaux [Nor16]. L'IoT est dynamisé par certains secteurs d'activité comme celui de l'automobile, des télécommunications et de la santé. À défaut d'y contribuer directement, l'IoT accélère le développement de certaines technologies comme le fog computing [Bon+12].

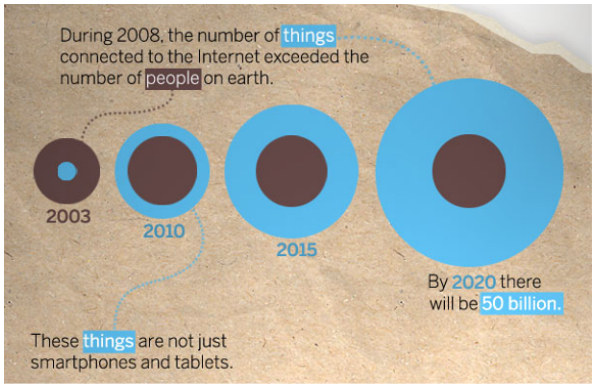

FIG. 3 : La croissance accélérée de l'Internet des objets d'après l'estimation de Cisco en 2011, *[Swa12]*

2.1.5 Domaines d'application

Nous retrouvons l'IoT dans de nombreux domaines. Haller *et al.* [HKS09] estimaient que les secteurs de l'industrie, de l'énergie, de la santé, des transports et des assurances seraient les plus impactés. Nous allons voir quelques domaines qui ont été marqués par l'Internet des objets. Un des premiers secteurs concernés est la domotique. En 2004, dans [GKC04], Gerhesfeld *et al.* utilisent l'exemple de la domotique pour présenter le concept de l'Internet 0. Ils évoquent déjà ce qui sera les ampoules connectées. En domotique, les objets connectés servent surtout pour le contrôle d'énergie. L'objectif est d'économiser de l'énergie en éteignant certains appareils comme les radiateurs par exemple aux moments opportuns [Wan+12]. D'autres fonctionnalités sont focalisées au bien-être comme le contrôle de l'humidité et de la température [Wan+13]. Ils existent d'autres objets connectés aux fonctionnalités moins substantielles comme les réfrigérateurs permettant d'afficher les emplois du temps et la qualité de conservation de la nourriture. Par extension à la domotique, l'IoT est une des briques des bâtiments intelligents. Dans ce domaine, ce sont surtout les capteurs qui sont employés. Ils permettent la détection d'anomalie comme une usure prématurée ou des fuites énergétiques [WL11]. Par exemple, un capteur peut permettre d'envoyer le relevé des compteurs d'eau afin de détecter des fuites. Dans une deuxième extension, il y a les villes intelligentes (*smart cities*) [Zan+14]. Dans ce cadre, l'Internet des objets sert principalement à l'optimisation des ressources (eau, électricité) mais pas exclusivement [Eja+17]. Les capteurs permettent d'obtenir des informations sur la qualité de vie, par exemple comme la qualité de l'air, les nuisances sonores et l'état du trafic routier.

Le domaine médical est intéressé par l'Internet des objets [Isl+15]. Les capteurs présentent un intérêt évident. Ils permettent de surveiller en temps réel différentes métriques physiologiques comme la température, le rythme cardiaque, le taux de glucose [Ist+11 ; GPM15]. À partir de ces relevés, il est possible de détecter des anomalies, lever des alertes. Malgré les avantages indéniables, l'utilisation de l'IoT dans le domaine médical soulève quelques inquiétudes. La confidentialité et le respect de la vie privée peuvent être affectés par la manipulation de données biométriques. L'IoT peut permettre une meilleure gestion des équipements hospitaliers que ce soit des lits ou des fauteuils roulants. D'autres applications sont possibles dans le cadre de la médecine.

2.2 IoT dans l'industrie

L'Internet des objets a un impact dans différents domaines. Par exemple, la voiture autonome est un objet IoT en cours de développement [KH16]. L'industrie subit aussi des mutations liées à

l'IoT dans son fonctionnement. Comme l'industrie a des besoins spécifiques, l'IoT pour l'industrie est nommée Industrial Internet of Things (IIoT). IIoT permet par exemple de détecter les pièces défectueuses, de mesurer la qualité d'un produit en bout de chaîne (détection de défauts). Yang *et al.* [YSW16] recensent quelques applications de l'IoT en milieu industriel. Nous allons en voir quelques-unes.

2.2.1 Gestion de l'énergie

L'IoT apporte des nouvelles perspectives pour l'industrie. La première d'entre elles concerne la gestion de l'énergie. Nous avons vu que l'efficience des ressources est un point important de l'industrie 4.0. L'IoT permet d'avoir une gestion active de l'alimentation des équipements. En 2014, Shrouf *et al.* [SOM14] proposent une approche pour augmenter l'efficience énergétique. L'approche consiste à surveiller et analyser la consommation énergétique en temps réel grâce à des capteurs et des sondes. Puis une fois analysée, les données permettent de définir des stratégies et faire émerger de nouvelles pratiques. Il est ensuite possible de faire une nouvelle itération jusqu'à obtenir une efficience maximale. Dans le même esprit, Wang *et al.* [Wan+16a] proposent d'augmenter l'efficience énergétique de l'Internet des objets industriel. Ils proposent une architecture pour gagner en efficience. L'idée est d'organiser les moments d'activités et de veilles de façon à ce qu'ils deviennent prédictibles. Les gains en efficience énergétique sont importants. Le passage à l'échelle permet de réaliser des économies non négligeables. Néanmoins, il n'est pas précisé si des dégradations des performances sont apparues.

2.2.2 Maintenances préventives

Nous avons vu qu'il était possible de régler le problème de l'efficience énergétique. Un autre point de l'industrie 4.0 est de limiter les temps morts. La maintenance préventive est une solution. Néanmoins, il faut qu'elle soit faite au moment opportun. En 2012, Xu *et al.* [XCM12] proposent d'utiliser l'Internet des objets pour faire de la prédiction de pannes. Les données sont acquises via des capteurs ou par les systèmes cyber-physiques eux-mêmes. Pour effectuer la prédiction, les articles [Wan+17] et [Lee+15] proposent d'utiliser les outils du *Big Data*. Ces outils sont spécialisés dans le traitement de grands volumes de données, ils ont donc de bonnes performances. Wan *et al.* [Wan+17] obtiennent de meilleures prédictions avec leur solution qu'avec les estimations empiriques traditionnelles.

2.2.3 Automatisation

L'Internet des objets permet de répondre à un besoin particulier de l'industrie : l'automatisation. Dans l'industrie 4.0, la flexibilité est un point clé. Pour cela, il faut que les lignes de production soient reconfigurables. Les robots qui composent ces lignes doivent pouvoir supporter des mises à jour de leur programme de fonctionnement. Cet ajout d'intelligence a été rendu possible grâce à l'Internet des objets. Les machines issues du couplage de la robotique et de l'IoT font parties des systèmes cyber-physiques [Jaz14]. Ces systèmes ont besoins d'être connectés aux réseaux. Le « monde des réseaux » fait donc face à de nouveaux défis technologiques à relever [WSJ17].

3 Réseaux de communication

Historiquement, les réseaux industriels sont composés d'éléments câblés. Les technologies comme Ethernet et RS232 sont éprouvés par des années d'utilisation. Néanmoins, l'utilisation de câbles implique la faible mobilité des éléments connectés et un coût de déploiement potentiellement élevé.

Cependant, cette mobilité réduite commence à devenir problématique au commencement de l'ère de l'industrie 4.0 [VT14]. Nous allons commencer par voir les technologies câblées car ce sont des technologies « historiquement » présentes. Ensuite, nous verrons différentes technologies sans-fil susceptibles de remplacer les réseaux industriels câblés. Nous ne pouvons pas être exhaustifs, car il existe un très grand nombre de technologies [WSJ17 ; Zur15]. La figure 4 illustre cette diversité.

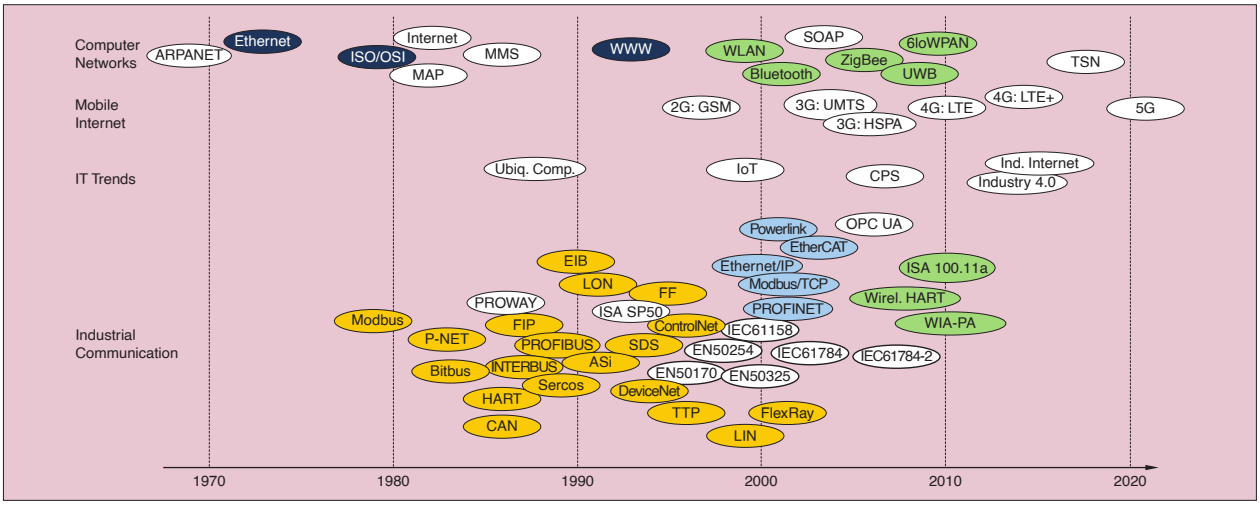

Fig. 4 : Les normes des réseaux industriels, [WSJ17]

3.1 Réseaux câblés

Depuis l'invention du télégraphe, le câble est utilisé pour envoyer une information d'un point à un autre sous forme de signaux électriques. Les réseaux câblés sont historiquement très présents, surtout en entreprises. Les réseaux câblés ont la réputation d'être fiables, robustes, sûrs et performants. Même si les réseaux câblés ont quelques inconvénients comme les contraintes de déploiement ou la très faible mobilité des éléments connectés, leur remplacement total n'est pas envisageable pour le moment. En termes de débit et de fiabilité, les réseaux câblés sont encore plus performants que les réseaux sans fil. Autre élément, comme ils sont historiquement présents, il serait très coûteux de vouloir les remplacer tous. Historiquement, ce sont la boucle de courant et RS-232 qui assuraient la communication entre un contrôleur et un actionneur ou un capteur. Ces solutions ne sont pas parfaites. Elles imposent des restrictions concernant la topologie par exemple. Pour résoudre ces problèmes, des alternatives ont été développées. Comme elles sont orientées industries, elles sont appelées « bus de terrain ». Nous pouvons citer par exemple l'initiative française FIP (Factory Instrumentation Protocol) et allemande PROFIBUS. La standardisation des bus de terrain s'est révélée assez problématique [FS02]. La version initiale de l'IEC 61158 regroupe donc 8 technologies différentes. La version amendée de 2008 compte finalement 16 technologies [Dec09]. Il existe donc une grande quantité de solutions, l'article [Fel05] et l'ouvrage conséquent [Zur15] en dénombrent et en détaillent une partie. Nous allons en voir quelques-unes choisies soit pour leur aspect historique, soit pour leur utilisation.

3.1.1 Couche physique

Nous allons voir quelques technologies définissant au moins la couche physique.

Boucle de courant La boucle de courant est une méthode de communication analogique. Le principe de fonctionnement est simple, il consiste à faire circuler un courant électrique dans une paire de conducteur. La valeur de l'intensité correspond à la valeur à transmettre. Comme la boucle de courant utilise une intensité historiquement comprise entre 4 et 20 mA, la boucle de courant peut être appelée « 4-20mA ». Il est possible de détecter une coupure dès que l'intensité est nulle. Cette technique est principalement utilisée avec des capteurs ou des actionneurs. La boucle de courant tend à être complétée par HART [How94] ou à être remplacée par des bus de terrain et Ethernet.

RS-232 RS-232 (ou EIA 232) est une norme de communication de type série. Cette norme a été validée par l'EIA en 1962. TIA/EIA-232-F est la dernière révision parue en 1997. Elle permet un échange asynchrone et bidirectionnel entre deux équipements (point à point). La norme définit seulement le fonctionnement électrique de la connexion, le brochage et le connecteur. Les codages et le débit de transmission ne sont donc pas définis dans la norme. Par ses spécifications, RS-232 est donc une norme de couche physique dans la pile OSI. Par exemple, Il est donc possible d'utiliser PPP et IP sur RS-232. Dans son livre *PC 97 Hardware Design Guide* [Cor97], Microsoft déprécie l'utilisation de la norme RS-232 au profit de norme comme USB. En pratique, UART (*Universal Asynchronous Receiver Transmitter*) est généralement utilisé sur RS-232. RS-232 peut atteindre un débit maximal de 115200 bit/s sur des très courtes distances.

RS-485 RS-485 (ou TIA/EIA 485) est une amélioration significative de TIA/EIA 422. TIA/EIA 422 est une extension de RS-232. Comme pour RS-232, la norme ne définit que le niveau physique, c.-à-d. le fonctionnement électrique, le brochage et le connecteur. RS-485 supporte le point à point ainsi que le multipoint. Il est donc possible d'avoir une topologie de type bus via RS-485. Les connexions peuvent aussi être établies en « full duplex ». En pratique, RS-485 peut atteindre un débit maximal de 10 Mbit/s sur de très courtes distances ou une distance de 1200 m avec un débit moindre [Max06].

USB USB (Universal Serial Bus) est un standard industriel créé en 1996. Il spécifie entièrement la couche physique, liaison et transaction. USB est né de l'encombrement, de la lenteur et de la multitude de ports séries incompatibles entre eux. USB permet à la fois de communiquer et d'alimenter électriquement un périphérique. Les différentes versions sont rétro-compatibles sous certaines conditions. En effet, le connecteur a évolué, il existe 3 types de connecteur (A, B et C). Les types A et B peuvent être déclinés en plusieurs formats (standard, mini et micro). Le connecteur type C est uniquement disponible au format « full duplex ». Pour des raisons de simplicité, USB fonctionne uniquement en mode maître-esclaves. Chaque périphérique a une adresse dépendante du constructeur. Dans le standard USB, les données transitent des paquets appelés *USB Requests Blocks* (URB). USB 3.2 possède un débit maximal de 20 Gbit/s. Comme USB possède des éléments pour devenir un protocole réseau, un brevet [BJK05] a été déposé pour permettre son utilisation dans le cadre d'un réseau pair-à-pair. Il serait théoriquement possible de mettre en place ce réseau pair-à-pair grâce à des câbles de pont USB-USB et hub USB. Il existe deux protocoles de transactions définis pour organiser les échanges de données. Le premier historiquement est *Bulk-Only Transport* (BOT). L'inconvénient de BOT est qu'il ne permet l'envoi que d'une commande à la fois. Le périphérique ne peut pas optimiser le séquencement des commandes, ce qui entraîne de possibles détériorations des performances. Pour pallier ce problème, l'USB Attached SCSI Protocol (UASP ou UAS) fut créé [Yu+11 ; Kau+15]. Il s'inspire de la gestion des commandes des disques durs SCSI. L'UASP permet l'envoi groupé de commandes pour laisser au périphérique le choix du séquencement des commandes.

FireWire FireWire est une technologie développée dans le début des années 1990 par Apple. FireWire a été standardisé par l'IEEE sous la norme IEEE 1394. Elle spécifie entièrement la couche physique, liaison et transaction. FireWire permet de communiquer et d'alimenter électriquement un périphérique. Les premières implémentations sont sorties en 1994. Elles pouvaient atteindre 100 Mbit/s en théorie sur une distance de 4,5 m typiquement [HM95]. La dernière révision de la norme, publiée en 2008, permet d'obtenir des débits théoriques de 3,2 Gbit/s. Deux connecteurs distincts et non compatibles sont définis (FireWire 400 et FireWire 800). De plus, la norme FireWire S800T (IEEE 1394c-2006) permet d'utiliser le même connecteur et les mêmes câbles[2] qu'Ethernet. Concernant la couche liaison, les données transitent sous forme de paquets. Chaque périphérique possède un identifiant unique IEEE EUI-64. IEEE 1394 permet la création de réseaux de type arbre et selon un fonctionnement pair à pair. IEEE 1394 devient une « vraie » norme réseau grâce à la RFC 2734 en 1999, elle définit l'utilisation d'IPv4 sur IEEE 1394 [Joh99]. Des articles comme [RDD99 ; DR00 ; Sch+01] ont montré son potentiel dans le milieu industriel. Bien que comparable à USB et Ethernet dans [RA02], IEEE 1394 n'a pas pu résister face à eux. FireWire est abandonné par Apple en 2008, et définitivement abandonné en 2013 avec le retrait de la proposition IEEE P1394d.

Ethernet Ethernet est un protocole réseau développé par Xerox qui est sorti en 1980 [SH80]. Ethernet a été standardisé par l'IEEE en 1983 sous le nom d'IEEE 802.3. Ethernet définit à la fois la couche physique et la couche liaison. En 1983, la première implémentation standardisée permettait un débit de 10 Mbit/s sur un câble coaxial [Sho+85]. En 1987, la paire cuivrée et la fibre optique furent ajoutées au standard. La dernière révision (802.3bs-2017) permet un débit maximal de 400 Gbit/s. Les premières implémentations ne permettaient que des topologies de type bus. Maintenant, Ethernet supporte les topologies en étoile et point à point. Concernant la partie liaison, les données transitent sous forme de trames. Les terminaux possèdent une adresse sur 48 bits, dépendante du constructeur [DP81]. La figure 5 représente la structure d'une trame Ethernet. Ethernet fonctionnement en mode CSMA/CD, celui-ci inclut un mécanisme de détection de collision. Ce mécanisme est essentiel sur la topologie de type bus, car la topologie bus est favorable aux collisions et Ethernet ne garantit pas la bonne livraison des données [Mol85]. Au fil des années, IEEE 802.3 est devenue le standard prépondérant dans l'univers des réseaux câblés. Une partie des sous-standards IEEE 802.1Q et le sous-standard 802.1AS permettent à Ethernet de supporter complètement le temps réel [IL11 ; CIS17].

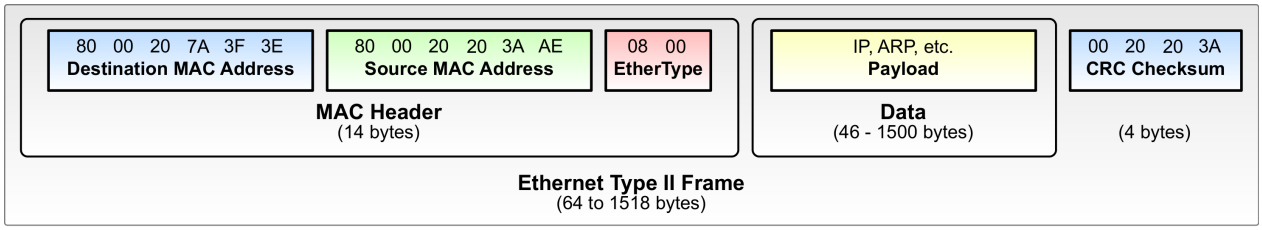

Fig. 5 : Structure d'une trame Ethernet, *[Con18a]*

3.1.2 Couche liaison

Nous avons vu précédemment des technologies définissant au moins la couche physique. Nous allons maintenant voir des technologies définissant la couche liaison.

2. Jusqu'à la catégorie 5e

EtherCAT EtherCAT est un protocole de niveau liaison, standardisé IEC 61158. Il a été développé par Beckhoff Automation en 2003. Il est actuellement supporté par EtherCAT Technology Group. Il s'appuie sur Ethernet pour la couche physique et la partie inférieure de la couche liaison. EtherCAT supporte les topologies de type étoile, bus et anneau [KDI10]. Il fonctionne en maître-esclaves. Le nœud nécessite seulement un système avec support temps réel et un port Ethernet. EtherCAT utilise des trames Ethernet « conformes », ce qui permet en théorie d'utiliser n'importe quels câbles et cartes réseaux compatibles avec Ethernet. En pratique, des puces FPGA et ASIC sont utilisées pour accélérer le traitement des trames sur les nœuds esclaves [Pry08]. EtherCAT utilise des paquets appelés télégrammes. Le télégramme est constitué de l'entête EtherCAT et des données (datagrammes). Il est ensuite inséré dans les trames Ethernet comme charge utile. Il est aussi possible d'encapsuler les télégrammes dans des paquets UDP [Fel05]. La figure 6 illustre la structure d'un télégramme dans une trame Ethernet. Concernant les performances, EtherCAT uti-

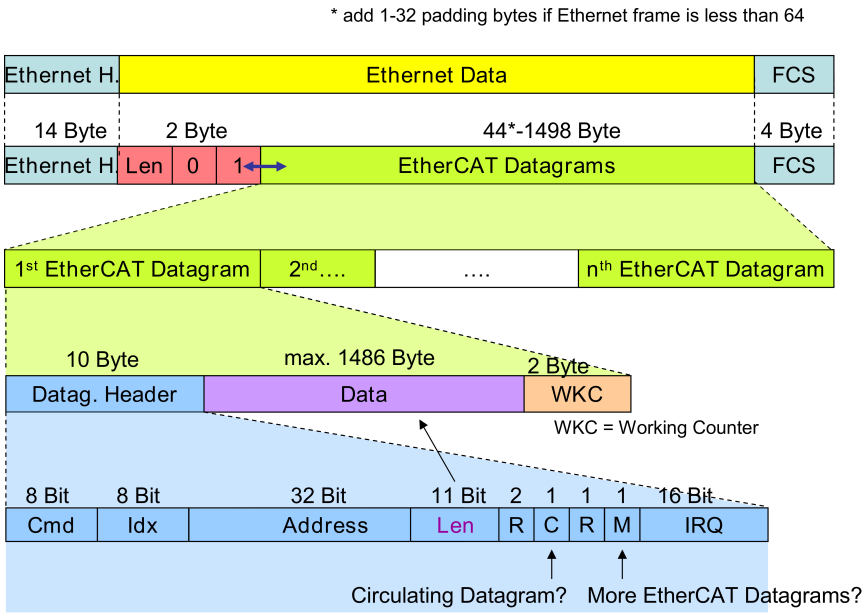

FIG. 6 : Structure d'une trame Ethernet contenant un télégramme EtherCAT, extrait d'ethercat.org

lise au mieux Fast Ethernet. Il n'utilise donc pas pleinement les liaisons Ethernet Gigabit. D'après l'article [JB04], la technologie EtherCAT serait indépendante du medium de transmission. Cette idée d'indépendance du médium est renforcée par Wu et Xie [WX17]. Ils proposent une extension d'EtherCAT pour les réseaux sans-fil IEEE 802.11 et IEEE 802.15.4. La majorité des comparatifs de performances sont purement théoriques p. ex. [Pry08] et [KDI10]. Concrètement, elle utilise uniquement les spécifications pour évaluer les performances. Les seules études comparatives pratiques ont été réalisées par EtherCAT Technology Group.

Sercos Sercos est un protocole de niveau liaison crée par VDW/ZVEI Joint Committee en 1987, standardisé IEC61784/61158/61800. Il est actuellement maintenu par Sercos International e.V., basé en Allemagne. Sercos fonctionne en mode temps réel isochrone. Les équipements peuvent communiquer en fonction de cycles d'horloge. L'isochronisme implique que les cycles ont une durée strictement identique. La dernière version est la version 3, sortie en 2003 [Sch04]. Les deux premières versions définissaient aussi la couche physique. La version 3 repose sur Ethernet pour la couche physique et la « partie inférieure » de la couche liaison. Sercos III supporte les topologies de type bus et anneau. Il fonctionne en mode maître-esclaves. Sercos III utilise des trames Ethernet

« conformes », ce qui permet en théorie d'utiliser n'importe quels câbles et cartes réseaux compatibles avec Ethernet. Des puces FPGA sont recommandées pour accélérer le traitement des trames sur les nœuds esclaves. Sercos III utilise des paquets appelés télégrammes. Le télégramme est constitué de l'entête Sercos et des données. Il est ensuite inséré dans les trames Ethernet comme charge utile. La figure 7 illustre l'intégration d'un télégramme dans une trame Ethernet. Concernant les performances, Sercos III utilise uniquement Fast Ethernet. Aucune étude comparative récente n'a été trouvée.

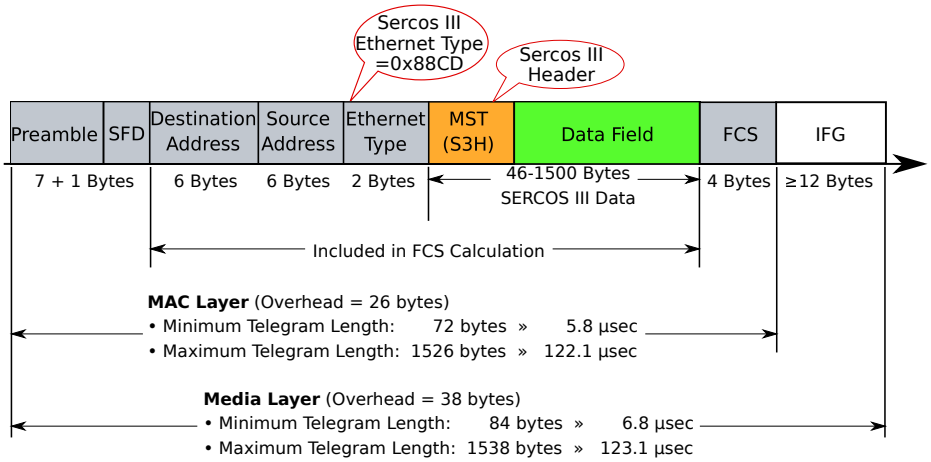

FIG. 7 : Structure d'une trame Ethernet contenant un télégramme Sercos III, *[Con18b]*

3.1.3 Couches applicatives

EtherNet/IP EtherNet/IP est un protocole de niveau applicatif (couches 5 à 7), créé par Rockwell Automation en 2001 [Bro01b]. EtherNet/IP désigne l'implémentation de Common Industrial Protocol (CIP) sur Ethernet et IP. En 2008, des tests ont été effectués pour mettre en œuvre EtherNet/IP sur un réseau hybride Ethernet et IEEE 802.11 [CVV08]. CIP utilise TCP et UDP en fonction du besoin. EtherNet/IP et CIP sont maintenus par ODVA, Inc. (anciennement Open DeviceNet Vendors Association). ODVA est une organisation responsable des marques et des spécifications de CIP, EtherNet/IP, DeviceNet, ControlNet et CompoNet. ODVA est basé aux Etats-Unis. Peu d'informations existent sur EtherNet/IP. Bien que les spécifications soient disponibles sur le site de l'ODVA, les articles trouvés ([Sch01] et [Bro01b]) sont anciens et rédigés par des employés Rockwell. À notre connaissance, il n'existe pas de comparatifs de performance.

3.1.4 Conclusion

Nous avons vu quelques technologies des réseaux câblés pouvant être présentes dans l'industrie. Nous les avons regroupés par « premier niveau de fonctionnalité » défini par la norme ou le standard. Certains comme RS-232 sont présentés à titre historique, d'autres comme Ethernet sont de plus en plus utilisés. Le tableau 1 récapitule brièvement les encapsulations protocolaires possibles. Une tendance se dessine depuis les années 2000. Les nouvelles technologies câblées pour les réseaux industriels ont adopté Ethernet comme élément de base. En effet, que ce soit Sercos, POWERLINK, PROFINET ou EtherCAT, ils ont tous choisi d'utiliser Ethernet. Le support du temps réel pour Ethernet montre aussi le rapprochement entre les technologies informatiques (IT) et les technologies opérationnelles (OT) .

Norme	Physique	Liaison	Réseau	Transport	Application
Boucle de courant	Boucle de courant	HART*			HART*
RS-232	RS-232	indépendant	indépendant	indépendant	indépendant
RS-485	RS-485	indépendant	indépendant	indépendant	indépendant
USB	USB	USB	indépendant	indépendant	indépendant
FireWire	FireWire Ethernet	FireWire	indépendant	indépendant	indépendant
Ethernet	Ethernet	Ethernet	indépendant	indépendant	indépendant
EtherCAT	Ethernet	EtherCAT	indépendant*	indépendant*	indépendant*
Sercos III	Ethernet	Sercos III	indépendant	indépendant	indépendant
EtherNet/IP	Ethernet	Ethernet	IP	UDP/TCP	CIP
PROFINET	IEEE 802.x	IEEE 802.x	IP	TCP/UDP	indépendant
PROFINET (NRT)	Ethernet	Ethernet	IP	UDP	RPC+PROFINET
PROFINET (RT)	Ethernet	Ethernet			PROFINET
PROFINET (IRT)	Ethernet	Ethernet modifié			PROFINET

Tab. 1 : Tableau récapitulatif des technologies réseaux câblés. L'indépendance est vis à vis de la norme. La marque « * » signifie que des conditions particulières s'appliquent.

3.2 Wireless Personal Area Network

Nous avons vu les réseaux câblés dans la sous partie précédente. Nous allons regarder différentes technologies réseaux sans-fil. Nous les avons regroupés en fonction de leur portée. Nous commencerons par les réseaux à faible portée (inférieur à 100 m). Ces réseaux ont des débits relativement faibles. Pour les technologies sans-fil, seules les bandes de fréquences utilisables en Europe sont indiquées. Par exemple, la bande de fréquences Industriel, Scientifique et Médical (ISM) 915 MHz n'est disponible qu'aux États-Unis. Son « équivalent » européen est la bande de fréquences ISM 868 MHz.

3.2.1 RFID

RFID (ou Radio Frequency IDentification) est une méthode de stockage de données et de communication sans fil. Un système RFID se compose à minima d'un lecteur et d'une radio-étiquette (ou tag RFID). Cette radio-étiquette est généralement composée d'une puce et d'une antenne. La communication s'effectue par ondes électromagnétiques (ondes magnétiques et micro-ondes). RFID utilise un ensemble de bandes de fréquences (125 kHz, 13,56 MHz, 433 MHz, 865-868 MHz, 2,45-5,8 GHz et 3,1-10 GHz). La portée de la RFID est assez variable en fonction de la bande de fréquences. Cela est lié à la puissance de transmission autorisée pour chaque gamme de fréquences. Par exemple, la norme RFID sur la bande de fréquences 125 kHz permet une distance de 10 cm. Tandis que la bande de fréquences 433 MHz permet une distance maximale de 100 m. Le débit disponible augmente en fonction de la fréquence. La RFID supporte 3 types de fonctionnements : actif, semi-actif et passif. En mode passif, le tag utilise l'énergie de l'onde émis par le lecteur comme alimentation. Il n'utilise pas de batteries. Les tags semi-actifs utilisent l'énergie de l'onde émis par le lecteur uniquement pour générer la réponse à la requête du lecteur. La puce est alimentée par une alimentation auxiliaire. Enfin, les tags actifs fonctionnent uniquement grâce à une source d'énergie auxiliaire. Les tags actifs offrent une meilleure portée ainsi qu'une plus grande capacité de mémoire. RFID est composée dans un ensemble de normes. La figure 8 montre quelques-unes de ces normes ainsi que leur utilisation. Par exemple, la norme ISO/IEC 14443 sert de support pour la technologie NFC (Near Field Communication). EAS signifie *Electronic Article Surveillance*. Concrètement, il s'agit des antivols présents en magasin. Ils sont généralement de petites tailles.

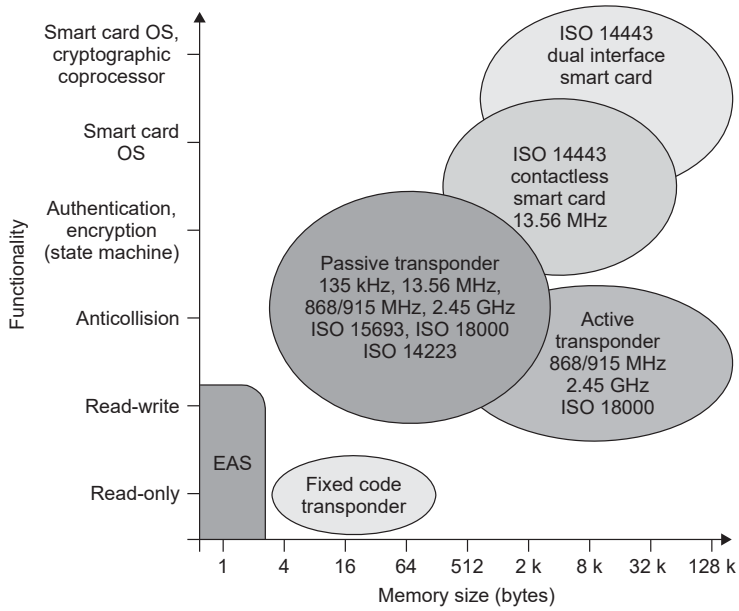

FIG. 8 : Technologies RFID : fonctionnalités en fonction de la capacité mémoire, *[FM10]*.

Le concept de communication par RFID est apparu en 1948 [Lan05]. Il faut attendre les années 1960 pour avoir les premières implémentations matérielles. Ces implémentations ne contenaient qu'un bit de mémoire. Concrètement, les systèmes détectaient la présence ou l'absence du tag. La figure 9 montre l'évolution des tags, que ce soit en termes de surface que de mémoire. Le tag de 1999 occupe une surface très réduite. Le reste est dédié à l'antenne.

Bien que les technologies RFID semblent pratiques, elles ne sont pas exemptes de problèmes de sécurité. Une de ces faiblesses concerne l'attaque par relais [IH11]. Le scénario nécessite un terminal bancaire compatible NFC, une carte bancaire compatible NFC ainsi que deux smartphones. Les deux smartphones sont reliés par un tunnel. Il est possible de faire transiter les communications NFC de la carte bancaire jusqu'au terminal de paiement par les deux smartphones. Les smartphones récupérèrent les données de la communication. D'autres faiblesses ont pu être identifiées. Il existe la possibilité de rejeu, de déni de service, d'usurpation, de clonage, d'écoute... [Hey+07 ; Fin09].

3.2.2 Z-Wave

Z-Wave est un protocole réseau sans-fil développé par Zensys, en 2001. Zensys est une société danoise. Elle a été rachetée par la société américaine Sigma Designs en 2008. Z-Wave est une technologie propriétaire. L'implémentation des couches physique et liaison est néanmoins conforme à la recommandation ITU-T G.9959. Ce protocole a été développé principalement pour une application domotique. Z-Wave fonctionne sur les bandes de fréquences 868 MHz et 2,4 GHz [MPV11]. Le débit peut atteindre 200 kbit/s. La portée est de 30 m en intérieur et 100 m en extérieur [GP10]. La dernière révision majeure s'appelle Z-Wave+. Elle est entièrement rétrocompatible avec Z-Wave. Malgré les éléments de sécurité apportés à Z-Wave+, il existe une faiblesse dans le protocole Z-Wave. Comme le montre Rouch *et al.* [ROU+17], il est possible de prendre le contrôle d'un réseau Z-Wave avec un équipement abordable (moins de 100€).

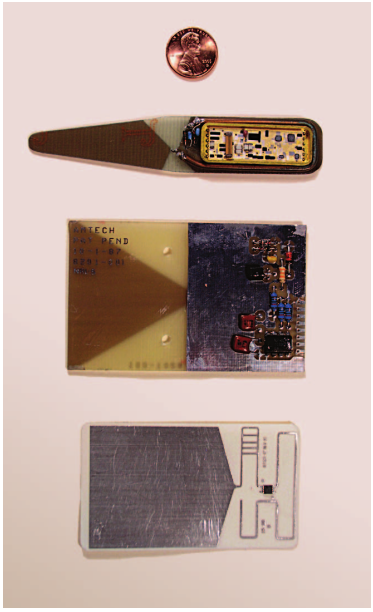

FIG. 9 : Evolution des tags RFID, de haut en bas : un tag en lecture seule 12 bits, 1976 ; un tag en lecture seule de 128 bits, 1987 ; un tag en lecture écriture de 1024 bits, 1999. *[Lan05]*

3.2.3 IEEE 802.15.4

IEEE 802.15.4 est un protocole de communication sans-fil standardisé par IEEE en 2003 [IEE03]. Nous ne considèrerons pas les amendements g [IEE+12], k [IEE+13] et leurs dérivés dans cette partie. Avec des portées de l'ordre du kilomètre, ils s'apparentent aux technologies à faible consommation et à grande portée (LWPAN) et sont donc distincts des technologies WPAN. Le standard IEEE 802.15.4 définit la couche physique et liaison. ZigBee est à l'origine de la norme IEEE 802.15.4 [Bak05]. IEEE 802.15.4 fonctionne sur les bandes de fréquences ISM 868 MHz et 2,4 GHz. La portée maximale est de 100 m. Le débit maximal est de 250 kbit/s. Il dépend de la technique d'étalement du spectre. IEEE 802.15.4 dispose de deux systèmes d'adressage différents. Le premier système est statique, il utilise des adresses type EUI64, donc sur 64 bits. Un système d'adressage dynamique est disponible. Les adresses sont sur 32 bits. La figure 10 illustre la structure d'une trame.

IEEE 802.15.4 définit plusieurs modes d'accès. Le premier est opportuniste avec évitement de collision (CSMA/CA). Alternativement, il peut aussi utiliser des balises de synchronisation. Il dispose aussi d'un créneau de communication garantie [KAT06]. Dans ce cas, le mode d'accès s'apparente au TDMA. En 2012, l'amendement IEEE 802.15.4e apporte des améliorations à la couche liaison [DAS14]. Il apporte notamment le mode TSCH (*Time Slotted Channel Hopping*). Il s'agit d'un fonctionnement proche du TDMA couplé à du multi-canaux et du saut de fréquences. Avec ce mode de fonctionnement, IEEE 802.15.4 se rapproche des normes pour les réseaux industriels WIA-PA, ISA100.11a et WirelessHART. Les ajouts d'IEEE 802.15.4e en fait un standard compatible avec les attentes d'un réseau industriel.

Il est possible d'utiliser IPv6 sur IEEE 802.15.4. Néanmoins, il est nécessaire d'apporter une couche d'adaptation. Cette couche d'adaptation s'appelle 6LoWPAN pour *IPv6 over Low-Power Wireless Personal Area Networks*. 6LoWPAN est un standard IETF issu de la RFC 4944 [Mon+07]. IPv6 n'est pas encore disponible pour le mode TSCH (*charter-ietf-6tisch-02*). IEEE 802.15.4-2003 possède quelques faiblesses de sécurité. Xiao *et al.* [Xia+05] citent 3 faiblesses de sécurité. Par

exemple, une attaque concerne la protection contre le rejeu. Une autre utilise l'absence de contrôle d'intégrité des trames *ACK*.

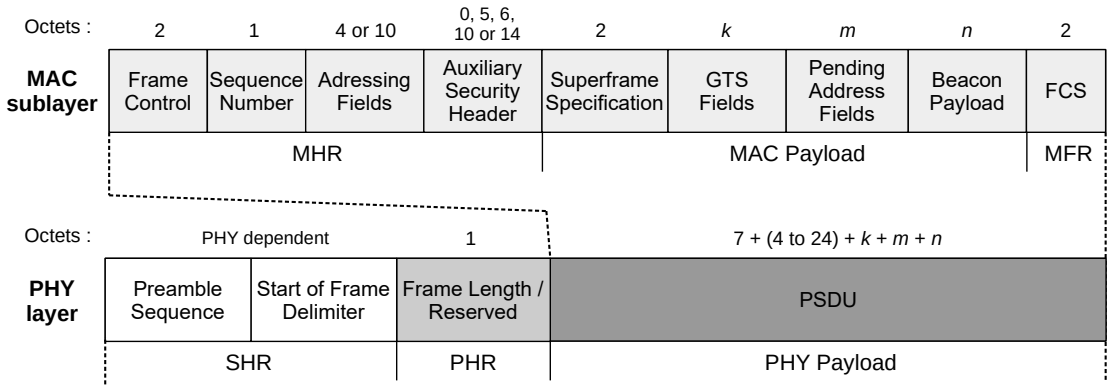

Fig. 10 : Structure d'une trame IEEE 802.15.4, *Extrait du cours ECEN 4242 (version 2011) du Pr. Liu de l'Université du Colorado*

IEEE 802.15.4 est repris partiellement par d'autres technologies. On peut citer WIA-PA, ISA100.11a et WirelessHART. Ces technologies n'utilisent généralement que la bande de fréquences ISM 2,4 GHz, les autres bandes de fréquences n'étant pas disponibles dans tous les pays. Nous allons détailler un peu plus les technologies utilisant IEEE 802.15.4.

WIA-PA WIA-PA (ou Wireless Networks for Industrial Automation–Process Automation) est un protocole réseau sans-fil. WIA-PA a été développé par la Chinese Industrial Wireless Alliance (CIWA) [Lia+11]. WIA-PA a été approuvé en 2007 par la CIWA. Il faut attendre 2011 pour que l'IEC le standardise sous la norme IEC 62601. WIA-PA s'appuie sur la couche physique et la partie « inférieure » (MAC) du standard IEEE. Concrètement, il reprend la couche physique, le système d'adressage et la structure des trames. WIA-PA étend certaines fonctionnalités d'IEEE 802.15.4, notamment les super-trames. Il ajoute aussi un mécanisme de saut de fréquences [Lia+13]. WIA-PA définit aussi la couche réseau et application. L'adresse de niveau réseau n'est constituée que de 16 bits. Le format de l'adresse est de type X.Y où X et Y sont compris entre 0 et 255. La couche réseau supporte l'agrégation des paquets et des données.

ISA100.11a ISA100.11a est une pile technologique réseau sans-fil développée par l'International Society of Automation (ISA) en 2009. En 2010, il a été standardisé par l'IEC sous le nom d'IEC 62734. ISA100.11a s'appuie sur la couche physique et la partie « inférieure » (MAC) de la couche liaison d'IEEE 802.15.4 [PC11]. ISA100.11a définit le reste de la couche liaison, la couche réseau, transport et application. Comme WIA-PA, ISA100.11a ajoute le saut de fréquences [Car08]. Il est possible d'utiliser TDMA pour maximiser l'utilisation du média. La couche réseau est assurée par IPv6 et sa couche d'adaptation 6LoWPAN. Cela permet de rendre le routage possible vers l'extérieur du réseau ISA100.11a. Néanmoins, pour des raisons d'efficience, les adresses IP sont sur 16 bits à l'intérieur du réseau ISA100.11a. Le format d'adresse IPv6 « standard » reste disponible si besoin. La couche transport utilise UDP avec des extensions [PC11 ; NR12]. La couche applicative utilise EDDL (*Electronic Device Description Language*, IEC 61804). Ce langage de description est utilisé par d'autres technologies comme HART et Foundation Fieldbus [Car08].

WirelessHART WirelessHART est une pile technologique réseau sans-fil développée par HART Communications Foundation et publiée en 2007 [Kim+08]. WirelessHART est standardisé IEC

62591 en 2010. WirelessHART reprend la couche physique d'IEEE 802.15.4 ainsi que la partie « inférieure » (MAC) de la couche liaison. Il définit le reste de la couche liaison, la couche réseau, transport et application. Afin d'avoir un comportement plus déterministe, WirelessHART utilise uniquement TDMA à la place de CSMA [CNM10]. Il ajoute aussi le support pour le saut de fréquences. La couche transport utilise UDP et TCP en fonction du besoin. Pour la couche application, WirelessHART reprend simplement HART.

ZigBee ZigBee (aussi typographié Zigbee) est une pile technologique réseau sans-fil conçue par ZigBee Alliance. ZigBee a été développé en 1998 et finalisé en 2004. ZigBee est à l'origine de la norme IEEE 802.15.4 [Bak05]. La pile est complétée par une couche réseau et application spécifiée dans ZigBee 1.0. ZigBee est principalement destiné à la domotique. Cependant, des révisions ont été apportées afin de rendre ZigBee utilisable dans d'autres secteurs. La plupart des réseaux fonctionnent avec IP. Comme ZigBee ne supporte pas IP dans sa spécification initiale, la communication avec le reste des infrastructures est délicate. Pour remédier à ce problème, deux solutions complémentaires ont été développées : ZigBee Pro et ZigBee IP [Fra+13]. ZigBee Pro permet la communication entre le domaine ZigBee et le domaine IP via une passerelle. ZigBee IP inclut le support natif d'IP pour tous les nœuds. Il permet donc HTTP sur TCP et optionnellement CoAP sur UDP. CoAP (ou Constrained Application Protocol) est un protocole équivalent à HTTP, mais destiné à l'IoT [BCS12]. Pour optimiser l'efficience, il est possible d'utiliser la couche d'adaptation 6LoWPAN. La figure 11 résume l'organisation des piles ZigBee Pro et ZigBee IP. Bien que ZigBee n'utilise que la bande ISM 2,4 GHz, ZigBee Pro et ZigBee IP peuvent aussi utiliser la bande ISM 868 MHz. D'après Vidgren *et al.* [Vid+13], il serait possible de saboter les nœuds terminaux avec ZigBee Pro 2007. Il suffirait de prendre le contrôle ou usurper un nœud maître (p. ex. *Zigbee Router* et *Zigbee Coordinator*) puis d'empêcher la mise en veille des nœuds esclaves. Une autre faiblesse réside dans l'envoi de la clé réseau. Si la clé réseau n'est pas pré-installé, elle est envoyée en clair. Il suffirait de pratiquer une écoute pour récupérer la clé réseau puis compromettre le réseau.

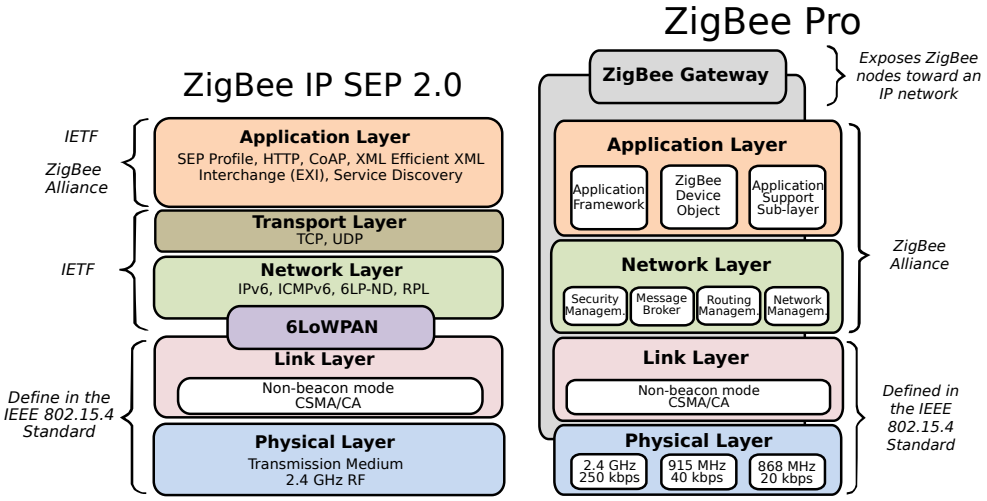

FIG. 11 : Piles technologiques ZigBee IP 2006 et ZigBee Pro 2007, *[Fra+13]*

3.2.4 Bluetooth

Bluetooth (BT) est une pile technologique pour les réseaux sans-fil. Bluetooth a été créé par l'entreprise suédoise Ericsson en 1994. Il est maintenant maintenu par Bluetooth Special Interest

Group, un consortium d'entreprises. Les versions 1.1 et 1.2 ont été normalisées sous le nom IEEE 802.15.1 [Bak05]. La standardisation IEEE n'est plus maintenue. La dernière version est la 5, publiée en 2016. Bluetooth utilise la bande de fréquences ISM 2,4 GHz. La portée maximale est de 200 m pour la version 5, et 100 m pour les versions précédentes [Col+18]. Le débit maximal est de 2 Mbit/s en version 5. Bluetooth utilise le saut de fréquences. Comme Bluetooth est assez énergivore, une version plus économe a été créée. Il s'agit de Bluetooth Low Energy (BLE) [GOP12]. Cette déclinaison est principalement destinée à l'IoT. Les performances sont plus modestes mais cela permet une durée de vie accrue. D'autres fonctionnalités comme le mode TDMA ont été ajoutées à BLE. Les adresses Bluetooth sont sur 48 bits avec une partie dépendante du constructeur, comme Ethernet. Bluetooth a connu plusieurs faiblesses de sécurité. En 2001, Jakobsson et Wetzel [JW01] proposent une première étude des faiblesses de BT 1.0B. La longueur du code PIN, la possibilité d'écoute passive et l'algorithme de chiffrement sont des faiblesses mises en avant. Certains virus utilisaient les faiblesses de Bluetooth pour se propager sur les téléphones portables [BS06]. D'après [BS06], certaines vulnérabilités proviennent de l'implémentation de la pile Bluetooth. Alors BLE est disponible depuis quelques années, Kwon *et al.* [Kwo+16] montrent qu'il est possible de pratiquer une cryptanalyse sur la clé de chiffrement en 20 secondes. Lonzetta *et al.* [Lon+18] proposent une liste détaillée des vulnérabilités de Bluetooth comme BlueJacking, BlueSnarfing, BlueBugging et récemment BlueBorne.

3.2.5 Conclusion

Nous avons différentes technologies réseaux WPAN. La portée maximale est d'environ 100 m. Leur débit ne dépasse pas les 2 Mbit/s. Leur objectif est avant tout de maximiser la durée de vie des équipements connectés. ZigBee, ISA100.11a, WIA-PA et WirelessHART partage la même couche physique. Il est donc normal que leur portée et leur débit soient identiques. Ce sont les couches supérieures qui les distinguent les uns des autres. Le tableau 2 récapitule brièvement les informations techniques des technologies rencontrées.

Technologie	Bandes de fréquences	Débit max.	Portée max.	Méthode de contrôle d'accès
RFID	125 kHz		10 cm	
	13,56 MHz		1 m	
	433 MHz		100 m	
	868 MHz		10 m	
Z-Wave	868 MHz et 2,4 GHz	200 kbit/s	100 m	CSMA
IEEE 802.15.4	868 MHz et 2,4 GHz	250 kbit/s	100 m	TDMA/CSMA
WIA-PA	2,4 GHz	250 kbit/s	100 m	TDMA+CSMA+FDMA
ISA100.11a	2,4 GHz	250 kbit/s	100 m	TDMA (+CSMA)
WirelessHART	2,4 GHz	250 kbit/s	100 m	TDMA (+CSMA)
Bluetooth 5	2,4 GHz	2 Mbit/s	200 m	CSMA/FDMA
Bluetooth LE	2,4 GHz	1 Mbit/s	100 m	TDMA/FDMA

Tab. 2 : Tableau récapitulatif des technologies WPAN.

3.3 Wireless Local Area Network

Nous avons vu des réseaux à faible portée. Leur portée n'excède pas 100 m. Nous allons nous intéresser aux technologies réseaux intermédiaires. Dans cette catégorie, il n'existe pour le moment

qu'une seule famille, les normes IEEE 802.11. En effet, la norme HiperLAN proposée par ETSI (European Telecommunications Standards Institute) est devenue obsolète.

3.3.1 IEEE 802.11

IEEE 802.11 a été standardisé par l'IEEE en 1997. Wi-Fi définit à la fois la couche physique et la couche liaison [DW93]. Bien que la norme dépende de l'IEEE, le nom Wi-Fi (ou wifi) est une marque déposée en 1999. Il est détenu par Wi-Fi Alliance. La norme initiale (IEEE 802.11-1997) fonctionnait sur la bande de fréquences ISM 2,4 GHz [IL97]. Le débit était de 2 Mbit/s. En pratique, cette norme a été très peu utilisée. La deuxième version d'IEEE 802.11 (IEEE 802.11a) fonctionne sur la bande de fréquences ISM 5 GHz [IEE+99]. Son débit maximum théorique est de 54 Mbit/s, ce qui la rend nettement plus intéressante que la version précédente. Le tableau 3 récapitule les informations essentielles sur les différentes normes IEEE 802.11.

Normes	Année	Bande de fréquences	Débit théorique max. (Mbit/s)	Portée (m)
IEEE 802.11-1997	1997	2.4 GHz	2	100
IEEE 802.11a	1999	5 GHz	54	120
IEEE 802.11b	1999	2,4 GHz	11	140
IEEE 802.11g	2003	2,4 GHz	54	140
IEEE 802.11n	2009	2,4 GHz et 5 GHz	600	250
IEEE 802.11ad	2012	60 GHz	6757	10
IEEE 802.11ac	2013	5 GHz	3466,8	35
IEEE 802.11af	2013	470 MHz-710 MHz	12	qq km
IEEE 802.11ah	2016	868 MHz	8	1000
IEEE 802.11ax	2019 (est.)	2,4 GHz et 5 GHz	NC	NC

Tab. 3 : Tableau récapitulatif des normes 802.11

Au niveau de la couche liaison, IEEE 802.11 est proche d'Ethernet. Les données transitent sous forme de trames. La figure 12 illustre la structure de la trame. Les terminaux possèdent une adresse sur 48 bits, dépendante du constructeur. IEEE 802.11 supporte différentes topologies. La topologie la plus commune est celle en étoile. Le point d'accès est au centre de l'étoile. IEEE 802.11 peut fonctionner au mode ad-hoc. Xu *et al.* [XS01] estiment que la couche liaison n'est pas pour autant optimale. IEEE 802.11 fonctionne en mode CSMA/CA puis une variante à partir IEEE 802.11e [IEE05]. En 2017, Cheng *et al.* [CYZ17] proposent d'utiliser le fonctionnement TDMA au lieu du CSMA/CA. Ce changement rend IEEE 802.11 déterministe à condition de synchroniser les éléments du réseau. Le fonctionnement TDMA permet une amélioration des performances en multi-saut. IEEE 802.11ax utilisera OFDMA au lieu d'une version améliorée de CSMA/CA [Bel16].

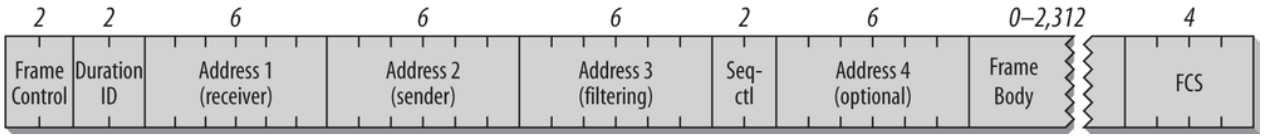

Fig. 12 : Structure d'une trame IEEE 802.11, *[Gas09]*

Wifi et la sécurité Afin de protéger les données échangées sur le réseau, IEEE 802.11 intègre la sécurité Wired Equivalent Privacy (WEP). WEP est disponible depuis la norme initiale de 1997.

WEP utilise un système de clé partagée pour l'authentification. La taille de la clé n'est que de 64 bits (clé de 40 bits + vecteur d'initialisation (IV) de 24 bits), ce qui parait très insuffisant de nos jours. Il peut aussi fonctionner sans authentification. Il utilise RC4 pour le chiffrement du flux de données. L'intégrité est réalisée par contrôle CRC-32. En 2001, Fluhrer, Mantin et Shamir [FMS01] proposent une première cryptanalyse de WEP. Cette attaque consiste en une première phase d'écoute, puis une phase d'attaque sur les trames écoutées. Dans de bonnes conditions, ces deux phases permettent de récupérer la clé partagée en quelques minutes. D'autres faiblesses ont été découvertes. L'augmentation de la taille de la clé à 128 bits (clé de 104 bits + IV de 24 bits) ne permet pas de combler ces faiblesses. WEP a donc été déprécié.

Suite à la publication des premières cryptanalyses de WEP, le protocole de sécurité Wi-Fi Protected Access (WPA) fut publié en 2003. WPA adopte le système d'authentification par clé prépartagé (PSK) et EAP (Extensible Authentication Protocol). WPA intègre TKIP (Temporal Key Integrity Protocol). RC4 est toujours utilisé, par contre la taille de clé est de 128 bits et la taille de l'IV de 48 bits. CRC-32 est remplacé par Michael [Fer02]. TKIP inclut d'autres éléments de sécurité supplémentaires. Malheureusement, comme TKIP reprend la conception de WEP, une première cryptanalyse est publiée en 2008 [TB09]. En 2004, WPA2 remplace WPA. TKIP est remplacé par CCMP, un protocole s'appuyant sur AES. WPA2 n'est pas infaillible [VP17], même si KRACK reste difficile à reproduire. Wi-Fi Alliance a annoncé WPA3 en 2018. Malheureusement, un an plus tard, la vulnérabilité *Dragonblood* a été trouvé dans WPA3 [VR19]. Elle impacte la méthode d'authentification *Dragonfly* et permet à un tiers de récupérer la clé de sécurité.

Le cas de 802.11af et 802.11ah A l'exception d'IEEE 802.11af [Flo+13], Wi-Fi fonctionne uniquement sur les bandes de fréquences non-licenciées ISM (Industriel, Scientifique et Médical). IEEE 802.11af est une norme un peu particulière. Elle fonctionne entre 470 MHz et 710 MHz, c.-à-d. une bande de fréquences réservée à la diffusion télévisuelle. IEEE 802.11af utilise donc la radio cognitive pour récupérer des bandes de fréquences inutilisées. Le débit est dépendant de l'utilisation du spectre. Néanmoins, il ne faut pas espérer des débits supérieurs à 12 Mbit/s [LM12]. Sa portée peut atteindre quelques kilomètres.

IEEE 802.11ah est la norme destinée à l'IoT et aux M2M (machine à machine) [Ada+14 ; Kho+15]. Elle porte le nom commercial de Wi-Fi Halow. Le débit est volontairement plus faible afin d'augmenter la durée de vie des équipements sur batteries. Sa portée permet d'avoir une solution intermédiaire avant les réseaux cellulaires.

3.4 Wireless Wide Area Network

Nous avons vu les réseaux à faible et moyenne portée. Nous allons aborder logiquement les réseaux à longue portée. Dans cette catégorie, nous pouvons distinguer deux grandes familles. La première famille est celle des réseaux cellulaires. La deuxième famille est composée des réseaux à faible débit et longue portée.

3.4.1 Réseaux cellulaires

Nous allons commencer par les réseaux cellulaires. Ces réseaux sont issus de technologies de télécommunication. Ces technologies sont validées par la coopération d'organisme de standardisation 3rd Generation Partnership Project (3GPP). Les réseaux cellulaires sont uniquement présents sur des bandes de fréquences licenciées.

LTE-MTC LTE-MTC (ou LTE-M, parfois eMTC) est une adaptation de la technologie LTE (Long Term Evolution) à destination de l'IoT. La première version est catégorisée LTE-M1 (Release 13). Afin d'augmenter la « durée de vie » des équipements connectés, LTE-M1 fonctionne avec une bande de fréquences de 1,4 MHz. Le débit est réduit en contrepartie. Il peut atteindre les 1 Mbit/s. LTE-M2 (Release 14) utilise une bande de fréquences de 5 MHz. Nous obtenons donc des débits autour des 3 Mbit/s [Lib+18]. LTE-M utilise la bande LTE 900 MHz [PR16]. La portée de LTE-M est supérieure à celle de la LTE « classique », jusqu'à 5 km en zone urbaine et 17 km en zone rurale [Che+17].

Narrowband IoT Narrowband IoT (NB-IoT) est une technologie inclue dans LTE (Long Term Evolution). NB-IoT est catégorisé LTE-NB1 (ou LTE-N1) (Release 13). NB-IoT fonctionne avec une bande de fréquences très réduite, seulement 180 kHz. Les débits ne dépassent pas les 250 kbit/s [Che+17]. La charge utile peut atteindre les 1600 ko [Mek+18]. La version Release 14 permet une légère augmentation des débits [Lib+18]. NB-IoT utilise la bande LTE 900 MHz. La portée de NB-IoT est supérieure à celle de la LTE « classique », jusqu'à 8 km en zone urbaine et 25 km en zone rurale [Che+17]. Mekki et al.[Mek+18] sont moins optimiste, ils proposent une portée maximale de 1 km en zone urbaine et 10 km en zone rurale.

EC-GSM-IoT EC-GSM-IoT (ou EC-GSM) est une extension d'EDGE pour l'IoT. Il est inclus dans la Release 13 de LTE. EC-GSM fonctionne avec une bande de fréquences réduite sur les bandes de fréquences d'EDGE. Les infrastructures des réseaux EDGE sont déjà déployées. De plus, EDGE est une technologie mature. EC-GSM utilise donc EDGE comme base. Quelques ajustements sont apportés afin de le rendre optimal pour l'IoT. L'article [FB18] fournit quelques éléments concernant les apports et changements d'EC-GSM. Pour autant, la portée « fonctionnelle » d'EC-GSM est plus grande que celle d'EDGE.

Conclusion Les réseaux cellulaires présentent de nombreux avantages. Ils sont présents uniquement sur des bandes de fréquences licenciées. Il y a peu de risque d'interférences. Le nombre de messages n'est pas limité. La bande passante disponible dépend uniquement de l'opérateur. Ces technologies utilisent l'infrastructure des réseaux EDGE et LTE déjà déployés. La portée est généralement d'une dizaine de kilomètres. Il y a aussi des inconvénients. Le premier est la dépendance envers un opérateur. En effet, l'infrastructure et le service dépendent de l'opérateur. La durée de vie des équipements sur batteries est souvent plus faible que pour d'autres technologies car les puissances d'émission sont généralement plus élevées.

3.4.2 Low-Power Wide-Area Network

Les réseaux cellulaires ne répondent pas à toutes les attentes. En effet, pour certains capteurs, il n'est pas nécessaire de disposer d'une grande bande passante. De nouveaux types de réseaux sont apparus pour combler ce manque. Ce sont les réseaux à faible consommation et à grande portée c.-à-d. les LPWAN.

LoRa LoRa (**Lo**ng **Ra**nge) est un protocole de communication à faible consommation et grande portée sortie en 2012. Il a été développé par Semtech. Semtech est une entreprise américaine spécialisée dans les semi-conducteurs. Le protocole LoRa dépend maintenant de LoRa Alliance. LoRa s'appuie sur un étalement de spectre type *Chirp spread spectrum* et une modulation brevetée [Hor10]. Une autre modulation peut être utilisée alternativement. Il fonctionne sur deux bandes ISM en dessous de 1 GHz. En Europe, la première s'étend de 868 MHz à 868,6 MHz et la deuxième est centrée

sur 433 MHz. Comme ces largeurs de bande sont étroites, les débits n'excèdent pas 37,5 kbit/s (LoRa) et 50 kbit/s (FSK) en envoi [SWH17]. Mroue *et al.* [Mro+18] proposent une simulation des performances de LoRa en fonction notamment du facteur d'étalement. LoRa peut aussi fonctionner sur la bande de fréquences ISM 2,4 GHz. Le débit maximal est de 200 kbit/s en LoRa et 2 Mbit/s en (G)FSK/MSK. Cette bande de fréquences permettrait d'obtenir des débits plus importants et de s'affranchir du *duty cycle*. Le *duty cycle* est une limite d'utilisation des bandes ISM 433 MHz et 868 MHz. Par exemple, pour la bande 868 MHz, le *duty cycle* impose un temps quotidien d'utilisation de 1 % maximum pour chaque équipement. LoRa a l'avantage d'être bidirectionnel. LoRa fonctionne avec une topologie en étoile. Ochoa *et al.* [Och+17] ont utilisé LoRa sur une topologie de type maillage (*mesh*). Enfin, LoRa peut atteindre une portée de 5 km en zone urbaine et 20 km en zone rurale en fonctionnement à 868 MHz [Mek+18]. Sur la bande ISM 2,4 GHz, la portée maximale estimée serait d'environ 10 km. Des expérimentations ont été réalisées pour apporter le multi-saut et la possibilité pour un nœud d'agir comme relais [Lia+17].

LoRa ne définit que la couche physique. Il faut attendre la publication de LoRaWAN en 2015 pour avoir les spécifications de la couche liaison. Deux systèmes d'adressage fonctionnent en même temps. Le premier système d'adressage utilise des adresses statiques de type EUI-64 donc sur 64 bits. Le deuxième système d'adressage est dynamique. Il utilise des adresses sur 32 bits. Afin de rendre IPv6 plus efficient sur LoRaWAN, des couches d'adaptation ont été créées. La première est 6LoRaWAN, un mécanisme de compression d'entête IPv6 sur LoRaWAN [TBS17 ; Web+16]. 6LoRaWAN n'a pas dépassé l'état de draft [VD16]. *Static Context Header Compression (SCHC) over LoRaWAN* est une autre couche d'adaptation pour IP sur LoRaWAN. Elle est actuellement à l'état de « draft » [Sor+19]. LoRaWAN définit plusieurs classes (A, B, C) [Aug+16]. La classe A est la moins énergivore mais elle est la moins flexible en termes de transmission. La classe B ajoute de la synchronisation. Le point d'accès peut savoir si le terminal est en écoute. De plus, la classe B propose quelques fenêtres de transmission supplémentaires par rapport à la classe A. La classe C est la plus énergivore. Le terminal est en écoute en quasi-permanence. Les classes B et C sont les plus adaptées aux besoins de faible latence. Dans la spécification, LoRaWAN a un fonctionnement proche d'ALOHA [Piy+18]. Piyare *et al.* [Piy+18] proposent un fonctionnement en TDMA sur demande afin d'optimiser les performances et la durée de vie des terminaux. Il est possible de déployer sa propre infrastructure LoRa ou de passer par un opérateur comme Orange ou Bouygues Telecom par exemple.

LoRa et LoRaWAN ne sont pas parfaits. En 2017, deux articles [Lee+17 ; Na+17] ont présenté des scénarios d'attaques contre LoRaWAN. Néanmoins, LoRaWAN supporte nativement le chiffrement (AES 128 bits). Adelantado *et al.* [Ade+17] mettent en avant quelques limitations. La première d'entre elles est le *duty cycle*. Concrètement, plus le réseau LoRaWAN grandira, moins il y aura de bande passante disponible.

Sigfox Sigfox est un protocole de communication à faible consommation et grande portée. La norme semble couvrir la couche physique et liaison [FS18]. Sigfox a été développé par l'entreprise française Sigfox. L'entreprise est aussi opérateur de sa propre technologie car celle-ci est entièrement propriétaire. Sigfox utilise la bande ISM sous les 1 GHz. En Europe, cela correspond à la bande de fréquences 868 MHz-868,6 MHz. Cette bande de fréquences est soumise au *duty cycle*. Le *duty cycle* est une restriction du temps d'utilisation. Concrètement, Sigfox n'a pas le droit d'utiliser cette bande de fréquences plus de 1 % du temps. Sigfox limite donc le nombre de messages quotidiens. La limite est de 140 messages en envoi et 4 en réception pour l'offre la plus complète [NGK16]. Sigfox peut atteindre une portée de 10 km en zone urbaine et 40 km en zone rurale [Mek+18]. Sigfox utilise un étalement de spectre Ultra Narrow Band (UNB). Le réseau a une topologie de type étoile. Comparativement, il existe beaucoup moins d'articles sur Sigfox que sur LoRa.

DASH7 DASH7 (ou DASH7 Alliance Protocol, D7AP) est un protocole de communication à faible consommation et grande portée. D7AP est un standard industriel spécifié par DASH7 Alliance [Wey+15]. Il s'appuie à l'origine sur la norme RFID ISO/IEC 18000-7. Le standard définit 6 couches du modèle OSI. Certains éléments notamment de la couche application sont hérités de la norme ISO/IEC 18000-7. D7AP utilise les bandes de fréquences ISM 433 MHz et 868 MHz. Le débit maximal est de 167 kbit/s. La portée maximale est de seulement 5 km en zone urbaine [RKS17]. DASH7 a la particularité de supporter les topologies de type arbre en plus des topologies en étoile. Le système d'adressage utilise des adresses sur 16 bits (Virtual ID) ou sur 64 bits de type IEEE EUI64 (Unique ID).

Les autres solutions concurrentes Sigfox, LoRa et DASH7 ne sont pas les seules technologies LPWAN. Il en existe d'autres mais elles ne sont pas forcément déployées en Europe. Elles ont toutes des particularités. Par exemple, Ingenu est déployé uniquement aux États-Unis pour le moment. À l'origine Ingenu s'appelait On-Ramp Wireless. Ingenu est développé par Ingenu, basé aux États-Unis. C'est une des rares solutions LPWAN fonctionnant sur la bande de fréquences ISM 2,4 GHz. Sa portée est de 15 km et son débit peut atteindre les 8 kbit/s [Cen+16]. Wize fait partie des dernières technologies LPWAN créées. Wize a été créé en 2017 initialement par GRDF, SUEZ et Sagecom, puis par Wize Alliance. Les cas d'usage de Wize sont liés à la télérelève notamment des compteurs de gaz et d'eau. Sa particularité est d'utiliser la bande ISM 169 MHz.

Conclusion En dehors des technologies issues des réseaux cellulaires, il existe de nombreuses solutions faible débit et longue portée. Le tableau 4 en propose un bref aperçu technique. Elles sont toutes relativement jeunes. Ces technologies ne sont pas toutes ouvertes. Certaines nécessitent de passer par un opérateur. Dans ce cas, le déploiement dépend des opérateurs. Nous n'avons pas évalué le coût de chaque technologie. Par exemple, le prix des puces LoRa est différent de celui des puces Sigfox. D'après Chen et al. [Che+17], le prix du module LoRa est inférieur à 5$, celui d'un module Sigfox serait proche des 10$. Autre point, la bande passante et le nombre de messages disponibles quotidiennement n'ont pas été détaillés.

Technologie	Bande de fréquences	Débit théorique max.		Portée		Charge utile
		Envoi	Réception	Zone urbaine	Zone rurale	
IEEE 802.15.4k	Diverses ISM	125 kbit/s		5 km		2047 o
IEEE 802.15.4g	Diverses ISM	800 kbit/s		quelques km		2047 o
DASH7	433 MHz et 868 MHz	166 kbit/s		5 km		256 o
LoRa	433 MHz et 868 MHz	50 kbit/s		5 km	20 km	jusqu'à 222 o
Sigfox	868 MHz	100 bit/s	600 bit/s	10 km	40 km	12 o (UL), 8 o (DL)
Ingenu	2,4 GHz	78 kbit/s	19,5 kbit/s	15 km		10 ko
Weightless N	470 MHz-790 MHz	0,5 Mbit/s	10 Mbit/s	5 km		jusqu'à 20 o

Tab. 4 : Tableau récapitulatif des solutions LPWAN, synthèse de [RKS17 ; GHI15 ; Xio+15 ; Cen+16 ; Xu+16 ; San+16]

Bibliographie

[Ada+14] T. Adame et al. « IEEE 802.11AH : the WiFi approach for M2M communications ». In : *IEEE Wireless Communications* 21.6 (déc. 2014), p. 144-152. ISSN : 1536-1284. DOI : 10.1109/MWC.2014.7000982 (cf. p. 24).

[Ade+17] F. Adelantado et al. « Understanding the Limits of LoRaWAN ». In : *IEEE Communications Magazine* 55.9 (sept. 2017), p. 34-40. ISSN : 0163-6804. DOI : 10.1109/MCOM.2017.1600613 (cf. p. 26).

[AIM10] Luigi Atzori, Antonio Iera et Giacomo Morabito. « The Internet of Things : A survey ». In : *Computer Networks* 54.15 (28 oct. 2010), p. 2787-2805. ISSN : 1389-1286. DOI : 10.1016/j.comnet.2010.05.010. URL : http://www.sciencedirect.com/science/article/pii/S1389128610001568 (visité le 05/12/2018) (cf. p. 9).

[Alm16] Francisco Almada-Lobo. « The Industry 4.0 revolution and the future of Manufacturing Execution Systems (MES) ». In : *Journal of Innovation Management* 3.4 (24 jan. 2016), p. 16-21. ISSN : 2183-0606. URL : https://journalengineering.fe.up.pt/index.php/IJMAI/article/view/249 (visité le 20/09/2018) (cf. p. 7).

[Ash09] Kevin Ashton. « That 'internet of things' thing ». In : *RFID journal* 22.7 (2009), p. 97-114 (cf. p. 8).

[Aug+16] Aloÿs Augustin et al. « A Study of LoRa : Long Range &amp ; Low Power Networks for the Internet of Things ». In : *Sensors* 16.9 (9 sept. 2016), p. 1466. DOI : 10.3390/s16091466. URL : https://www.mdpi.com/1424-8220/16/9/1466 (visité le 13/11/2018) (cf. p. 26).

[Bak05] N. Baker. « ZigBee and Bluetooth strengths and weaknesses for industrial applications ». In : *Computing Control Engineering Journal* 16.2 (avr. 2005), p. 20-25. ISSN : 0956-3385. DOI : 10.1049/cce:20050204 (cf. p. 19, 21, 22).

[BCS12] C. Bormann, A. P. Castellani et Z. Shelby. « CoAP : An Application Protocol for Billions of Tiny Internet Nodes ». In : *IEEE Internet Computing* 16.2 (mar. 2012), p. 62-67. ISSN : 1089-7801. DOI : 10.1109/MIC.2012.29 (cf. p. 21).

[Bel16] B. Bellalta. « IEEE 802.11ax : High-efficiency WLANS ». In : *IEEE Wireless Communications* 23.1 (fév. 2016), p. 38-46. ISSN : 1536-1284. DOI : 10.1109/MWC.2016.7422404 (cf. p. 23).

[BJK05] Paul H. Bouchier, Ronald E. Gilbert Jr et Christine Koerber. « Method and system for using a universal serial bus (USB) as a peer-to-peer network ». Brev. amér. 6839771B1. Hewlett-Packard Development Co LP. 4 jan. 2005. URL : https://patents.google.com/patent/US6839771B1/en (visité le 30/10/2018) (cf. p. 13).

[Bon+12] Flavio Bonomi et al. « Fog computing and its role in the internet of things ». In : *Proceedings of the first edition of the MCC workshop on Mobile cloud computing*. ACM, 2012, p. 13-16 (cf. p. 9).

[Bro01a] David L. Brock. « The electronic product code (epc) ». In : *Auto-ID Center White Paper MIT-AUTOID-WH-002* (2001) (cf. p. 8).

[Bro01b] P. Brooks. « Ethernet/IP-industrial protocol ». In : *ETFA 2001. 8th International Conference on Emerging Technologies and Factory Automation. Proceedings (Cat. No.01TH8597)*. ETFA 2001. 8th International Conference on Emerging Technologies and Factory Automation. Proceedings (Cat. No.01TH8597). T. 2. Oct. 2001, 505-514 vol.2. DOI : 10.1109/ETFA.2001.997725 (cf. p. 16).

[BS06] A. Bose et K. G. Shin. « On Mobile Viruses Exploiting Messaging and Bluetooth Services ». In : *2006 Securecomm and Workshops*. 2006 Securecomm and Workshops. Août 2006, p. 1-10. doi : 10.1109/SECCOMW.2006.359562 (cf. p. 22).

[CA11] Thomas Chen et Saeed Abu-Nimeh. « Lessons from stuxnet ». In : *Computer* 44.4 (2011), p. 91-93 (cf. p. 6).

[Car08] Dick Caro. *Wireless networks for industrial automation*. OCLC : 670630160. Research Triangle Park, NC : ISA, 2008. isbn : 978-1-61583-562-1. url : http://app.knovel.com/hotlink/toc/id:kpWNIAE00A/wireless-networks-for (visité le 23/11/2018) (cf. p. 20).

[Cen+16] M. Centenaro et al. « Long-range communications in unlicensed bands : the rising stars in the IoT and smart city scenarios ». In : *IEEE Wireless Communications* 23.5 (oct. 2016), p. 60-67. issn : 1536-1284. doi : 10.1109/MWC.2016.7721743 (cf. p. 27).

[Che+17] J. Chen et al. « Narrowband Internet of Things : Implementations and Applications ». In : *IEEE Internet of Things Journal* 4.6 (déc. 2017), p. 2309-2314. issn : 2327-4662. doi : 10.1109/JIOT.2017.2764475 (cf. p. 25, 27).

[Chr17] Christine Kerdellant. « La France doit embrasser en même temps les industries 3.0 et 4.0 - Editorial ». In : *l'Usine Nouvelle* 3509 (30 mar. 2017). issn : 0042-126X. url : https://www.usinenouvelle.com/editorial/la-france-doit-embrasser-en-meme-temps-les-industries-3-0-et-4-0.N519464 (visité le 22/10/2018) (cf. p. 3).

[CIS17] CISCO. *Time-Sensitive Networking : A Technical Introduction White Paper*. Rapport technique. CISCO, 2017, p. 8. url : https://www.cisco.com/c/dam/en/us/solutions/collateral/industry-solutions/white-paper-c11-738950.pdf (visité le 09/01/2019) (cf. p. 14).

[CNM10] Deji Chen, Mark Nixon et Aloysius Mok. « Why WirelessHART ». In : *WirelessHART™ : Real-Time Mesh Network for Industrial Automation*. Sous la dir. de Deji Chen, Mark Nixon et Aloysius Mok. Boston, MA : Springer US, 2010, p. 195-199. isbn : 978-1-4419-6047-4. doi : 10.1007/978-1-4419-6047-4_15. url : https://doi.org/10.1007/978-1-4419-6047-4_15 (visité le 30/10/2018) (cf. p. 21).

[Col+18] M. Collotta et al. « Bluetooth 5 : A Concrete Step Forward toward the IoT ». In : *IEEE Communications Magazine* 56.7 (juil. 2018), p. 125-131. issn : 0163-6804. doi : 10.1109/MCOM.2018.1700053 (cf. p. 22).

[Con18a] Contributeurs de Wikipédia. *Ethernet frame*. In : *Wikipedia*. Page Version ID : 874358840. 18 déc. 2018. url : https://en.wikipedia.org/w/index.php?title=Ethernet_frame&oldid=874358840 (visité le 19/12/2018) (cf. p. 14).

[Con18b] Contributeurs de Wikipédia. *SERCOS III*. In : *Wikipedia*. Page Version ID : 855929777. 21 août 2018. url : https://en.wikipedia.org/w/index.php?title=SERCOS_III&oldid=855929777 (visité le 19/12/2018) (cf. p. 16).

[Cor97] Microsoft Corporation, éd. *PC 97 hardware design guide : the technical reference for designing PCs and peripherals for the Microsoft Windows family of operating systems*. Microsoft professional editions. OCLC : 833181213. Redmond, Wash : Microsoft Press, 1997. 427 p. isbn : 978-1-57231-381-1 (cf. p. 13).

[CVV08] G. Cena, A. Valenzano et S. Vitturi. « Hybrid wired/wireless networks for real-time communications ». In : *IEEE Industrial Electronics Magazine* 2.1 (mar. 2008), p. 8-20. issn : 1932-4529. doi : 10.1109/MIE.2008.917155 (cf. p. 16).

[CYZ17] Yujun Cheng, Dong Yang et Huachun Zhou. « Det-WiFi : A Multihop TDMA MAC Implementation for Industrial Deterministic Applications Based on Commodity 802.11 Hardware ». In : *Wireless Communications and Mobile Computing* 2017 (2017) (cf. p. 23).

[DAS14] Domenico De Guglielmo, Giuseppe Anastasi et Alessio Seghetti. « From ieee 802.15. 4 to ieee 802.15. 4e : A step towards the internet of things ». In : *Advances onto the Internet of Things*. Springer, 2014, p. 135-152 (cf. p. 19).

[Dec09] J. Decotignie. « The Many Faces of Industrial Ethernet [Past and Present] ». In : *IEEE Industrial Electronics Magazine* 3.1 (mar. 2009), p. 8-19. issn : 1932-4529. doi : 10.1109/MIE.2009.932171 (cf. p. 12).

[DM08] M. Darianian et M. P. Michael. « Smart Home Mobile RFID-Based Internet-of-Things Systems and Services ». In : *2008 International Conference on Advanced Computer Theory and Engineering*. 2008 International Conference on Advanced Computer Theory and Engineering. Déc. 2008, p. 116-120. doi : 10.1109/ICACTE.2008.180 (cf. p. 8).

[DP81] Yogen K. Dalal et Robert S. Printis. « 48-bit absolute internet and Ethernet host numbers ». In : *ACM SIGCOMM Computer Communication Review*. T. 11. ACM, 1981, p. 240-245 (cf. p. 14).

[DR00] P. Dallemagne et L. Ruiz. « An application layer for using Firewire in industrial applications ». In : *2000 IEEE International Workshop on Factory Communication Systems. Proceedings (Cat. No.00TH8531)*. 2000 IEEE International Workshop on Factory Communication Systems. Proceedings (Cat. No.00TH8531). Sept. 2000, p. 109-116. doi : 10.1109/WFCS.2000.882540 (cf. p. 14).

[DV08] Adam Dunkels et Jean-Philippe Vasseur. « IP for smart objects ». In : *Ipso alliance white paper* 1 (2008) (cf. p. 8).

[DW93] Wim Diepstraten et N. WCND-Utrecht. « IEEE 802.11 wireless access method and physical specification ». In : *Power* 5.10 (1993) (cf. p. 23).

[Ehr17] Jesse M. Ehrenfeld. « WannaCry, Cybersecurity and Health Information Technology : A Time to Act ». In : *Journal of Medical Systems* 41.7 (24 mai 2017), p. 104. issn : 1573-689X. doi : 10.1007/s10916-017-0752-1. url : https://doi.org/10.1007/s10916-017-0752-1 (visité le 27/11/2018) (cf. p. 6).

[Eja+17] W. Ejaz et al. « Efficient Energy Management for the Internet of Things in Smart Cities ». In : *IEEE Communications Magazine* 55.1 (jan. 2017), p. 84-91. issn : 0163-6804. doi : 10.1109/MCOM.2017.1600218CM (cf. p. 10).

[Eva11] Dave Evans. *How the Next Evolution of the Internet Is Changing Everything*. Rapport technique. CISCO, 2011, p. 11. url : https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf (visité le 09/01/2019) (cf. p. 9).

[Fan+05] Y. Fan * et al. « Architecture and operational mechanisms of networked manufacturing integrated platform ». In : *International Journal of Production Research* 43.12 (15 juin 2005), p. 2615-2629. issn : 0020-7543. doi : 10.1080/00207540500045162. url : https://doi.org/10.1080/00207540500045162 (visité le 12/11/2018) (cf. p. 7).

[FB18] Joseph Finnegan et Stephen Brown. « A Comparative Survey of LPWA Networking ». In : *arXiv :1802.04222 [cs]* (12 fév. 2018). arXiv : 1802.04222. url : http://arxiv.org/abs/1802.04222 (visité le 15/11/2018) (cf. p. 25).

[Fel05] M. Felser. « Real-Time Ethernet - Industry Prospective ». In : *Proceedings of the IEEE* 93.6 (juin 2005), p. 1118-1129. issn : 0018-9219. doi : 10.1109/JPROC.2005.849720 (cf. p. 12, 15).

[Fer02] Niels Ferguson. « Michael : an improved MIC for 802.11 WEP ». In : *IEEE doc* 802.2 (2002) (cf. p. 24).

[Fin09] Klaus Finkenzeller. « Known attacks on RFID systems, possible countermeasures and upcoming standardisation activities ». In : *5th European Workshop on RFID Systems and Technologies*. 2009, p. 1-31 (cf. p. 18).

[Flo+13] A. B. Flores et al. « IEEE 802.11af : a standard for TV white space spectrum sharing ». In : *IEEE Communications Magazine* 51.10 (oct. 2013), p. 92-100. issn : 0163-6804. doi : 10.1109/MCOM.2013.6619571 (cf. p. 24).

[FM10] Klaus Finkenzeller et Dörte Müller. *RFID handbook : fundamentals and applications in contactless smart cards, radio frequency identification and near-field communication*. 3. ed. OCLC : 724127873. Chichester : Wiley, 2010. 462 p. isbn : 978-0-470-69506-7 (cf. p. 18).

[FMS01] Scott Fluhrer, Itsik Mantin et Adi Shamir. « Weaknesses in the Key Scheduling Algorithm of RC4 ». In : *Selected Areas in Cryptography*. Sous la dir. de Serge Vaudenay et Amr M. Youssef. Lecture Notes in Computer Science. Springer Berlin Heidelberg, 2001, p. 1-24. isbn : 978-3-540-45537-0 (cf. p. 24).

[Fra+13] M. Franceschinis et al. « On the performance of ZigBee Pro and ZigBee IP in IEEE 802.15.4 networks ». In : *2013 IEEE 9th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*. 2013 IEEE 9th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob). Oct. 2013, p. 83-88. doi : 10.1109/WiMOB.2013.6673344 (cf. p. 21).

[FS02] M. Felser et T. Sauter. « The fieldbus war : history or short break between battles ? » In : *4th IEEE International Workshop on Factory Communication Systems*. 4th IEEE International Workshop on Factory Communication Systems. Août 2002, p. 73-80. doi : 10.1109/WFCS.2002.1159702 (cf. p. 12).

[FS18] Guillaume Ferré et Eric Pierre Simon. « An introduction to Sigfox and LoRa PHY and MAC layers ». Avr. 2018. url : https://hal.archives-ouvertes.fr/hal-01774080 (visité le 13/11/2018) (cf. p. 26).

[Gas09] Matthew S. Gast. *802.11 Wireless Networks : The Definitive Guide*. O'Reilly Media, juin 2009. 656 p. isbn : 978-0-596-10052-0. url : http://shop.oreilly.com/product/9780596100520.do (visité le 14/11/2018) (cf. p. 23).

[GHI15] Berhane G. Gebremedhin, Jussi Haapola et Jari Iinatti. « Performance evaluation of IEEE 802.15. 4k priority channel access with DSSS PHY ». In : *European Wireless 2015; 21th European Wireless Conference; Proceedings of*. VDE, 2015, p. 1-6 (cf. p. 27).

[GKC04] Neil Gershenfeld, Raffi Krikorian et Danny Cohen. « The Internet of Things ». In : *Scientific American* 291.4 (2004), p. 76-81. issn : 0036-8733. url : https://www.jstor.org/stable/26060727 (visité le 29/11/2018) (cf. p. 8, 10).

[GOP12] Carles Gomez, Joaquim Oller et Josep Paradells. « Overview and Evaluation of Bluetooth Low Energy : An Emerging Low-Power Wireless Technology ». In : *Sensors* 12.9 (29 août 2012), p. 11734-11753. doi : 10.3390/s120911734. url : https://www.mdpi.com/1424-8220/12/9/11734 (visité le 19/11/2018) (cf. p. 22).

[GP10] C. Gomez et J. Paradells. « Wireless home automation networks : A survey of architectures and technologies ». In : *IEEE Communications Magazine* 48.6 (juin 2010), p. 92-101. issn : 0163-6804. doi : 10.1109/MCOM.2010.5473869 (cf. p. 18).

[GPM15] M. S. D. Gupta, V. Patchava et V. Menezes. « Healthcare based on IoT using Raspberry Pi ». In : *2015 International Conference on Green Computing and Internet of Things (ICGCIoT)*. 2015 International Conference on Green Computing and Internet of Things (ICGCIoT). Oct. 2015, p. 796-799. doi : 10.1109/ICGCIoT.2015.7380571 (cf. p. 10).

[Gri17] D. A. Grier. « The Radical Technology of Industrie 4.0 ». In : *Computer* 50.4 (avr. 2017), p. 120-120. issn : 0018-9162. doi : 10.1109/MC.2017.109 (cf. p. 5).

[GT09] Dominique Guinard et Vlad Trifa. « Towards the web of things : Web mashups for embedded devices ». In : *Workshop on Mashups, Enterprise Mashups and Lightweight Composition on the Web (MEM 2009), in proceedings of WWW (International World Wide Web Conferences), Madrid, Spain*. T. 15. 2009 (cf. p. 8).

[Hey+07] Thomas S. Heydt-Benjamin et al. « Vulnerabilities in first-generation RFID-enabled credit cards ». In : *International Conference on Financial Cryptography and Data Security*. Springer, 2007, p. 2-14 (cf. p. 18).

[HKS09] Stephan Haller, Stamatis Karnouskos et Christoph Schroth. « The Internet of Things in an Enterprise Context ». In : *Future Internet – FIS 2008*. Sous la dir. de John Domingue, Dieter Fensel et Paolo Traverso. Lecture Notes in Computer Science. Springer Berlin Heidelberg, 2009, p. 14-28. isbn : 978-3-642-00985-3 (cf. p. 10).

[HM95] G. Hoffman et D. Moore. « IEEE 1394 : a ubiquitous bus ». In : *Digest of Papers. COMPCON'95. Technologies for the Information Superhighway*. Digest of Papers. COMPCON'95. Technologies for the Information Superhighway. Mar. 1995, p. 334-338. doi : 10.1109/CMPCON.1995.512405 (cf. p. 14).

[Hor10] Craig A. Hornbuckle. « Fractional-N synthesized chirp generator ». Brev. amér. 7791415B2. Semtech Corp. 7 sept. 2010. url : https://patents.google.com/patent/US7791415/en (visité le 12/11/2018) (cf. p. 25).

[How94] Mark Howarth. « HART — Standard for 4–20mA Digital Communications ». In : *Measurement and Control* 27.1 (1er fév. 1994), p. 5-7. issn : 0020-2940. doi : 10.1177/002029409402700102. url : https://doi.org/10.1177/002029409402700102 (visité le 30/10/2018) (cf. p. 13).

[IEE+12] IEEE Computer Society et al. *IEEE standard for local and metropolitan area networks. Part 15.4, Amendment 3, Part 15.4, Amendment 3,* OCLC : 800045409. New York : Institute of Electrical et Electronics Engineers, 2012. isbn : 978-0-7381-7259-0. url : http://ieeexplore.ieee.org/servlet/opac?punumber=6190696 (visité le 21/11/2018) (cf. p. 19).

[IEE+13] IEEE Computer Society et al. *IEEE standard for local and metropolitan area networks. Amendment 5 : Physical layer specifications for low energy, critical infrastructure monitoring networks Part 15.4, Part 15.4,* OCLC : 858036474. 2013. ISBN : 978-0-7381-8446-3. URL : http://ieeexplore.ieee.org/servlet/opac?punumber=6581826 (visité le 21/11/2018) (cf. p. 19).

[IEE+99] IEEE Computer Society et al. *Supplement to IEEE standard for Information technology– telecommunications and information exchange between systems– local and metropolitan area networks – specific requirements : part 11 : wireless LAN medium access control (MAC) and physical layer (PHY) specifications : High-speed physical layer in the 5 GHz band.* OCLC : 50293188. New York, N.Y., USA : Institute of Electrical et Electronics Engineers, 1999. ISBN : 978-0-7381-1809-3. URL : http://ieeexplore.ieee.org/lpdocs/epic03/standards.htm (visité le 14/11/2018) (cf. p. 23).

[IEE03] IEEE Computer Society. *IEEE Std 802.15.4-2003 : IEEE Standard for Information Technology - Telecommunications and Information Exchange Between Systems - Local and Metropolitan Area Networks Specific Requirements Part 15.4 : Wireless Medium Access Control (MAC) and Physical Layer (.* OCLC : 956670333. S.l. : IEEE, 2003. ISBN : 978-0-7381-3686-8. URL : http://ieeexplore.ieee.org/servlet/opac?punumber=8762 (visité le 21/11/2018) (cf. p. 19).

[IEE05] IEEE Computer Society. « IEEE Standard for Information technology–Local and metropolitan area networks–Specific requirements–Part 11 : Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications - Amendment 8 : Medium Access Control (MAC) Quality of Service Enhancements ». In : *IEEE Std 802.11e-2005 (Amendment to IEEE Std 802.11, 1999 Edition (Reaff 2003)* (nov. 2005), p. 1-212. DOI : 10.1109/IEEESTD.2005.97890 (cf. p. 23).

[IH11] W. Issovits et M. Hutter. « Weaknesses of the ISO/IEC 14443 protocol regarding relay attacks ». In : *2011 IEEE International Conference on RFID-Technologies and Applications.* 2011 IEEE International Conference on RFID-Technologies and Applications. Sept. 2011, p. 335-342. DOI : 10.1109/RFID-TA.2011.6068658 (cf. p. 18).

[IL11] IEEE Computer Society et LAN/MAN Standards Committee. « IEEE Standard for Local and Metropolitan Area Networks - Timing and Synchronization for Time-Sensitive Applications in Bridged Local Area Networks ». In : *IEEE Std 802.1AS-2011* (mar. 2011), p. 1-292. DOI : 10.1109/IEEESTD.2011.5741898 (cf. p. 14).

[IL97] IEEE Computer Society et LAN/MAN Standards Committee. *Information technology – telecommunications and information exchange between systems – local and metropolitan area networks – specific requirements – part 11, wireless LAN medium access control (MAC) and physical layer (PHY) specifications.* OCLC : 38598622. New York, N.Y. : Institute of Electrical et Electronics Engineers, 1997. ISBN : 978-1-55937-935-9 (cf. p. 23).

[Isl+15] S. M. R. Islam et al. « The Internet of Things for Health Care : A Comprehensive Survey ». In : *IEEE Access* 3 (2015), p. 678-708. ISSN : 2169-3536. DOI : 10.1109/ACCESS.2015.2437951 (cf. p. 10).

[Ist+11] R. S. H. Istepanian et al. « The potential of Internet of m-health Things “m-IoT” for non-invasive glucose level sensing ». In : *2011 Annual International Conference of the IEEE Engineering in Medicine and Biology Society.* 2011 Annual International

Conference of the IEEE Engineering in Medicine and Biology Society. Août 2011, p. 5264-5266. DOI : 10.1109/IEMBS.2011.6091302 (cf. p. 10).

[Jaz14] N. JAZDI. « Cyber physical systems in the context of Industry 4.0 ». In : *2014 IEEE International Conference on Automation, Quality and Testing, Robotics*. 2014 IEEE International Conference on Automation, Quality and Testing, Robotics. Mai 2014, p. 1-4. DOI : 10.1109/AQTR.2014.6857843 (cf. p. 11).

[JB04] D. JANSEN et H. BUTTNER. « Real-time ethernet the EtherCAT solution ». In : *Computing Control Engineering Journal* 15.1 (fév. 2004), p. 16-21. ISSN : 0956-3385. DOI : 10.1049/cce:20040104 (cf. p. 15).

[Joh99] P. JOHANSSON. *IPv4 over IEEE 1394*. RFC 2734. Internet Requests for Comments. RFC Editor, 1999, p. 29. URL : https://www.rfc-editor.org/info/rfc2734 (visité le 01/02/2019) (cf. p. 14).

[JW01] Markus JAKOBSSON et Susanne WETZEL. « Security Weaknesses in Bluetooth ». In : *Topics in Cryptology — CT-RSA 2001*. Sous la dir. de David NACCACHE. Lecture Notes in Computer Science. Springer Berlin Heidelberg, 2001, p. 176-191. ISBN : 978-3-540-45353-6 (cf. p. 22).

[Kag13] Henning KAGERMANN. *Recommendations for Implementing the Strategic Initiative INDUSTRIE 4.0 : Securing the Future of German Manufacturing Industry ; Final Report of the Industrie 4.0 Working Group*. Forschungsunion, avr. 2013, p. 82 (cf. p. 4, 5, 7).

[KAT06] A. KOUBAA, M. ALVES et E. TOVAR. « GTS allocation analysis in IEEE 802.15.4 for real-time wireless sensor networks ». In : *Proceedings 20th IEEE International Parallel Distributed Processing Symposium*. Proceedings 20th IEEE International Parallel Distributed Processing Symposium. Avr. 2006, 8 p. DOI : 10.1109/IPDPS.2006.1639415 (cf. p. 19).

[Kau+15] S. KAUL et al. « Novel multi-interface USB prototype device for merging commonly used peripheral devices ». In : *2015 International Conference on Industrial Instrumentation and Control (ICIC)*. 2015 International Conference on Industrial Instrumentation and Control (ICIC). Mai 2015, p. 17-22. DOI : 10.1109/IIC.2015.7150584 (cf. p. 13).

[KDI10] M. KNEZIC, B. DOKIC et Z. IVANOVIC. « Topology aspects in EtherCAT networks ». In : *Proceedings of 14th International Power Electronics and Motion Control Conference EPE-PEMC 2010*. Proceedings of 14th International Power Electronics and Motion Control Conference EPE-PEMC 2010. Sept. 2010, T1–1–T1-6. DOI : 10.1109/EPEPEMC.2010.5606688 (cf. p. 15).

[KG04] R. KRIKORIAN et N. GERSHENFELD. « Internet 0—inter-device internetworking ». In : *BT technology journal* 22.4 (2004), p. 278-284 (cf. p. 8).

[KH16] X. KRASNIQI et E. HAJRIZI. « Use of IoT Technology to Drive the Automotive Industry from Connected to Full Autonomous Vehicles ». In : *IFAC-PapersOnLine*. 17th IFAC Conference on International Stability, Technology and Culture TECIS 2016 49.29 (1er jan. 2016), p. 269-274. ISSN : 2405-8963. DOI : 10.1016/j.ifacol.2016.11.078. URL : http://www.sciencedirect.com/science/article/pii/S2405896316325162 (visité le 14/12/2018) (cf. p. 10).

[Kho+15] Evgeny KHOROV et al. « A survey on IEEE 802.11ah : An enabling networking technology for smart cities ». In : *Computer Communications*. Special Issue on Networking and Communications for Smart Cities 58 (1er mar. 2015), p. 53-69. ISSN : 0140-3664. DOI : 10.1016/j.comcom.2014.08.008. URL : http://www.sciencedirect.com/science/article/pii/S0140366414002989 (visité le 14/11/2018) (cf. p. 24).

[Kim+08] A. N. KIM et al. « When HART goes wireless : Understanding and implementing the WirelessHART standard ». In : *2008 IEEE International Conference on Emerging Technologies and Factory Automation*. 2008 IEEE International Conference on Emerging Technologies and Factory Automation. Sept. 2008, p. 899-907. DOI : 10.1109/ETFA.2008.4638503 (cf. p. 20).

[Kri04] Raffi Chant KRIKORIAN. « Internet 0 ». Thèse de doct. Massachusetts Institute of Technology, 2004 (cf. p. 8).

[Kus13] D. KUSHNER. « The real story of stuxnet ». In : *IEEE Spectrum* 50.3 (mar. 2013), p. 48-53. ISSN : 0018-9235. DOI : 10.1109/MSPEC.2013.6471059 (cf. p. 6).

[Kwo+16] G. KWON et al. « Bluetooth low energy security vulnerability and improvement method ». In : *2016 IEEE International Conference on Consumer Electronics-Asia (ICCE-Asia)*. 2016 IEEE International Conference on Consumer Electronics-Asia (ICCE-Asia). Oct. 2016, p. 1-4. DOI : 10.1109/ICCE-Asia.2016.7804832 (cf. p. 22).

[Lan05] J. LANDT. « The history of RFID ». In : *IEEE Potentials* 24.4 (oct. 2005), p. 8-11. ISSN : 0278-6648. DOI : 10.1109/MP.2005.1549751 (cf. p. 18, 19).

[Lee+15] Jay LEE et al. « Industrial Big Data Analytics and Cyber-physical Systems for Future Maintenance & Service Innovation ». In : *Procedia CIRP*. Proceedings of the 4th International Conference on Through-life Engineering Services 38 (1er jan. 2015), p. 3-7. ISSN : 2212-8271. DOI : 10.1016/j.procir.2015.08.026. URL : http://www.sciencedirect.com/science/article/pii/S2212827115008744 (visité le 17/12/2018) (cf. p. 11).

[Lee+17] JungWoon LEE et al. « Risk analysis and countermeasure for bit-flipping attack in LoRaWAN ». In : *2017 International Conference on Information Networking (ICOIN)*. 2017 International Conference on Information Networking (ICOIN). Jan. 2017, p. 549-551. DOI : 10.1109/ICOIN.2017.7899554 (cf. p. 26).

[Lee03] Jay LEE. « E-manufacturing—fundamental, tools, and transformation ». In : *Robotics and Computer-Integrated Manufacturing*. Leadership of the Future in Manufacturing 19.6 (1er déc. 2003), p. 501-507. ISSN : 0736-5845. DOI : 10.1016/S0736-5845(03)00060-7. URL : http://www.sciencedirect.com/science/article/pii/S0736584503000607 (visité le 29/11/2018) (cf. p. 7).

[Li+10] Bo-Hu LI et al. « Cloud manufacturing : a new service-oriented networked manufacturing model ». In : *Computer integrated manufacturing systems* 16.1 (2010), p. 1-7 (cf. p. 7).

[Lia+11] Wei LIANG et al. « Survey and experiments of WIA-PA specification of industrial wireless network ». In : *Wireless Communications and Mobile Computing* 11.8 (1er août 2011), p. 1197-1212. ISSN : 1530-8677. DOI : 10.1002/wcm.976. URL : https://onlinelibrary.wiley.com/doi/abs/10.1002/wcm.976 (visité le 23/11/2018) (cf. p. 20).

[Lia+13] Wei Liang et al. « Research of Adaptive Frequency Hopping Technology in WIA-PA Industrial Wireless Network ». In : *Advances in Wireless Sensor Networks*. Sous la dir. de Ruchuan Wang et Fu Xiao. Communications in Computer and Information Science. Springer Berlin Heidelberg, 2013, p. 248-262. isbn : 978-3-642-36252-1 (cf. p. 20).

[Lia+17] C. Liao et al. « Multi-Hop LoRa Networks Enabled by Concurrent Transmission ». In : *IEEE Access* 5 (2017), p. 21430-21446. issn : 2169-3536. doi : 10.1109/ACCESS.2017.2755858 (cf. p. 26).

[Lib+18] Olof Liberg et al. *Cellular Internet of things : technologies, standards, and performance*. OCLC : 1004271367. 2018. isbn : 978-0-12-812459-8. (Visité le 25/09/2018) (cf. p. 25).

[LM12] Demian Lekomtcev et Roman Maršálek. « Comparison of 802.11 af and 802.22 standards–physical layer and cognitive functionality ». In : *Elektro Revue* 3.2 (2012), p. 12-18 (cf. p. 24).

[Lon+18] Angela M. Lonzetta et al. « Security Vulnerabilities in Bluetooth Technology as Used in IoT ». In : *Journal of Sensor and Actuator Networks* 7.3 (sept. 2018), p. 28. doi : 10.3390/jsan7030028. url : https://www.mdpi.com/2224-2708/7/3/28 (visité le 04/02/2019) (cf. p. 22).

[Lu17] Yang Lu. « Industry 4.0 : A survey on technologies, applications and open research issues ». In : *Journal of Industrial Information Integration* 6 (1er juin 2017), p. 1-10. issn : 2452-414X. doi : 10.1016/j.jii.2017.04.005. url : http://www.sciencedirect.com/science/article/pii/S2452414X17300043 (visité le 20/09/2018) (cf. p. 7).

[Lun+14] Denise Lund et al. « Worldwide and regional internet of things (iot) 2014–2020 forecast : A virtuous circle of proven value and demand ». In : *International Data Corporation (IDC), Tech. Rep* 1 (2014) (cf. p. 9).

[LXZ15] Shancang Li, Li Da Xu et Shanshan Zhao. « The internet of things : a survey ». In : *Information Systems Frontiers* 17.2 (1er avr. 2015), p. 243-259. issn : 1572-9419. doi : 10.1007/s10796-014-9492-7. url : https://doi.org/10.1007/s10796-014-9492-7 (visité le 25/09/2018) (cf. p. 8).

[Max06] Maxim Integrated Products, Inc. *How Far and How Fast Can You Go with RS-485 ? - Application Note - Maxim*. Maxim Integrated - Analog, linear, & mixed-signal devices. 25 juil. 2006. url : https://www.maximintegrated.com/en/app-notes/index.mvp/id/3884 (visité le 23/10/2018) (cf. p. 13).

[MBR15] Roberto Minerva, Abyi Biru et Domenico Rotondi. « Towards a definition of the Internet of Things (IoT) ». In : *IEEE Internet Initiative* 1 (2015), p. 1-86 (cf. p. 7, 9).

[Mek+18] Kais Mekki et al. « A comparative study of LPWAN technologies for large-scale IoT deployment ». In : *ICT Express* (4 jan. 2018). issn : 2405-9595. doi : 10.1016/j.icte.2017.12.005. url : http://www.sciencedirect.com/science/article/pii/S2405959517302953 (visité le 26/09/2018) (cf. p. 25, 26).

[MFD00] Benoit Montreuil, Jean-Marc Frayret et Sophie D'Amours. « A strategic framework for networked manufacturing ». In : *Computers in Industry* 42.2 (1er juin 2000), p. 299-317. issn : 0166-3615. doi : 10.1016/S0166-3615(99)00078-0. url : http://www.sciencedirect.com/science/article/pii/S0166361599000780 (visité le 12/11/2018) (cf. p. 7).

[Mol85] Michael K. Molloy. « Collision resolution on the CSMA/CD bus ». In : *Computer Networks and ISDN Systems*. Local Area Networks 9.3 (1er mar. 1985), p. 209-214. ISSN : 0169-7552. DOI : 10.1016/0169-7552(85)90044-3. URL : http://www.sciencedirect.com/science/article/pii/0169755285900443 (visité le 08/11/2018) (cf. p. 14).

[Mon+07] G. Montenegro et al. *Transmission of IPv6 Packets over IEEE 802.15.4 Networks*. RFC 4944. Internet Requests for Comments. RFC Editor, 2007. URL : https://www.rfc-editor.org/info/rfc4944 (visité le 01/02/2019) (cf. p. 19).

[MPV11] L. Mainetti, L. Patrono et A. Vilei. « Evolution of wireless sensor networks towards the Internet of Things : A survey ». In : *SoftCOM 2011, 19th International Conference on Software, Telecommunications and Computer Networks*. SoftCOM 2011, 19th International Conference on Software, Telecommunications and Computer Networks. Sept. 2011, p. 1-6 (cf. p. 18).

[Mro+18] H. Mroue et al. « MAC layer-based evaluation of IoT technologies : LoRa, SigFox and NB-IoT ». In : *2018 IEEE Middle East and North Africa Communications Conference (MENACOMM)*. 2018 IEEE Middle East and North Africa Communications Conference (MENACOMM). Avr. 2018, p. 1-5. DOI : 10.1109/MENACOMM.2018.8371016 (cf. p. 26).

[Na+17] SeungJae Na et al. « Scenario and countermeasure for replay attack using join request messages in LoRaWAN ». In : *2017 International Conference on Information Networking (ICOIN)*. 2017 International Conference on Information Networking (ICOIN). Jan. 2017, p. 718-720. DOI : 10.1109/ICOIN.2017.7899580 (cf. p. 26).

[NGK16] K. E. Nolan, W. Guibene et M. Y. Kelly. « An evaluation of low power wide area network technologies for the Internet of Things ». In : *2016 International Wireless Communications and Mobile Computing Conference (IWCMC)*. 2016 International Wireless Communications and Mobile Computing Conference (IWCMC). Sept. 2016, p. 439-444. DOI : 10.1109/IWCMC.2016.7577098 (cf. p. 26).

[Nor16] Amy Nordrum. *Popular Internet of Things Forecast of 50 Billion Devices by 2020 Is Outdated*. IEEE Spectrum : Technology, Engineering, and Science News. 18 août 2016. URL : https://spectrum.ieee.org/tech-talk/telecom/internet/popular-internet-of-things-forecast-of-50-billion-devices-by-2020-is-outdated (visité le 09/01/2019) (cf. p. 9).

[NR12] Mark Nixon et T. X. Round Rock. « A Comparison of WirelessHART and ISA100. 11a ». In : *Whitepaper, Emerson Process Management* (2012), p. 1-36 (cf. p. 20).

[Och+17] M. N. Ochoa et al. « Evaluating LoRa energy efficiency for adaptive networks : From star to mesh topologies ». In : *2017 IEEE 13th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*. 2017 IEEE 13th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob). Oct. 2017, p. 1-8. DOI : 10.1109/WiMOB.2017.8115793 (cf. p. 26).

[Orm03] H. Orman. « The Morris worm : a fifteen-year perspective ». In : *IEEE Security Privacy* 99.5 (sept. 2003), p. 35-43. ISSN : 1540-7993. DOI : 10.1109/MSECP.2003.1236233 (cf. p. 6).

[PC11] Stig Petersen et Simon Carlsen. « WirelessHART Versus ISA100.11a : The Format War Hits the Factory Floor ». In : *IEEE Industrial Electronics Magazine* 5.4 (déc. 2011), p. 23-34. ISSN : 1932-4529. DOI : 10.1109/MIE.2011.943023. URL : http://ieeexplore.ieee.org/document/6102417/ (visité le 25/09/2018) (cf. p. 20).

[Piy+18] Rajeev Piyare et al. « On-Demand LoRa : Asynchronous TDMA for Energy Efficient and Low Latency Communication in IoT ». In : *Sensors* 18.11 (nov. 2018), p. 3718. DOI : 10.3390/s18113718. URL : https://www.mdpi.com/1424-8220/18/11/3718 (visité le 06/12/2018) (cf. p. 26).

[PR16] S. Persia et L. Rea. « Next generation M2M Cellular Networks : LTE-MTC and NB-IoT capacity analysis for Smart Grids applications ». In : *2016 AEIT International Annual Conference (AEIT)*. 2016 AEIT International Annual Conference (AEIT). Oct. 2016, p. 1-6. DOI : 10.23919/AEIT.2016.7892789 (cf. p. 25).

[Pry08] G. Prytz. « A performance analysis of EtherCAT and PROFINET IRT ». In : *2008 IEEE International Conference on Emerging Technologies and Factory Automation*. 2008 IEEE International Conference on Emerging Technologies and Factory Automation. Sept. 2008, p. 408-415. DOI : 10.1109/ETFA.2008.4638425 (cf. p. 15).

[RA02] G. Ramamurthy et K. Ashenayi. « Comparative study of the FireWire/spl trade/ IEEE-1394 protocol with the Universal Serial Bus and Ethernet ». In : *The 2002 45th Midwest Symposium on Circuits and Systems, 2002. MWSCAS-2002.* The 2002 45th Midwest Symposium on Circuits and Systems, 2002. MWSCAS-2002. T. 2. Août 2002, p. II-II. DOI : 10.1109/MWSCAS.2002.1186910 (cf. p. 14).

[RDD99] L. Ruiz, P. Dallemagne et J. D. Decotignie. « Using Firewire as industrial network ». In : *Proceedings. SCCC'99 XIX International Conference of the Chilean Computer Science Society*. Proceedings. SCCC'99 XIX International Conference of the Chilean Computer Science Society. Nov. 1999, p. 201-208. DOI : 10.1109/SCCC.1999.810189 (cf. p. 14).

[RKS17] U. Raza, P. Kulkarni et M. Sooriyabandara. « Low Power Wide Area Networks : An Overview ». In : *IEEE Communications Surveys Tutorials* 19.2 (2017), p. 855-873. ISSN : 1553-877X. DOI : 10.1109/COMST.2017.2652320 (cf. p. 27).

[ROU+17] Loïc ROUCH et al. « A Universal Controller to Take Over a Z-Wave Network ». In : *Black Hat Europe 2017*. London, United Kingdom, déc. 2017, p. 1-9. URL : https://hal.inria.fr/hal-01684569 (visité le 20/11/2018) (cf. p. 18).

[San+16] Ramon Sanchez-Iborra et al. « State of the Art in LP-WAN Solutions for Industrial IoT Services ». In : *Sensors* 16.5 (17 mai 2016), p. 708. DOI : 10.3390/s16050708. URL : http://www.mdpi.com/1424-8220/16/5/708 (visité le 20/09/2018) (cf. p. 27).

[SBE01] Sanjay Sarma, David Brock et Daniel Engels. « Radio frequency identification and the electronic product code ». In : *IEEE micro* 21.6 (2001), p. 50-54 (cf. p. 8).

[Sch+01] M. Scholles et al. « IEEE 1394 "FireWire" system design for industrial and factory automation applications ». In : *ETFA 2001. 8th International Conference on Emerging Technologies and Factory Automation. Proceedings (Cat. No.01TH8597)*. ETFA 2001. 8th International Conference on Emerging Technologies and Factory Automation. Proceedings (Cat. No.01TH8597). T. 2. Oct. 2001, 627-630 vol.2. DOI : 10.1109/ETFA.2001.997744 (cf. p. 14).

[Sch01] V. Schiffer. « The CIP family of fieldbus protocols and its newest member - Ethernet/IP ». In : *ETFA 2001. 8th International Conference on Emerging Technologies and Factory Automation. Proceedings (Cat. No.01TH8597)*. ETFA 2001. 8th International Conference on Emerging Technologies and Factory Automation. Proceedings (Cat. No.01TH8597). Oct. 2001, 377-384 vol.1. doi : 10.1109/ETFA.2001.996391 (cf. p. 16).

[Sch04] E. Schemm. « SERCOS to link with ethernet for its third generation ». In : *Computing Control Engineering Journal* 15.2 (avr. 2004), p. 30-33. issn : 0956-3385. doi : 10.1049/cce:20040205 (cf. p. 15).

[SH80] John F. Shoch et Jon A. Hupp. « Measured performance of an Ethernet local network ». In : *Communications of the ACM* 23.12 (1980), p. 711-721 (cf. p. 14).

[Sho+85] J. F. Shoch et al. « The Ethernet ». In : *Local Area Networks : An Advanced Course*. Sous la dir. de D. Hutchison, J. A. Mariani et W. D. Shepherd. Berlin, Heidelberg : Springer Berlin Heidelberg, 1985, p. 1-35. isbn : 978-3-540-39286-6 (cf. p. 14).

[SOM14] F. Shrouf, J. Ordieres et G. Miragliotta. « Smart factories in Industry 4.0 : A review of the concept and of energy management approached in production based on the Internet of Things paradigm ». In : *2014 IEEE International Conference on Industrial Engineering and Engineering Management*. 2014 IEEE International Conference on Industrial Engineering and Engineering Management. Déc. 2014, p. 697-701. doi : 10.1109/IEEM.2014.7058728 (cf. p. 11).

[Sor+19] Nicolas Sornin et al. *Static Context Header Compression (SCHC) over LoRaWAN*. Internet-Draft draft-ietf-lpwan-schc-over-lorawan-00. Work in Progress. Internet Engineering Task Force, avr. 2019. 15 p. url : https://datatracker.ietf.org/doc/html/draft-ietf-lpwan-schc-over-lorawan-00 (cf. p. 26).

[SU05] I. T. U. Strategy et Policy Unit. « ITU Internet Reports 2005 : The internet of things ». In : *Geneva : International Telecommunication Union (ITU)*. Internet Report 1 (2005), p. 62 (cf. p. 8).

[Swa12] Melanie Swan. « Sensor Mania ! The Internet of Things, Wearable Computing, Objective Metrics, and the Quantified Self 2.0 ». In : *Journal of Sensor and Actuator Networks* 1.3 (déc. 2012), p. 217-253. doi : 10.3390/jsan1030217. url : https://www.mdpi.com/2224-2708/1/3/217 (visité le 08/01/2019) (cf. p. 10).

[SWH17] Rashmi Sharan Sinha, Yiqiao Wei et Seung-Hoon Hwang. « A survey on LPWA technology : LoRa and NB-IoT ». In : *ICT Express* 3.1 (1er mar. 2017), p. 14-21. issn : 2405-9595. doi : 10.1016/j.icte.2017.03.004. url : http://www.sciencedirect.com/science/article/pii/S2405959517300061 (visité le 15/10/2018) (cf. p. 26).

[Tao+11] Fei Tao et al. « Cloud manufacturing : a computing and service-oriented manufacturing model ». In : *Proceedings of the Institution of Mechanical Engineers, Part B : Journal of Engineering Manufacture* 225.10 (2011), p. 1969-1976 (cf. p. 7).

[TB09] Erik Tews et Martin Beck. « Practical attacks against WEP and WPA ». In : *Proceedings of the second ACM conference on Wireless network security*. ACM, 2009, p. 79-86 (cf. p. 24).

[TBS17] S. Thielemans, M. Bezunartea et K. Steenhaut. « Establishing transparent IPv6 communication on LoRa based low power wide area networks (LPWANS) ». In : *2017 Wireless Telecommunications Symposium (WTS)*. 2017 Wireless Telecommunications Symposium (WTS). Avr. 2017, p. 1-6. doi : 10.1109/WTS.2017.7943535 (cf. p. 26).

[TEL12] TELECOMMUNICATION STANDARDIZATION SECTOR OF ITU. *Overview of the Internet of Things*. Recommendation ITU-T Y.2060/Y.4000. International Telecommunication Union, 15 juin 2012, p. 22. URL : http://handle.itu.int/11.1002/1000/11559 (cf. p. 8).

[TM06] Frederic THIESSE et Florian MICHAHELLES. « An overview of EPC technology ». In : *Sensor review* 26.2 (2006), p. 101-105 (cf. p. 8).

[Tra+17] Amy J. C. TRAPPEY et al. « A review of essential standards and patent landscapes for the Internet of Things : A key enabler for Industry 4.0 ». In : *Advanced Engineering Informatics* 33 (1er août 2017), p. 208-229. ISSN : 1474-0346. DOI : 10.1016/j.aei.2016.11.007. URL : http://www.sciencedirect.com/science/article/pii/S1474034616301471 (visité le 20/09/2018) (cf. p. 7).

[Ute17] Martin UTERSINGER. « Le virus Petya a coûté plus d'un milliard d'euros aux entreprises ». In : *Le Monde* (7 nov. 2017). ISSN : 0395-2037. URL : https://www.lemonde.fr/pixels/article/2017/11/07/le-virus-petya-a-coute-plus-d-un-milliard-d-euros-aux-entreprises_5211421_4408996.html (visité le 27/11/2018) (cf. p. 6).

[VD16] Xavier VILAJOSANA et Mischa DOHLER. *Transmission of IPv6 Packets over LoRaWAN*. Internet-Draft draft-vilajosana-6lpwa-lora-hc-01. Work in Progress, Expired & archived. Internet Engineering Task Force, juin 2016. 11 p. URL : https://datatracker.ietf.org/doc/html/draft-vilajosana-6lpwa-lora-hc-01 (cf. p. 26).

[Vid+13] N. VIDGREN et al. « Security Threats in ZigBee-Enabled Systems : Vulnerability Evaluation, Practical Experiments, Countermeasures, and Lessons Learned ». In : *2013 46th Hawaii International Conference on System Sciences*. 2013 46th Hawaii International Conference on System Sciences. Jan. 2013, p. 5132-5138. DOI : 10.1109/HICSS.2013.475 (cf. p. 21).

[VP17] Mathy VANHOEF et Frank PIESSENS. « Key reinstallation attacks : Forcing nonce reuse in WPA2 ». In : *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*. ACM, 2017, p. 1313-1328 (cf. p. 24).

[VR19] Mathy VANHOEF et Eyal RONEN. *Dragonblood : A Security Analysis of WPA3's SAE Handshake*. Rapport technique 383. 2019, p. 16. URL : https://eprint.iacr.org/2019/383 (visité le 25/04/2019) (cf. p. 24).

[VT14] A. VARGHESE et D. TANDUR. « Wireless requirements and challenges in Industry 4.0 ». In : *2014 International Conference on Contemporary Computing and Informatics (IC3I)*. 2014 International Conference on Contemporary Computing and Informatics (IC3I). Nov. 2014, p. 634-638. DOI : 10.1109/IC3I.2014.7019732 (cf. p. 12).

[Wan+12] Junbo WANG et al. « A location-aware lifestyle improvement system to save energy in smart home ». In : *4th International Conference on Awareness Science and Technology*. 4th International Conference on Awareness Science and Technology. Août 2012, p. 109-114. DOI : 10.1109/iCAwST.2012.6469598 (cf. p. 10).

[Wan+13] M. WANG et al. « An IoT-based appliance control system for smart homes ». In : *2013 Fourth International Conference on Intelligent Control and Information Processing (ICICIP)*. 2013 Fourth International Conference on Intelligent Control and Information Processing (ICICIP). Juin 2013, p. 744-747. DOI : 10.1109/ICICIP.2013.6568171 (cf. p. 10).

[Wan+16a] K. Wang et al. « Green Industrial Internet of Things Architecture : An Energy-Efficient Perspective ». In : *IEEE Communications Magazine* 54.12 (déc. 2016), p. 48-54. ISSN : 0163-6804. DOI : 10.1109/MCOM.2016.1600399CM (cf. p. 11).

[Wan+16b] Shiyong Wang et al. « Implementing Smart Factory of Industrie 4.0 : An Outlook ». In : *International Journal of Distributed Sensor Networks* 12.1 (1er jan. 2016), p. 3159805. ISSN : 1550-1477. DOI : 10.1155/2016/3159805. URL : https://doi.org/10.1155/2016/3159805 (visité le 29/10/2018) (cf. p. 7).

[Wan+17] J. Wan et al. « A Manufacturing Big Data Solution for Active Preventive Maintenance ». In : *IEEE Transactions on Industrial Informatics* 13.4 (août 2017), p. 2039-2047. ISSN : 1551-3203. DOI : 10.1109/TII.2017.2670505 (cf. p. 11).

[Web+16] P. Weber et al. « IPv6 over LoRaWAN™ ». In : *2016 3rd International Symposium on Wireless Systems within the Conferences on Intelligent Data Acquisition and Advanced Computing Systems (IDAACS-SWS)*. 2016 3rd International Symposium on Wireless Systems within the Conferences on Intelligent Data Acquisition and Advanced Computing Systems (IDAACS-SWS). Sept. 2016, p. 75-79. DOI : 10.1109/IDAACS-SWS.2016.7805790 (cf. p. 26).

[Wel+09] E. Welbourne et al. « Building the Internet of Things Using RFID : The RFID Ecosystem Experience ». In : *IEEE Internet Computing* 13.3 (mai 2009), p. 48-55. ISSN : 1089-7801. DOI : 10.1109/MIC.2009.52 (cf. p. 8).

[Wey+15] M. Weyn et al. « DASH7 alliance protocol 1.0 : Low-power, mid-range sensor and actuator communication ». In : *2015 IEEE Conference on Standards for Communications and Networking (CSCN)*. 2015 IEEE Conference on Standards for Communications and Networking (CSCN). Oct. 2015, p. 54-59. DOI : 10.1109/CSCN.2015.7390420 (cf. p. 27).

[WL11] C. Wei et Y. Li. « Design of energy consumption monitoring and energy-saving management system of intelligent building based on the Internet of things ». In : *2011 International Conference on Electronics, Communications and Control (ICECC)*. 2011 International Conference on Electronics, Communications and Control (ICECC). Sept. 2011, p. 3650-3652. DOI : 10.1109/ICECC.2011.6066758 (cf. p. 10).

[WSJ17] M. Wollschlaeger, T. Sauter et J. Jasperneite. « The Future of Industrial Communication : Automation Networks in the Era of the Internet of Things and Industry 4.0 ». In : *IEEE Industrial Electronics Magazine* 11.1 (mar. 2017), p. 17-27. ISSN : 1932-4529. DOI : 10.1109/MIE.2017.2649104 (cf. p. 11, 12).

[WX17] X. Wu et L. Xie. « On the Wireless Extension of EtherCAT Networks ». In : *2017 IEEE 42nd Conference on Local Computer Networks (LCN)*. 2017 IEEE 42nd Conference on Local Computer Networks (LCN). Oct. 2017, p. 235-238. DOI : 10.1109/LCN.2017.15 (cf. p. 15).

[XCM12] Xiaoli Xu, Tao Chen et Mamoru Minami. « Intelligent fault prediction system based on internet of things ». In : *Computers & Mathematics with Applications*. Advanced Technologies in Computer, Consumer and Control 64.5 (1er sept. 2012), p. 833-839. ISSN : 0898-1221. DOI : 10.1016/j.camwa.2011.12.049. URL : http://www.sciencedirect.com/science/article/pii/S0898122111011059 (visité le 17/12/2018) (cf. p. 11).

[Xia+05] Yang Xiao et al. « Security services and enhancements in the IEEE 802.15.4 wireless sensor networks ». In : *GLOBECOM '05. IEEE Global Telecommunications Conference, 2005.* GLOBECOM '05. IEEE Global Telecommunications Conference, 2005. T. 3. Nov. 2005, 5 pp.–. DOI : 10.1109/GLOCOM.2005.1577958 (cf. p. 19).

[Xio+15] X. Xiong et al. « Low power wide area machine-to-machine networks : key techniques and prototype ». In : *IEEE Communications Magazine* 53.9 (sept. 2015), p. 64-71. ISSN : 0163-6804. DOI : 10.1109/MCOM.2015.7263374 (cf. p. 27).

[XS01] S. Xu et T. Saadawi. « Does the IEEE 802.11 MAC protocol work well in multihop wireless ad hoc networks ? » In : *IEEE Communications Magazine* 39.6 (juin 2001), p. 130-137. ISSN : 0163-6804. DOI : 10.1109/35.925681 (cf. p. 23).

[Xu+16] R. Xu et al. « A Software Defined Radio Based IEEE 802.15.4k Testbed for M2M Applications ». In : *2016 IEEE 84th Vehicular Technology Conference (VTC-Fall).* 2016 IEEE 84th Vehicular Technology Conference (VTC-Fall). Sept. 2016, p. 1-5. DOI : 10.1109/VTCFall.2016.7880880 (cf. p. 27).

[Xu12] Xun Xu. « From cloud computing to cloud manufacturing ». In : *Robotics and Computer-Integrated Manufacturing* 28.1 (1er fév. 2012), p. 75-86. ISSN : 0736-5845. DOI : 10.1016/j.rcim.2011.07.002. URL : http://www.sciencedirect.com/science/article/pii/S0736584511000949 (visité le 12/11/2018) (cf. p. 7).

[YSW16] C. Yang, W. Shen et X. Wang. « Applications of Internet of Things in manufacturing ». In : *2016 IEEE 20th International Conference on Computer Supported Cooperative Work in Design (CSCWD).* 2016 IEEE 20th International Conference on Computer Supported Cooperative Work in Design (CSCWD). Mai 2016, p. 670-675. DOI : 10.1109/CSCWD.2016.7566069 (cf. p. 11).

[Yu+11] I.-Kang Yu et al. « Method and systems for storing and accessing data in USB attached-SCSI (UAS) and bulk-only-transfer (BOT) based flash-memory device ». Brev. amér. 8060670B2. Super Talent Electronics Inc. 15 nov. 2011. URL : https://patents.google.com/patent/US8060670B2/en (visité le 06/05/2019) (cf. p. 13).

[Zan+14] A. Zanella et al. « Internet of Things for Smart Cities ». In : *IEEE Internet of Things Journal* 1.1 (fév. 2014), p. 22-32. ISSN : 2327-4662. DOI : 10.1109/JIOT.2014.2306328 (cf. p. 10).

[ZGC11] Deze Zeng, Song Guo et Zixue Cheng. « The web of things : A survey ». In : *JCM* 6.6 (2011), p. 424-438 (cf. p. 8).

[ZLZ15] K. Zhou, Taigang Liu et Lifeng Zhou. « Industry 4.0 : Towards future industrial opportunities and challenges ». In : *2015 12th International Conference on Fuzzy Systems and Knowledge Discovery (FSKD).* 2015 12th International Conference on Fuzzy Systems and Knowledge Discovery (FSKD). Août 2015, p. 2147-2152. DOI : 10.1109/FSKD.2015.7382284 (cf. p. 3).

[Zur15] Richard Zurawski, éd. *Industrial communication technology handbook.* Second edition. Industrial information technology series. OCLC : 935211357. Boca Raton London New York : CRC Press, Taylor & Francis Group, 2015. 1 p. ISBN : 978-1-138-07181-0 (cf. p. 12).