dossier.

Stille Intelligenz: IoT im Einsatz

Entwicklungen und Herausforderungen | Aus dem Alltag ist das Internet der Dinge kaum wegzudenken. Auch in der Energieversorgung ist die Technologie in vielen Anwendungen wie der Messtechnik weiter auf dem Vormarsch.

En toute discrétion : l'IoT en action

Développements et défis | L'Internet des objets fait de plus en plus partie de notre quotidien. Cette technologie trouve aussi un nombre croissant d'applications dans l'approvisionnement énergétique, notamment dans le secteur des techniques de mesure.

Extreme Miniaturisierung
Das IoT setzt zunehmend auf Kleinstgeräte. Der kleinste Rechner dieser zwei Generationen des Michigan Micro Motes M³ misst unter 1 mm³ und ist energieautark.

Miniaturisation à l'extrême
L'IoT fait de plus en plus appel à des dispositifs de très petite taille. Le plus petit ordinateur de ces deux générations de Michigan Micro Motes M³ mesure moins de 1 mm³ et est autonome en énergie.

Bild | Figure: Michael Simari, University of Michigan

MONIKA FREUNEK

Der Blick in eine beliebige Alltagsumgebung verrät es: Wir leben im Zeitalter der verteilten und allgegenwärtigen Intelligenz. Im Jahr 2021 verfügte der US-amerikanische Durchschnittshaushalt über 25 elektronische Geräte [1]. Die meisten dieser Geräte sind Teil des Internets der Dinge, auch als Internet of Things (IoT) bekannt. Doch was ist das IoT genau, wie ist der heutige Stand der Technik und welche Rolle spielt es in der Energieversorgung?

Aus technischer Sicht umfasst ein IoT-Gerät einen Prozessor, einen Zeitgeber, einen Datenspeicher, eine Kommunikationseinheit und einen Sensor und/oder Aktor **(Bild 1)**. Die konkrete Ausführung richtet sich nach den Anforderungen der Anwendung, etwa an die Sensorgenauigkeit, den tolerierten Jitter des Zeitgebers, die Prozessorleistung oder etwaige Maximalwerte für Volumen und Energiebedarf. IoT-Geräte werden auch als Feldknoten oder Edge Nodes bezeichnet. Über eine Netzwerkverbindung erfolgt die Kommunikation von Mess- und Steuerdaten mit der jeweiligen Anwendungssoftware. Diese kann sich vor Ort auf einem sogenannten Edge Computing Device befinden oder etwa in einem Rechenzentrum eines Cloud-Dienstes. Das IoT besteht also nicht aus einem einzigen System, sondern aus mehreren Netzwerken, die sich in Datenprotokoll, Kommunikationsweg und -geschwindigkeit teilweise signifikant unterscheiden.

Entwicklungsgeschichte

Als erstes bekanntes IoT-Gerät gilt eine Cola-Maschine der Carnegie Mellon University in den USA. Um unnötige Wege durch das Gebäude zu einem leeren oder gar mit lauwarmem Inhalt gefüllten Automaten zu vermeiden, rüsteten Studenten das Gerät 1982 mit Sensorik sowie einem Arpanet-Anschluss aus [2].

Die Vision des verteilten Rechnens in grösserem Ausmass entstand rund zehn Jahre später. Der amerikanische Computerwissenschaftler Mark Weiser sah nach dem Schritt vom Grossrechner zum Personal Computer den Beginn einer dritten Computerära [3]. Computer würden in ihrer Grösse an die Aufgabe angepasst variieren und weitestgehend mit der Umgebung verschmelzen. Ohne Aufmerksamkeit zu erregen oder zu benötigen, würden sie Informationen sammeln und mittels Kommunikationsnetzen zur Unterstützung von Prozessen zur Verfügung stellen. Diese Art des Computings wurde auch als stilles oder ubiquitäres Computing bezeichnet. Mit der steigenden Verbreitung des Internets setzte sich der Begriff «Internet der Dinge» durch. Etwa zeitgleich begannen in den USA im Auftrag der Defense Advanced Research Projects Agency (Darpa) mit «Smart Dust» und «Energy Harvesting» zwei ambitionierte Forschungsprojekte: die Entwicklung drahtloser Sensorknoten mit einem Maximalvolumen von 1 mm³ und eine vollständig autarke Energieversorgung drahtloser Sensorik über die Umgebungsenergie. Anders als in den weitestgehend verkabelten Anwendungen der Energiebranche wird in diesem Bereich der Sensor- und Computertechnik bis heute um jedes Bit und jedes Joule gekämpft.

Il suffit de regarder autour de soi pour s'en convaincre : nous vivons à l'ère de l'intelligence distribuée et omniprésente. En 2021, le ménage américain moyen disposait de 25 appareils électroniques [1], la plupart constituant des éléments de l'Internet des objets, ou Internet of Things (IoT). Mais qu'est-ce que l'IoT exactement, quelles sont ses dernières avancées et quel rôle joue-t-il dans l'approvisionnement en énergie ?

D'un point de vue technique, un dispositif IoT comprend un processeur, une horloge, une mémoire pour le stockage des données, une unité de communication ainsi qu'un capteur et/ou un actionneur (figure 1). La conception concrète dépend des exigences relatives à l'application considérée, par exemple en matière de précision du capteur, de tolérance de gigue (jitter) de l'horloge, de puissance du processeur ou d'éventuelles valeurs maximales liées au volume du dispositif et à sa consommation d'énergie. Les dispositifs IoT sont également appelés nœuds de périphérie ou « edge nodes ». La communication des données de mesure au logiciel de l'application ainsi que des données de contrôle correspondantes s'effectue via une connexion réseau. Le logiciel peut se trouver sur place, sur un dispositif appelé « edge computing device », ou dans un centre de données d'un service cloud, par exemple. L'IoT n'est donc pas composé d'un seul système, mais de plusieurs réseaux parfois très différents en termes de protocole de données ainsi que de mode et de vitesse de communication.

Historique du développement

Le premier appareil IoT recensé était un distributeur de Coca-Cola de la Carnegie Mellon University aux États-Unis : en 1982, des étudiants avaient équipé ce dernier de capteurs ainsi que d'une connexion Arpanet, afin d'éviter des déplacements inutiles à travers le bâtiment jusqu'à un automate vide ou au contenu tiède [2].

Une vision du calcul distribué à plus grande échelle est apparue une dizaine d'années plus tard. Après le passage de l'ordinateur central à l'ordinateur personnel, l'informaticien américain Mark Weiser avait dès lors prévu le début d'une troisième ère informatique [3]. La taille des ordinateurs varierait, selon lui, en fonction de la tâche à accomplir et ceux-ci se fondraient en grande partie dans l'environnement. Sans attirer l'attention et sans avoir besoin de le faire, ils collecteraient des informations afin de soutenir des processus et les mettraient à disposition via des réseaux de communication. Ce type d'informatique était alors également appelé informatique ubiquitaire. Avec l'essor de l'Internet, le terme « Internet des objets » a toutefois fini par s'imposer. À peu près au même moment, deux projets de recherche ambitieux, « Smart Dust » et « Energy Harvesting », ont été lancés aux États-Unis sur mandat de la Defense Advanced Research Projects Agency (Darpa) : ils concernaient le développement de nœuds de capteurs sans fil d'un volume maximal de 1 mm³ ainsi que d'une alimentation en énergie entièrement autonome des capteurs sans fil via l'énergie

Gemeinsam mit den Fortschritten in der Mikrosystemtechnik erzielten die bald weltweiten Forschungsarbeiten rasante und immer wieder abenteuerliche Fortschritte. So gelang die Entwicklung des sparsamsten Prozessors der Welt mit einem Energiebedarf von wenigen Picojoule [4], die Entwicklung von intelligenten Fussböden und Schuhen, die Bewegungsenergie zum Betrieb von IoT-Geräten nutzen, und das junge Feld der Hocheffizienzphotovoltaik für Innenräume und miniaturisierte Systeme entstand. Tatsächlich sind die oben genannten Forschungsziele inzwischen alle erreicht worden. Der kleinste Computer der Welt, der Michigan Micro Mote M³, hat ein Volumen von rund 1 mm³, ist mittels eines speziellen Photovoltaikmoduls energieautark und kann Messungen durchführen und versenden. **Bild 2** zeigt den M³ im Einsatz in der biologischen Feldforschung [5].

Lange bedeutete der massenhafte Einsatz von IoT-Geräten aufwendige und individuelle Datenauswertungen, die zudem rasch an die Grenzen sinnvoll vertretbarer Rechenkapazitäten kamen. Die vereinfachte Verfügbarkeit von Massendatenverarbeitung im Rahmen der Entwicklungen von Clouddiensten, Maschinenlernen und Künstlicher Intelligenz stellt für das IoT einen Technologieschub dar, an dessen Anfang wir erst stehen.

IoT in der Energiewelt

Im Energiebereich wie auch im breiten industriellen und gesellschaftlichen Umfeld standen lange die Entwicklungen in der Kommunikationstechnik im Vordergrund, allen voran die zunehmende Verfügbarkeit von Internet und Mobilfunktechnologien. Die Vernetzung machte ein neues Betriebskonzept möglich: das intelligent gesteuerte Netz, auch als Smart Grid bekannt. Schon einfache Umsetzungen bedingen Informationen über Energiemengen und deren Handelszeitpunkt und -ort und setzen damit in der Regel auf IoT-Technik. Anwendungen wie Smart Homes und Elektromobilität benötigen Sensorik und Aktorik, die via Smartphone, Computer oder auch Drittanbieter gesteuert werden. Diese Systeme sollen im Rahmen des Smart Grids langfristig mit den Systemen der Energieversorgungsunternehmen (EVU) vereint werden und sind es physikalisch bereits über den bezogenen Strom. Das Internet der Dinge ist also ein fester Bestandteil unserer Energieversorgung.

Anders als gerade beim Smart Grid oft schematisch dargestellt, erfordern individuelle Aufgaben zumeist individuelle IoT-Lösungen. Beispielsweise ist die Vernetzung von Smart-Home-Systemen im Kontext von Steueraufgaben durch ein EVU technisch wie regulatorisch komplex. So gelten für die eingesetzte Messtechnik an der Handelsschnittstelle zum Kunden andere gesetzliche Vorgaben hinsichtlich Sicherheit und Genauigkeit als für Technik im privaten Einsatz. Ebenso unterliegen Datenflüsse den Vorgaben des Unbundlings und können so durchaus eigene Messtechnik nötig machen. Es besteht also eine Vielfalt von Technologielösungen und -generationen, die nebeneinander betrieben werden.

ambiante. Dans ce domaine de la technologie des capteurs et de l'informatique, on se bat encore aujourd'hui pour chaque bit et chaque joule, ce qui n'est, par contre, pas nécessaire pour les applications généralement câblées du secteur de l'énergie.

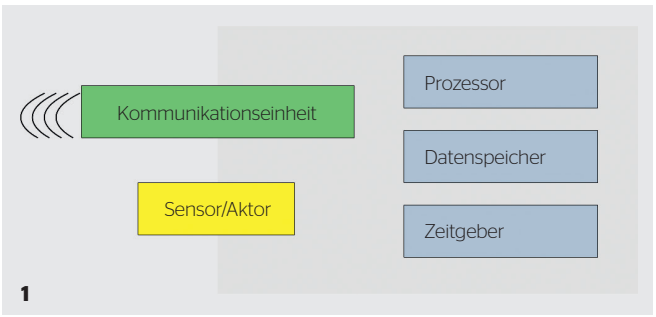
Les progrès réalisés dans le domaine de la technologie des microsystèmes et les travaux de recherche effectués, désormais bientôt à l'échelle mondiale, ont permis des avancées fulgurantes et souvent audacieuses. C'est ainsi qu'il a été possible de développer le processeur le plus économe au monde, dont la consommation d'énergie ne dépasse pas quelques picojoules [4], ainsi que des chaussures et des sols intelligents qui utilisent l'énergie de nos mouvements pour faire fonctionner des dispositifs IoT. Et c'est également ainsi que le domaine naissant du photovoltaïque à haut rendement pour les espaces intérieurs et les systèmes miniaturisés a pu voir le jour. De fait, les objectifs de recherche susmentionnés ont désormais tous été atteints. Le plus petit ordinateur du monde, le Michigan Micro Mote M³, affiche un volume d'environ 1 mm³, il est autonome en énergie grâce à un module photovoltaïque spécial, et il est à même d'effectuer et d'envoyer des mesures. La figure 2 montre le M³ en action dans le cadre de recherches biologiques sur le terrain [5].

Pendant longtemps, l'utilisation massive de dispositifs IoT a impliqué des analyses de données individuelles et complexes qui ont, en outre, rapidement atteint les limites raisonnablement acceptables en matière de capacités de calcul. La mise à disposition simplifiée de possibilités de traitement de quantités importantes de données dans le cadre du développement des services cloud, de l'apprentissage automatique et de l'intelligence artificielle représente une avancée technologique majeure pour l'IoT, et nous n'en sommes qu'au début.

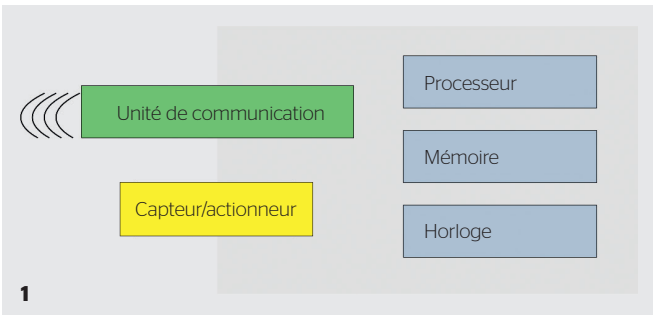
L'IoT dans le domaine de l'énergie

Dans le secteur de l'énergie, tout comme dans les domaines industriel et social au sens large, l'accent a longtemps été mis sur les développements des technologies de la communication, et en particulier sur la disponibilité croissante d'Internet et des technologies mobiles. La mise en réseau a rendu possible un nouveau concept d'exploitation : le réseau intelligent, également connu sous le nom de smart grid. Même les mises en œuvre les plus simples nécessitent des informations relatives aux quantités d'énergie ainsi qu'au moment et au lieu où elles sont échangées, et reposent donc généralement sur la technologie IoT. Les applications telles que la domotique (smart home) et l'électromobilité nécessitent des capteurs et des actionneurs contrôlés via un smartphone, un ordinateur ou un prestataire tiers. Dans le cadre du smart grid, ces systèmes devront à long terme rejoindre les systèmes des entreprises d'approvisionnement en énergie (EAE) et ils le font déjà physiquement via l'électricité soutirée. L'Internet des objets fait donc partie intégrante de notre approvisionnement en énergie.

Contrairement à ce qui est souvent schématisé dans le cas du smart grid, les tâches individuelles nécessitent



1



1

2

1 Grundkomponenten eines IoT-Geräts.

Composants de base d'un dispositif IoT.

2 IoT für das Schneckenhaus – der Michigan Micro Mote M^3 im Einsatz bei der Feldforschung.

IoT domestique à l'échelle de l'escargot – le Michigan Micro Mote M^3 utilisé pour la recherche sur le terrain.

Bilder | Figures: Monika Freunek / Cindy Bick/University of Michigan

Einsatzgebiete

Beispiele von IoT-Systemen im Energiebereich umfassen Smart Meter, Drohnen- und Satellitensysteme zum Einsatz in Assetmanagement und Betrieb, GPS-gestützte Lösungen in Logistik, Dispatching und Flottenführung, meteorologische Sensorik in der Überwachung und Steuerung von Photovoltaik- und Windkraftanlagen oder Videokameras im Sicherheitsbereich. Im Bürobereich findet sich IoT-Technik in elektronischen Zutrittssystemen, intelligenten Kaffeemaschinen und Getränkeautomaten, Smartphones und Smartwatches. Im privaten Bereich sind typische Beispiele Sprachassistenten wie Alexa, intelligente Zutrittssysteme und Überwachungstechnik, Roboter in Haushalt und Garten sowie Anlagen der Prosumertechnik. Moderne Fahrzeuge setzen eine Vielzahl von IoT-Geräten in Routenführung, Fehlerdiagnostik, Wartung und Fahrassistenz ein.

Fragen der Sicherheit

Über gemeinsam genutzte Schnittstellen von verschiedenen IoT-Systemen sind verschiedene Netzwerke verbunden. Diese Vermaschung von IoT- und anderen Computersystemen ist nur mit bewusstem Aufwand vermeidbar. Werden etwa Smartphones und Smartwatches sowohl im Betriebskontext als auch im privaten Bereich genutzt, gibt es eine Schnittstelle zwischen den Systemen des EVU und privaten Systemen. Gerade diese Vermaschungen sind es, die IoT-Systeme aus Sicht von Angreifern im Cyberraum so attraktiv machen. So demonstrierten Sicherheitsforscher die Steuerung eines Smart Homes mittels eines von aussen gehackten intelligenten Fernsehers. Umgekehrt wurden vielfach Mailprogramme als Eintrittspforte in die physische Welt genutzt, um Steuerungen zu manipulieren oder zu verschlüsseln.

Verschärft wird diese Ausgangslage durch das sogenannte Internet of Forgotten Things (IoFT): Viele IoT-Geräte sind schon lange in Betrieb. Einige sind Bestandsgeräte mit nachgerüsteter Kommunikationstechnik, die damit teilweise unbeabsichtigt zum IoT-System geworden sind. Zudem verfügen Geräte erster Generationen oft nicht über die Möglichkeit, sichere Passwörter nach aktuellen Standards, Zweifaktor-Authentifikation oder Benutzermanagement umzusetzen. Entsprechend gross ist inzwischen der weltweite Bestand unzureichend geschützter IoT-Systeme.

Die Abgrenzung zwischen der sogenannten Operational Technology (OT), IoT und klassischer Informations- und Kommunikationstechnik (IKT) ist dabei nicht immer trivial. Aus Sicht der Informationssicherheit ist es einfach: Alles mit einer Kommunikationsadresse und einem Prozessor unterliegt einem entsprechenden Schutzbedarf und muss laufend aktuell inventarisiert sein. Der Schutz von IoT-Geräten selbst neuster Generation stellt die technische sowie die regulatorische Welt vor eine der grössten Herausforderungen unserer Zeit. Aus Sicht von Energieversorgern stehen hier besonders Bestände erster Generationen des IoT im Vordergrund sowie die für den Energiebereich typischen langen Betriebszeiten von Geräten. Dies sind **généralement des solutions IoT individuelles. Par exemple, la mise en réseau de systèmes de domotique dans le contexte de tâches de contrôle par une EAE se révèle complexe autant sur le plan technique que réglementaire. Les techniques de mesure utilisées à l'interface commerciale avec les clients sont notamment soumises à d'autres exigences légales en matière de sécurité et de précision que celles dédiées à un usage privé. De même, les flux de données doivent répondre aux exigences du dégroupage et peuvent ainsi nécessiter des techniques de mesure qui leur sont propres. Il existe donc une multitude de solutions et de générations de technologies exploitées en parallèle.**

Domaines d'application

Les compteurs intelligents (smart meters), les systèmes de drones et de satellites utilisés pour la gestion des actifs et l'exploitation, les solutions GPS pour la logistique, le dispatching et la gestion de flottes, les capteurs météorologiques pour la surveillance et le contrôle des installations photovoltaïques et éoliennes, ou encore les caméras utilisées dans le domaine de la sécurité sont autant d'exemples de systèmes IoT exploités dans le secteur de l'énergie. Dans les bureaux, la technologie IoT est présente dans les systèmes d'accès électroniques, les machines à café et distributeurs de boissons intelligents, les smartphones et les montres intelligentes. Dans le domaine privé, des exemples typiques sont les assistants vocaux tels qu'Alexa, les systèmes d'accès intelligents et la technologie de surveillance, les robots domestiques et de jardinage, ainsi que les installations liées à la technologie des prosommateurs. Les véhicules modernes utilisent, eux aussi, une multitude de dispositifs IoT pour le guidage routier, le diagnostic des défaillances, la maintenance et l'assistance à la conduite.

Questions relatives à la sécurité

Différents réseaux sont connectés via des interfaces utilisées par divers systèmes IoT. Ce maillage de systèmes IoT et d'autres systèmes informatiques ne peut être évité qu'au prix d'un effort délibéré. Par exemple, si des smartphones et des montres intelligentes sont utilisés à la fois dans le contexte de l'entreprise et dans la sphère privée, il existe dès lors une interface entre les systèmes des EAE et les systèmes privés. C'est précisément ce maillage qui rend les systèmes IoT des cibles si attrayantes pour les cyberattaques. Des chercheurs en sécurité ont ainsi démontré qu'il était possible de contrôler une maison intelligente au moyen d'une smart TV piratée de l'extérieur. D'un autre côté, les programmes de messagerie ont souvent été utilisés comme point d'entrée dans le monde physique pour manipuler ou crypter des commandes.

Cette situation de départ est aggravée par ce que l'on appelle l'Internet des objets oubliés (Internet of Forgotten Things, IoFT). En effet, de nombreux dispositifs IoT sont en service depuis longtemps : certains sont des appareils existants dont la technologie de communication a été

Zeiträume, in denen Technologie altert und damit eine zunehmende Wahrscheinlichkeit für Schwachstellen aufweist. Weiter gilt es, die steigende Gewichtung von faktisch mit den Infrastrukturen von Energieversorgern vernetzten, privat betriebenen Elementen regulatorisch und sicherheitstechnisch ausreichend abzudecken.

Grundsätzlich erzeugt jede Erhebung, Kommunikation und Speicherung von Information einen potenziellen Schutzbedarf und kostet Energie. Die aktuelle Frage des IoT ist weniger die Machbarkeit von Lösungen, sondern der intelligente Einsatz der Technik. Gleichzeitig gilt es, den Nachholbedarf in der Sicherung auch bereits installierter Systeme sowie hinsichtlich der regulatorischen Rahmenbedingungen abzudecken. Erste Entwicklungen in diese Richtung umfassen den Cybersecurity Improvement Act 2022 in den USA oder die IoT-Zertifizierung des deutschen BSI.

Längst stehen die nächsten Generationen von IoT-Systemen in den Startlöchern, z. B. mit der Erforschung von «neuronalem Staub», in dem mit Computern vernetzte Insekten als Drohnenschwärme Rechenoperationen durchführen. Die nächste Herausforderung des IoT wird sein, dieses zum Nutzen aller in die Gesellschaft zu implementieren und rechtzeitig die richtigen Betriebsvoraussetzungen auch regulatorischer Art zu schaffen.

Referenzen | Références

[1] www.reuters.com/technology/smart-devices-get-pandemic-boost-us-households-deloitte-survey-2021-06-09.
[2] www.cs.cmu.edu/~coke.
[3] M. Weiser, «The computer for the 21st Century», Scientific American, 265(3), pp. 75–84, 1991.
[4] M. Seok et al., «The Phoenix Processor: A 30 pW Platform for Sensor Applications», IEEE Symposium on VLSI Circuits (VLSI-Symp), Invited Paper to the IEEE Journal of Solid-State Circuits (JSSC), Special Issue on VLSI Circuits, pp. 188–189, 2008.
[5] C.S. Bick, I. Lee, T. Coote et al., «Millimeter-sized smart sensors reveal that a solar refuge protects tree snail Partula hyalina from extirpation», Commun. Biol. 4, 744, 2021.

Autorin | Auteure

Dr.-Ing. **Monika Freunek** ist Geschäftsführerin der Lighthouse Science Consulting and Technologies Inc., Kanada.
Dr **Monika Freunek** est directrice de Lighthouse Science Consulting and Technologies Inc., au Canada.
→ Lighthouse SCT, New Brunswick, Canada
→ monika.freunek@lighthouse-sct.com

mise à jour et qui sont donc devenus, parfois involontairement, des systèmes IoT. De plus, les appareils de première génération ne disposent souvent pas de la possibilité de mettre en œuvre des mots de passe sécurisés selon les normes actuelles, une authentification à deux facteurs ou une gestion des utilisateurs. Le nombre de systèmes IoT insuffisamment protégés dans le monde est par conséquent élevé.

La distinction entre les technologies opérationnelles (OT), l'IoT et les technologies de l'information et de la communication (TIC, ou ICT) classiques n'est pas toujours triviale. Du point de vue de la sécurité de l'information, c'est simple : tout ce qui possède une adresse de communication et un processeur est soumis à un besoin de protection correspondant et doit faire l'objet d'un inventaire continuellement actualisé. La protection des dispositifs IoT, même de la dernière génération, constitue l'un des plus grands défis de notre époque pour les domaines technique et réglementaire. Du côté des fournisseurs d'énergie, les stocks des premières générations de dispositifs IoT se trouvent en première ligne, tout comme les longues durées d'exploitation des équipements, typiques du secteur de l'énergie. Il s'agit de laps de temps au cours desquels la technologie vieillit et est donc soumise à une probabilité croissante d'apparition de vulnérabilités. En outre, il convient de couvrir suffisamment sur les plans réglementaire et sécuritaire la part croissante d'éléments exploités de manière privée qui sont aussi connectés aux infrastructures des fournisseurs d'énergie.

En principe, toute collecte, toute communication et tout stockage d'informations génère un besoin potentiel de protection et coûte de l'énergie. La question à laquelle l'IoT doit actuellement répondre n'est pas tant la capacité à réaliser des solutions que l'utilisation intelligente de la technologie. Parallèlement, il convient de combler le retard en termes de sécurité, y compris pour les systèmes déjà installés, ainsi qu'en matière de conditions-cadres réglementaires. Les premiers développements dans ce sens comprennent le Cybersecurity Improvement Act 2022 aux États-Unis, ou la certification IoT du BSI (Bundesamt für Sicherheit in der Informationstechnik), l'Office fédéral de la sécurité des technologies de l'information allemand.

Les prochaines générations de systèmes IoT se trouvent depuis longtemps dans les starting-blocks. Un exemple : les recherches réalisées dans le domaine de la « poussière neuronale », dans lequel des insectes, ou plutôt des essaims de drones, connectés à des ordinateurs effectuent des opérations de calcul. Le prochain défi de l'IoT consistera à implémenter ce dernier pour le bénéfice de tous au sein de la société et à créer à temps les conditions d'exploitation appropriées, y compris sur le plan réglementaire.