LIVRE BLANC

# MQTT - Permettre la connectivité des périphériques de bordure à l'ère de l'IIoT

**Chase Shih**
*Chef de produit Moxa*

MOXA®

## Résumé

*Bien que le protocole MQTT existe depuis près de trois décennies, sa conception le rend idéal pour les applications IIoT (Internet Industriel des Objets), la dernière tendance en matière d'automatisation. Cela s'avère particulièrement vrai pour les applications qui mettent l'accent sur la « notification active » dans laquelle les périphériques ne fournissent des données que lorsque cela est nécessaire, par opposition à la « notification passive » dans laquelle les périphériques sont interrogés à intervalles réguliers. La conception broker/client de MQTT élimine la nécessité pour tous les périphériques du système d'être en ligne en même temps. Les clients (c'est-à-dire les « périphériques » ou les « objets ») communiquent directement avec l'agent (ou broker) qui joue le rôle d'intermédiaire pour transmettre les messages entre les clients.*

## Préface

L'amélioration de la qualité de vie des personnes a toujours été l'une des principales motivations pour rechercher de nouvelles et meilleures améliorations technologiques. En outre, avec la poussée actuelle pour connecter de plus en plus de périphériques à Internet, le développement de meilleurs produits pour les applications dites IoT constitue aujourd'hui l'un des sujets les plus brulants. L'un des plus grands défis auxquels sont confrontés les ingénieurs de l'IoT industriel (abrégé IIoT) est que les « objets », souvent appelés « périphériques de bordure », n'ont pas toujours accès à une connexion filaire ou sans fil stable. Étant donné que les périphériques de bordure fournissent des données (généralement par intermittence) à un système central, la manière de collecter les données de ces périphériques constitue une préoccupation majeure. Plusieurs protocoles, dont MQTT, AMQP et CoAP, sont des candidats possibles pour répondre aux exigences de connexion IIoT. Toutefois, le protocole MQTT est devenu le premier choix pour la plupart des applications IIoT. Si l'on se réfère à la figure 1 ci-dessous, plus de la moitié des développeurs IoT utilisent MQTT comme protocole de communication, ce qui démontre clairement que MQTT est le meilleur protocole pour les applications IoT.



Moxa est un fournisseur incontournable de solutions de connectivité de pointe, de mise en réseau industriel et d'infrastructure réseau pour la mise en place de l'Internet Industriel des Objets. Fort de plus de 30 ans d'expérience dans le secteur industriel, Moxa a connecté plus de 50 millions de périphériques dans le monde et met un réseau de distribution et d'assistance au service de ses clients dans plus de 70 pays. Moxa fournit au secteur industriel des réseaux fiables et des relations clients sincères pour les infrastructures de communication industrielle et lui procure une valeur commerciale durable. Vous trouverez des informations sur les solutions Moxa à l'adresse www.moxa.com.

**Comment contacter Moxa**
Tél : 1-714-528-6777
Fax : 1-714-528-6778

Reliable Networks ▲ Sincere Service

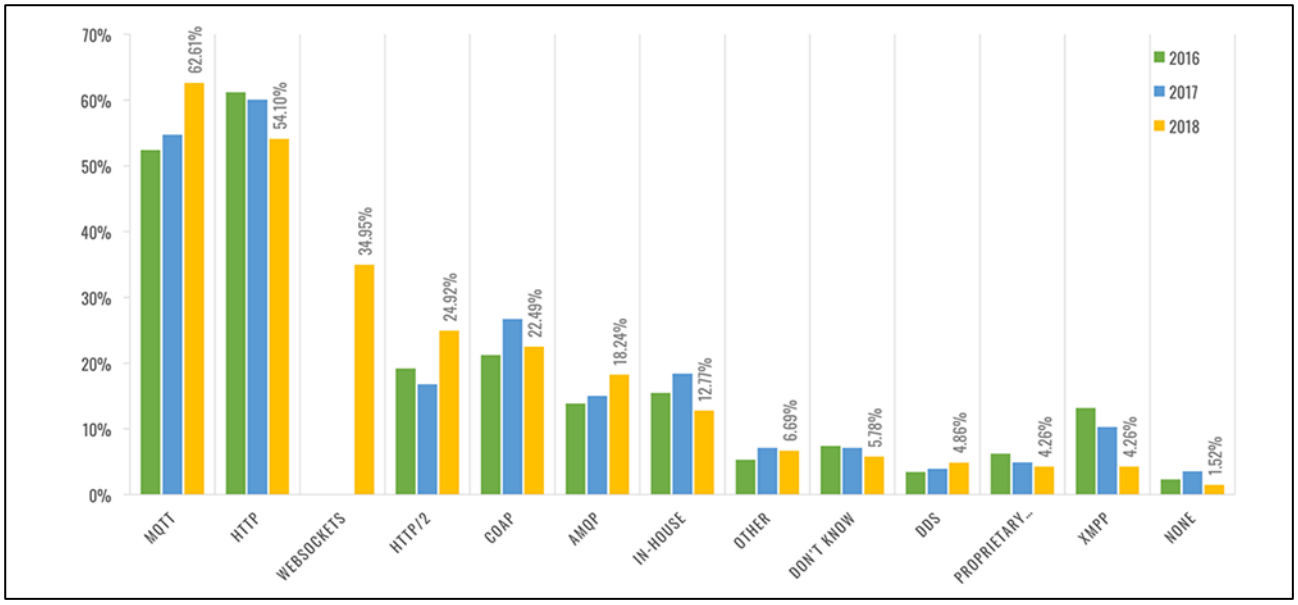


Figure 1. MQTT est le principal protocole pour les applications IoT.



## Qu'est-ce que le protocole MQTT ?

Le protocole de messagerie MQTT a été développé en 1999 par IBM et Cirrus Link. En 2013, il a été accepté comme norme ISO, à partir de la version 3.1. MQTT utilise un modèle publication/abonnement (voir la figure 2) pour échanger des messages. Comme illustré sur la figure, un système MQTT comprend un agent et plusieurs clients, ces derniers pouvant être soit des éditeurs, soit des abonnés. Les éditeurs envoient des données à l'agent sous la forme de paquets MQTT, composés d'un « sujet » et d'une « charge utile ». L'agent distribue ensuite les données aux abonnés en fonction des sujets pour lesquels ils ont exprimé un intérêt.

Le protocole MQTT ne spécifie pas de format standard pour la transmission des données, bien qu'il soit courant que les applications utilisent le protocole JSON ou du texte brut. Comparé à d'autres protocoles, MQTT présente des avantages qui en font un outil idéal pour les applications IoT.


Figure 2. Modèle publication/abonnement

### Modèle de messagerie publication/abonnement

Par rapport aux autres protocoles de type demande/réponse, le modèle publication/abonnement utilisé par MQTT permet aux développeurs IoT de résoudre certains problèmes de connexion courants. Par exemple, les modèles demande/réponse exigent que le client et le serveur soient en ligne en même temps pour garantir la transmission et la réception des données. Cependant, en particulier pour les applications IIoT, il peut s'avérer impossible pour les périphériques de maintenir une connexion suffisamment forte au réseau pour recevoir

les données requises et, par conséquent, le modèle demande/réponse n'est pas adapté à ces applications.

Le modèle publication/abonnement de MQTT est taillé sur mesure pour les situations dans lesquelles il n'est pas garanti que les périphériques soient connectés au réseau au même moment. L'agent MQTT s'avère essentiel à cet égard. L'agent agit comme un centre d'information en acceptant les données qui lui sont envoyées par des clients désignés comme « éditeurs », puis en les envoyant à des clients désignés comme « abonnés ». Lorsque l'agent envoie les données à un abonné, il vérifie d'abord si le client cible est en ligne ou non. Si ce n'est pas le cas, l'agent peut conserver les données jusqu'à ce que l'abonné soit en ligne, puis les envoyer. L'un des avantages de cette stratégie est que seul l'agent doit être en ligne en permanence. Les clients, qu'ils soient éditeurs ou abonnés, ne doivent être en ligne que lorsqu'une connexion est disponible ou qu'ils ont besoin d'envoyer ou de recevoir des données.

### En fonction des événements

Lorsqu'ils utilisent un modèle publication/abonnement, les clients MQTT ne publient des données vers l'agent que lorsque certaines conditions sont remplies (par exemple, un signal d'avertissement peut indiquer que la température d'un périphérique particulier est trop élevée). Une autre façon de décrire ce type de fonctionnement est que les clients mettent activement à jour les données, au lieu d'attendre passivement qu'un autre périphérique demande les données. Pour les applications IoT, les frais de communication sont facturés en fonction du nombre de paquets de données transmis. Par rapport à un modèle demande/réponse, MQTT permet de réaliser des économies puisque seule une communication unidirectionnelle est nécessaire pour effectuer les transmissions de données.

### Communication plusieurs à plusieurs

L'un des principaux avantages de MQTT est qu'un modèle publication/abonnement peut être utilisé pour établir facilement une communication plusieurs à plusieurs. Le concept de machine à machine (M2M), qui est une réalisation de la communication plusieurs à plusieurs, constitue l'un des sujets les plus brûlants de l'IIoT. Dans les applications M2M d'usine, les machines de chaque station partagent leurs propres états de processus avec les machines des autres stations. Cette manière de partager des informations sert à automatiser l'optimisation de la production sans que les opérateurs aient besoin d'intervenir manuellement. Puisque MQTT est utilisé pour implémenter la communication M2M, les machines n'ont qu'à établir une connexion avec l'agent au lieu de se connecter directement les unes aux autres, ce qui permet de gagner un temps considérable sur le « handshaking ». Étant donné qu'un seul agent est dédié au traitement de la communication entre toutes les machines, la transmission des données est plus fiable.

### Conception de QoS

Le protocole MQTT utilise trois niveaux de QoS pour hiérarchiser les données :

- **QoS 0 : une fois au plus**
  Dans ce cas, le client publie un message à l'agent une seule fois. L'agent n'accuse pas réception du message et ne fournit au client aucune notification concernant la communication avec les abonnés. La seule garantie est que l'éditeur sait qu'il a envoyé le message. Cependant, il ne sait pas si l'agent ou les abonnés ont reçu le message. Bien

que la QoS 0 soit de loin la politique de qualité de service la plus rapide, elle est également la moins fiable.

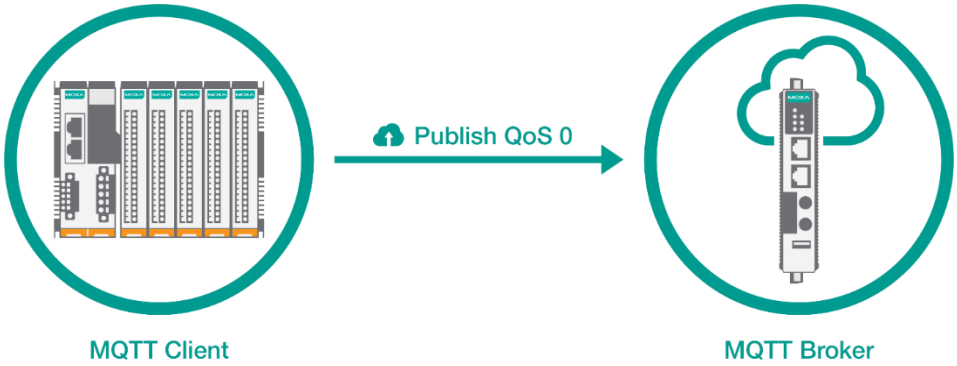


Figure 3. QoS 0 : une fois au plus

- **QoS 1 : une fois au moins**
  Dans ce cas, lorsqu'un client publie un message à l'agent, il s'attend à ce que l'agent accuse réception ou non du message par un client. Si l'éditeur ne reçoit pas d'accusé de réception de l'agent dans un intervalle de temps prédéfini, il republiera le message encore et encore jusqu'à ce que l'accusé de réception soit reçu. Par rapport à QoS 0, QoS 1 est plus fiable, même si vous pouvez vous attendre à une plus grande lenteur dans le temps.

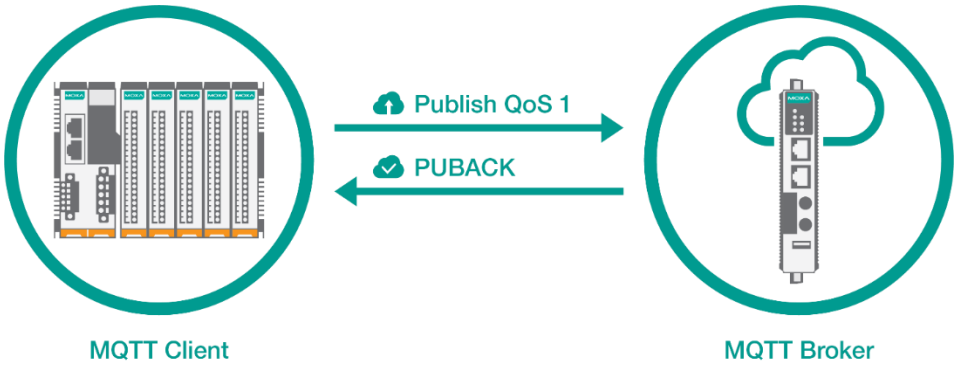


Figure 4. QoS 1 : une fois au moins

- **QoS 2 : une fois exactement**
  Dans ce cas, le client et l'agent échangent quatre messages. Le client publie d'abord les données auprès de l'agent, puis le client et l'agent échangent trois messages (PUBREC, PUBREL et PUBCOMP) pour s'assurer que les données ne sont livrées qu'une seule fois. QoS 2 est la politique de qualité de service MQTT la plus fiable, mais aussi la plus lente.

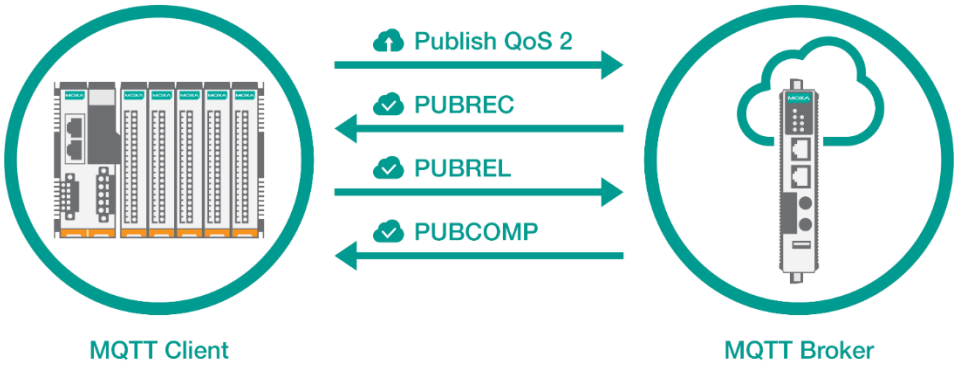


Figure 5. QoS 2 : une fois exactement

### Sécurité

La sécurité est une préoccupation majeure pour les applications IIoT. Avec un nombre croissant de périphériques connectés à Internet, savoir comment minimiser les risques de piratage des données est une priorité absolue. La figure 6 indique clairement que la sécurité est de loin la principale préoccupation pour les applications IIoT. En ce qui concerne MQTT, l'agent prend en charge les noms de compte et les mots de passe pour empêcher les clients non autorisés de se connecter à l'agent pour s'abonner à des sujets. MQTT prend également en charge l'encryptage TLS pour les transmissions de données afin de minimiser considérablement les risques de piratage des données pendant la transmission.

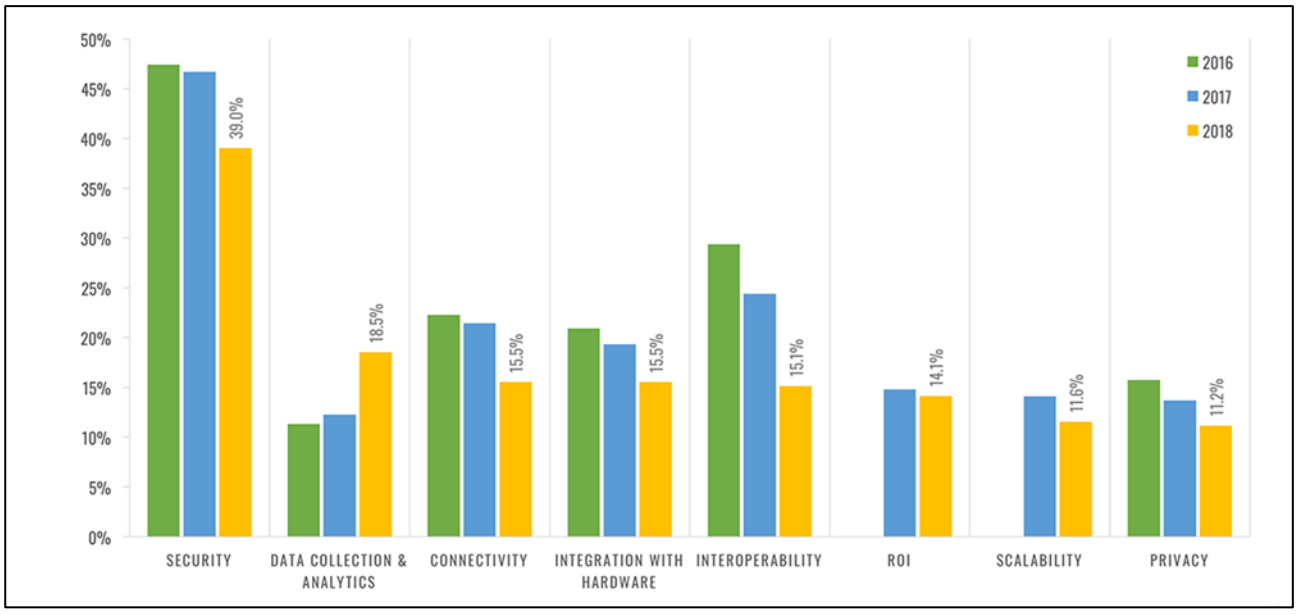


Figure 6. La sécurité est la principale préoccupation lors de l'adoption de l'IoT.



## Architecture d'application MQTT

Comme nous l'avons souligné au début de cet article, les applications traditionnelles d'OT sont réaménagées en applications IIoT qui utilisent le protocole populaire MQTT. Deux grandes architectures de système sont utilisées.

### Connexion directe au cloud

La plupart des services de cloud public (AWS, Azure, Google Cloud, Alibaba Cloud, etc.) prennent en charge le protocole MQTT pour permettre aux périphériques de bordure de se connecter directement au cloud. Pour rester compétitifs et contribuer à façonner l'avenir du secteur, les services de cloud doivent au moins offrir les avantages suivants :

- Gain de temps

  Étant donné que le service de cloud assure la maintenance du matériel (serveur cloud, processeur, mémoire, etc.), le fait de laisser ces tâches de maintenance plus spécialisées aux experts IT du service de cloud permet aux utilisateurs de consacrer plus de temps au développement de leurs propres solutions.

- Service ininterrompu

  Les clients attendent une fiabilité proche des 100 % de la part des fournisseurs de services de cloud, ce qui octroie une importance primordiale à la fiabilité et la stabilité du réseau. Chaque fournisseur de services de cloud indique clairement le niveau de stabilité de service garanti qu'il entend fournir dans son accord de niveau de service (SLA). Par exemple, dans l'accord de niveau de service d'Amazon Compute, Amazon s'engage à assurer une disponibilité mensuelle de 99,99 %,[1] ce qui signifie que le temps d'indisponibilité du service est inférieur à 4,32 minutes par mois. Il n'est pas exagéré de qualifier ce niveau de service de « service ininterrompu ».

- Riche ensemble d'outils d'exploration des données

  Les services de cloud fournissent un riche ensemble d'outils, tels que la visualisation de données, les algorithmes de données, la machine virtuelle et l'apprentissage machine, dans le cadre de leurs plateformes. En ayant accès à ces outils, les utilisateurs peuvent plus facilement mettre en œuvre un certain nombre d'applications diverses. Par exemple, les ingénieurs peuvent utiliser un service de cloud pour l'exploration des données afin de réduire leurs efforts de maintenance des serveurs et d'améliorer leur efficacité opérationnelle.

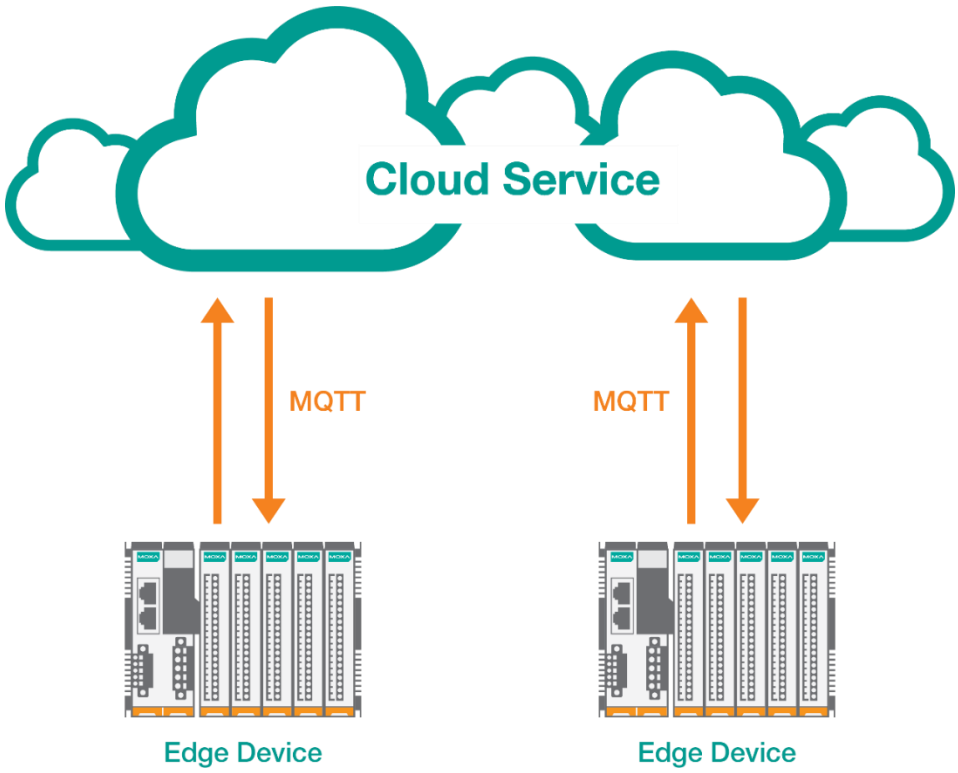


Figure 7. Architecture pour la connexion directe au cloud

**Connexion à une passerelle locale**

La connexion directe des périphériques de bordure au cloud présente certains avantages, mais vous devez également être conscient des diverses préoccupations liées à l'adoption de services de cloud pour les applications IIoT.

- La première préoccupation est le coût. Étant donné que les services de cloud facturent les utilisateurs en fonction du nombre de paquets de données transmis, il n'est pas rentable de transmettre directement les données des périphériques de bordure à un service de cloud. Même si les périphériques de bordure se connectent au cloud via un réseau cellulaire, vous devez payer le service cellulaire.

- La deuxième préoccupation concerne la sécurité des données. Bien que les services de cloud offrent des environnements bien protégés pour le stockage des données des utilisateurs, certains utilisateurs hésitent encore à télécharger des données sensibles sur le cloud.

Pour la plupart des applications IIoT, la mise en place d'une passerelle sur le site de terrain pour collecter les données des périphériques de bordure et/ou pour permettre la communication M2M sur le site de terrain est un moyen d'éviter ces préoccupations. La passerelle est généralement un ordinateur embarqué, et bien qu'elle ne doive pas nécessairement être configurée pour les rôles d'agent MQTT et de client MQTT, elle peut l'être. En tant qu'agent MQTT, la passerelle peut gérer la transmission des données M2M sur le site de terrain. En tant que client MQTT, la passerelle peut collecter les données des périphériques sur le site de terrain et envoyer les données utilisables à un système SCADA, une IHM ou un service de cloud. La solution de passerelle minimise encore les coûts en utilisant MQTT pour permettre la communication M2M sur le site de terrain au lieu de passer par le cloud.

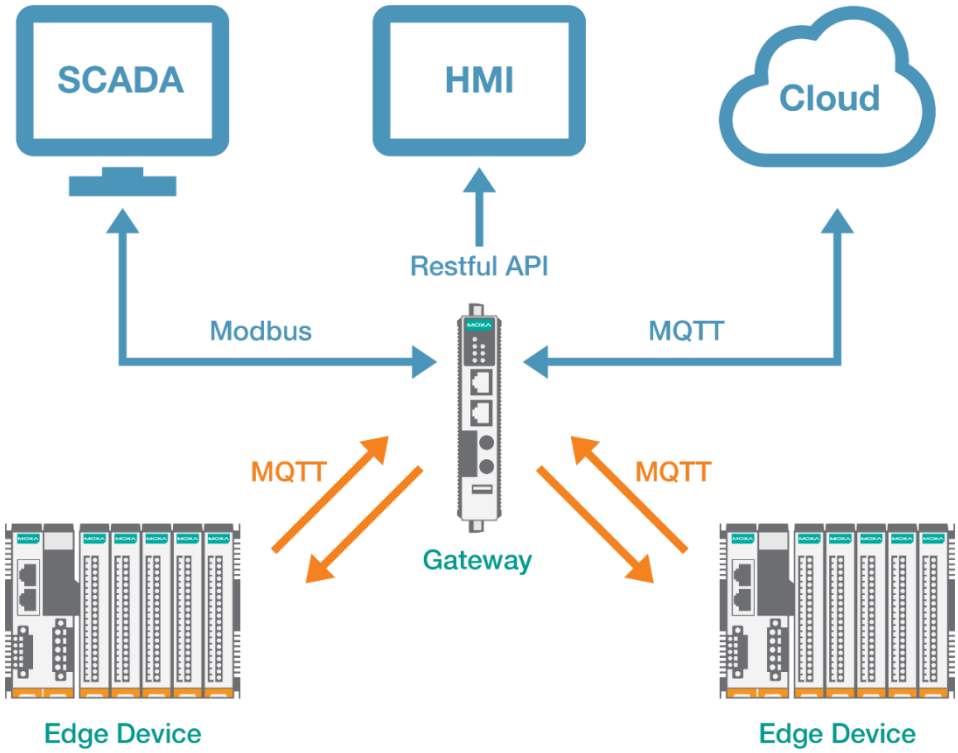


Figure 8. Architecture pour la connexion à une passerelle locale

## Défis de la conversion en application IIoT

Lors de la transformation d'une application OT traditionnelle en application IIoT, vous pouvez vous attendre à rencontrer certains ou l'ensemble les défis suivants.

**Les anciens périphériques actuellement utilisés ne prennent pas en charge MQTT.**

Dans les usines, les ingénieurs d'installation utilisent généralement une configuration d'E/S à distance pour l'accès aux données et la surveillance de l'environnement de fonctionnement. En outre, des passerelles de protocole sont utilisées pour collecter les données des compteurs de puissance et pour surveiller la consommation d'énergie. Avec la tendance IIoT qui bat son plein, si le protocole MQTT doit être utilisé pour transmettre des données vers le cloud, les ingénieurs d'installation devront d'abord étudier et acheter de nouveaux produits d'E/S à distance et des passerelles qui prennent en charge MQTT. Compte tenu du grand nombre d'anciens périphériques encore utilisés sur les sites de terrain du monde entier, la conversion d'une usine à une configuration basée sur IIoT risque de nécessiter un investissement considérable.

**La fusion de l'IT avec les applications d'automatisation traditionnelles est plus facile à dire qu'à faire.**

L'une des tâches fondamentales d'une application IIoT consiste à collecter et à transmettre des données OT vers le cloud, après quoi les données peuvent être traitées et/ou analysées. Le défi vient du fait que les secteurs IT et OT utilisent des protocoles de transmission différents. Modbus, qui est l'un des protocoles les plus employés dans le domaine de l'OT, utilise des paquets de données avec de petits en-têtes et charges utiles afin de permettre la transmission des paquets sur des réseaux à bande passante limitée. De leur côté, un grand nombre des ingénieurs IT ne connaissent pas Modbus car ils utilisent des protocoles IT, tels que MQTT, RESTful API et SNMP, pour collecter des données.

**La sécurité est une préoccupation majeure.**

Le maintien de la sécurité du réseau est une préoccupation majeure pour les applications IIoT. D'après l'expérience passée, les cyberattaques proviennent de l'extérieur de l'usine. La première étape pour améliorer la cybersécurité consiste donc à installer un routeur sécurisé, à configurer le pare-feu pour empêcher les pirates d'entrer et, de manière générale, à améliorer la sécurité du réseau pour prévenir les attaques extérieures. Le plus souvent, les périphériques de bordure de l'intranet d'une usine ne prennent en charge que des fonctions de sécurité limitées (le cas échéant) et utilisent toujours des protocoles non cryptés. Modbus, par exemple, est couramment utilisé pour transmettre des données vers et depuis des périphériques de bordure. Ces dernières années, certaines cyberattaques très médiatisées ont attiré l'attention sur les problèmes de sécurité des réseaux industriels. Par exemple, en août 2018, TSMC a été victime d'une cyberattaque d'une variante de WannaCry, entraînant une chute de revenus estimée à près de 200 millions de dollars[2]. L'attaque résultait du fait que le dernier correctif de sécurité n'avait pas été installé sur tous les périphériques de l'intranet de TSMC, ce qui signifie qu'en principe, l'attaque aurait dû être facile à prévenir. La leçon importante à retirer de cet incident est que la sécurité du réseau doit être implémentée, d'une manière ou d'une autre, au niveau des périphériques de bordure.

## Solution de Moxa

Les périphériques d'E/S à distance modulaires de la série ioThinx 4510 de Moxa, récemment mis sur le marché, présentent des fonctionnalités clés qui les rendent parfaitement adaptés aux applications IIoT.

### Prise en charge du client MQTT

La série ioThinx 4510 prend en charge le client MQTT qui permet aux périphériques connectés à l'ioThinx 4510 de se connecter facilement aux services de cloud. Bien que la série ioThinx 4510 soit présentée comme un produit d'E/S à distance d'entrée de gamme, sa prise en charge de MQTT en fait un atout puissant. En effet, vous pouvez utiliser l'interface utilisateur de l'ioThinx 4510 pour définir vos propres sujets MQTT, puis, en fonction de ces sujets, déterminer quels clients s'abonnent à quelles données. Outre les données de canal, la série ioThinx 4510 peut également fournir aux abonnés des attributs de données (mode de canal, valeurs maximales ou minimales, etc.) afin que les périphériques de type IT connectés au réseau puissent obtenir le dernier statut d'un produit ioThinx 4510 via MQTT. La charge utile MQTT utilise le format JSON qui est largement utilisé dans le secteur IT actuel. Lorsque les abonnés reçoivent un paquet MQTT, ils peuvent facilement chercher les données à l'aide d'un mot clé particulier « valeur » pour trouver les données qu'ils recherchent dans la charge utile.

### Passerelle Modbus intégrée

La série ioThinx 4510 possède une interface série 3 en 1 intégrée qui peut être utilisée pour implémenter une passerelle Modbus. Il suffit de quelques clics pour configurer ioThinx 4510 afin de collecter les données d'un périphérique Modbus série. À l'instar des données E/S, les données Modbus série sont accessibles par MQTT. Grâce à cette fonction, les données E/S et les données série peuvent être collectées à l'aide d'un seul périphérique de la série ioThinx 4510, ce qui réduit considérablement la complexité et le coût de votre système. Outre les données Modbus, la série ioThinx 4510 peut accéder à d'autres protocoles tels que Modbus/TCP, RESTful API et SNMP. En résumé, la série ioThinx 4510 permet une transmission simple et directe des données série vers le cloud.

### Améliorations de la sécurité

Afin de protéger les données des utilisateurs, la série ioThinx 4510 prend en charge TLS v1.2 pour crypter les données envoyées via les transmissions MQTT. Cette technologie de cryptage des données largement utilisée et reconnue protège les données transmises sur un réseau contre les attaques de tiers. ioThinx 4510 prend également en charge les noms de compte et les mots de passe pour l'agent afin d'empêcher la publication de données à des agents non autorisés. De plus, la série prend en charge RESTful API via https et SNMPv3 afin que tous les protocoles IT pris en charge puissent transmettre avec un cryptage des données. Pour le protocole Modbus/TCP qui transmet les données en texte clair, la série ioThinx 4510 dispose d'une fonction de contrôle d'accès qui s'appuie sur une liste d'adresses IP autorisées à accéder à ioThinx 4510, ce qui renforce la sécurité opérationnelle.

Grâce à ces fonctions avancées et à la prise en charge de divers modules d'E/S, la série ioThinx 4510 aide non seulement les ingénieurs IT à collecter des données sur le terrain, mais elle permet aussi aux ingénieurs OT de transmettre ces données aux services de cloud en toute sécurité. En fait, la série ioThinx 4510 élimine le fossé qui sépare les mondes IT et OT.

## Références

[1] Contrat de niveau de service Amazon Compute, Amazon Web Services : https://aws.amazon.com/compute/sla/

[2] Wu, D., Gurman, M. (5 août 2018). iPhone Chipmaker Races to Recover After Crippling Computer Virus (Un fabricant de puces de l'iPhone s'empresse de récupérer après un virus informatique dévastateur.), *Bloomberg* : https://www.bloomberg.com/news/articles/2018-08-05/iphone-chipmaker-races-to-recover-after-crippling-computer-virus

TECHNIQUES DE L'INGÉNIEUR

# GAGNEZ DU TEMPS ET SÉCURISEZ VOS PROJETS EN UTILISANT UNE SOURCE ACTUALISÉE ET FIABLE

Techniques de l'Ingénieur propose la plus importante collection documentaire technique et scientifique en français !

Grâce à vos droits d'accès, retrouvez l'ensemble des **articles et fiches pratiques de votre offre, leurs compléments et mises à jour,** et bénéficiez des **services inclus.**

| | | | |
|---|---|---|---|
| RÉDIGÉE ET VALIDÉE PAR DES EXPERTS | MISE À JOUR PERMANENTE | 100 % COMPATIBLE SUR TOUS SUPPORTS NUMÉRIQUES | SERVICES INCLUS DANS CHAQUE OFFRE |

- **+ de 350 000 utilisateurs**
- **+ de 10 000 articles de référence**
- **+ de 80 offres**
- **15 domaines d'expertise**

- **Automatique - Robotique**
- **Biomédical - Pharma**
- **Construction et travaux publics**
- **Électronique - Photonique**
- **Énergies**
- **Environnement - Sécurité**
- **Génie industriel**
- **Ingénierie des transports**
- **Innovation**
- **Matériaux**
- **Mécanique**
- **Mesures - Analyses**
- **Procédés chimie - Bio - Agro**
- **Sciences fondamentales**
- **Technologies de l'information**

**Pour des offres toujours plus adaptées à votre métier, découvrez les offres dédiées à votre secteur d'activité**

Depuis plus de 70 ans, Techniques de l'Ingénieur est la source d'informations de référence des bureaux d'études, de la R&D et de l'innovation.

**www.techniques-ingenieur.fr**

**CONTACT :** Tél. : + 33 (0)1 53 35 20 20 - Fax : +33 (0)1 53 26 79 18 - E-mail : infos.clients@teching.com

TECHNIQUES DE L'INGÉNIEUR

# LES AVANTAGES ET SERVICES compris dans les offres Techniques de l'Ingénieur

## ACCÈS

**Accès illimité aux articles en HTML**
Enrichis et mis à jour pendant toute la durée de la souscription

**Téléchargement des articles au format PDF**
Pour un usage en toute liberté

**Consultation sur tous les supports numériques**
Des contenus optimisés pour ordinateurs, tablettes et mobiles

## SERVICES ET OUTILS PRATIQUES

**Questions aux experts***
Les meilleurs experts techniques et scientifiques vous répondent

**Articles Découverte**
La possibilité de consulter des articles en dehors de votre offre

**Dictionnaire technique multilingue**
45 000 termes en français, anglais, espagnol et allemand

**Archives**
Technologies anciennes et versions antérieures des articles

**Impression à la demande**
Commandez les éditions papier de vos ressources documentaires

**Alertes actualisations**
Recevez par email toutes les nouveautés de vos ressources documentaires

*Questions aux experts est un service réservé aux entreprises, non proposé dans les offres écoles, universités ou pour tout autre organisme de formation.

# ILS NOUS FONT CONFIANCE

AgroParisTech · AIRBUS · cea · CESI Enseignement Supérieur et Formation Professionnelle · cnes Centre National d'Études Spatiales · CSTB le futur en construction · ENGIE · GE · L'ORÉAL · Leroy-Somer · École Polytechnique Université Paris-Saclay · SAFRAN Aerospace Defence Security · Sagemcom · SAINT-GOBAIN · Schneider Electric · THALES · TOTAL · Valeo · VEOLIA · Wallonie · SPW Service public de Wallonie

**www.techniques-ingenieur.fr**

**CONTACT :** Tél. : + 33 (0)1 53 35 20 20 - Fax : +33 (0)1 53 26 79 18 - E-mail : infos.clients@teching.com