Trois piliers pour relever les défis actuels du secteur de l'énergie et des services d'utilité publique

Alcatel·Lucent
Enterprise

eBook

Sommaire

- Identifier les défis liés à l’énergie et aux services d’utilité publique
- Trois piliers pour relever ces défis
  1. La sécurité d’abord
  2. Augmenter l’efficacité opérationnelle
  3. Améliorer l’engagement des clients
- ALE répond aux besoins du secteur de l’énergie et des services d’utilité publique

Identifier les défis liés à l'énergie et aux services d'utilité publique

Aujourd'hui, le changement climatique oblige les entreprises du secteur de l'énergie et des services d'utilité publique à évoluer vers davantage d'énergies renouvelables, en réduisant leur empreinte carbone et en limitant la pollution. Cette réalité mondiale pousse les entreprises de ce secteur à mettre en œuvre des politiques d'efficacité et des améliorations technologiques visant à réduire leur consommation et à accroître leur résilience afin d'assurer une continuité de service et des plans de reprise d'activité efficaces.

Ces opérateurs sont confrontés à trois types de défis :

- **A l'échelle mondiale,** les entreprises du secteur de l'énergie et des services d'utilité publique doivent améliorer la sécurité de leurs opérations, réduire leur empreinte carbone, se protéger contre les cyberattaques et se conformer aux nouvelles réglementations
- **Sur le plan technologique,** ces entreprises doivent faire face à des projets de migration, à l'obsolescence de leurs technologies, à l'interfonctionnement entre les nouveaux et les anciens systèmes et à la gestion de réseaux à très grande échelle
- **En ce qui concerne la clientèle,** elles doivent concevoir des stratégies de relation client innovantes et proposer de nouveaux services qui répondent aux nouvelles habitudes de consommation de leurs clients

Trois piliers pour relever les défis

Une approche reposant sur trois piliers, axée sur le renforcement de la sécurité, l'augmentation de l'efficacité opérationnelle et l'amélioration de l'engagement client, aide les opérateurs du secteur de l'énergie et des services d'utilité publique à relever ces défis.

1. La sécurité d'abord

Face à l'omniprésence des failles de cybersécurité, du vandalisme et des attaques terroristes, le secteur de l'énergie et des services d'utilité publique doit être préparé à faire face à ces menaces. Des investissements sont nécessaires dans un certain nombre de domaines, notamment la mise en place d'une infrastructure puissante et sécurisée pour les réseaux et les communications, la protection des personnes et des équipements, et le développement de mécanismes permettant de faire face aux menaces liées à la cybersécurité.

Le réseau informatique doit assurer plusieurs niveaux de résilience, optimiser les flux de trafic et minimiser les interruptions de service. Un plan de résilience, garantissant la continuité des services, et un plan de reprise d'activité efficace après sinistre sont indispensables. Le plan de résilience doit s'appuyer sur une infrastructure de réseau stratégique, fiable et robuste. Il doit être cybersécurisé, adapté aux applications et doté d'une plateforme de gestion unifiée.

Un **réseau performant** se doit d'être résilient et sécurisé pour interconnecter les différents domaines. Il doit continuer à fonctionner sans interruption, même lorsqu'il se trouve compromis.

Les communications doivent englober toute une série d'activités telles que la sécurité opérationnelle, la sécurité du personnel, la protection des travailleurs sur le terrain, tout particulièrement dans des environnements dangereux. La mise en œuvre d'un plan de résilience nécessite **une infrastructure de communication fiable** pour assurer la continuité des opérations.

Une infrastructure de réseau et de communication fiable

Les solutions de réseau et de communication doivent être extrêmement fiables et pérennes, capables de relever les défis d'aujourd'hui et de demain.

La colonne vertébrale du réseau doit posséder les capacités suivantes :

- Segmentation des services
- Convergence des réseaux d'applications multi-services
- QoS déterministe pour répondre aux exigences spécifiques des applications.
- Haute disponibilité du réseau
- Sécurité granulaire
- Synchronisation précise du réseau
- Gestion simple et centralisée du réseau

Parmi les éléments d'une infrastructure de communication fiable, on peut citer :

- la redondance à chaud pour un système de communication performant
- la redondance géographique pour la sauvegarde des sites locaux
- des communications fiables pour une plateforme de communication toujours active
- le déploiement de sites distants garantissant la continuité des services grâce à des fonctions de survivabilité locale
- la conformité multi-terminaux pour répondre à des usages spécifiques (IP, SIP, TDM, analogique)
- la virtualisation complète permettant d'optimiser le déploiement du centre de données
- l'architecture hybride pour protéger les investissements et évoluer vers de nouveaux modèles
- la prise en charge des services informatiques dématérialisés (cloud) privés et publics

Assurer la sécurité des personnes

Le personnel de sécurité et les intervenants de la sécurité publique doivent être en capacité d'agir rapidement et efficacement pour faire face aux situations d'urgence. Ils ne doivent pas être perturber dans leur mission par des problèmes opérationnels. Pour pouvoir réagir rapidement, ces intervenants ont besoin d' informations précises sur l'appelant, notamment sa localisation et des détails décrivant la situation d'urgence. Il est également primordial de diffuser des messages pour inciter le personnel à se mobiliser ainsi que d'enregistrer les conversations à des fins de formation et d'accompagnement, voire pour des investigations ultérieures. Les éléments suivants permettent aux travailleurs sur le terrain, effectuant des tâches dangereuses, de travailler en toute sécurité :

- La **solution pour les travailleurs isolés** inclut un terminal capable de déclencher des alarmes en cas d'incident et d'indiquer l'emplacement du travailleur. Ces terminaux fournissent des informations telles que la présence d'un homme à terre, l'absence de mouvement, des fonctions d'alerte avec bouton ou cordon de secours. En complément, un serveur de notification accroît la réactivité du personnel opérationnel dans l'ensemble des infrastructures, en dirigeant les appels d'urgence vers les bons intervenants. Ces services de notification permettent également de diffuser des messages sur n'importe quel terminal pour mobiliser le personnel en cas d'incident.
- La **solution d'assistance visuelle à distance** (RVA) permet des communications mains libres et des interactions enrichies entre le technicien sur le terrain et les experts. Ces services rendent possible les sessions vocales et vidéo ainsi que le partage de documents (photos et vidéos), pouvant être collectés et centralisés.

Protéger les équipements

Les contrôles d'accès sont essentiels pour protéger les infrastructures contre la criminalité et les attaques, mais les infrastructures de l'énergie et des services d'utilité publiques sont étendues, ce qui les rend souvent difficiles à surveiller. La mise en œuvre des mesures suivantes facilite la surveillance de ces activités :

- **Les caméras de vidéosurveillance** offrent une vue d'ensemble des entrées et des sorties. La vidéo intelligente, qui utilise l'IA et les outils d'analyse, facilite l'identification et la mise en corrélation des comportements suspects dans l'ensemble des infrastructures
- **Les capteurs de protection contre les intrusions**, connectés au réseau de données, remplacent les protocoles propriétaires et les systèmes de communication spécifiques par des systèmes IP faciles à intégrer
- **Les processus d'alarme et les flux de travail sécurisés** permettent aux services opérationnels de surveiller les alarmes provenant d'une large gamme de capteurs (tels que la détection d'incendie, de fuites, de température ou de pression et autres). Les capteurs de l'Internet Industriel des Objets (IIoT) permettent de rationaliser le flux des notifications d'alarme vers le personnel opérationnel
- **Le serveur de notification d'urgence** suit un scénario précis pour initier l'action appropriée, incluant des notifications vers un large éventail de terminaux téléphoniques, d'applications de collaboration et d'interfaces
- **Les commutateurs et les points d'accès industriels** offrent des capacités de qualité industrielle, une sécurité renforcée et des performances supérieures pour les applications critiques fonctionnant dans des environnements difficiles et à des températures extrêmes. Ils permettent de mettre en place un réseau dans des zones où il est nécessaire d'assurer une connectivité physique pour les solutions de sécurité. Ce réseau est conforme aux certifications, cybersécurisé et administrable à distance.

eBook
Trois piliers pour relever les défis actuels du secteur de l'énergie et des services d'utilité publique

La cybersécurité au-delà du réseau

Lorsqu'il s'agit de détecter des menaces, d'autres aspects que la sécurité physique doivent être pris en compte car de nombreuses menaces sont désormais numériques. Les machines sont de plus en plus perfectionnées, dotées de nombreux systèmes de capteurs, tels que l'IIoT, et donc connectées, ce qui permet d'améliorer l'efficacité opérationnelle. Elles sont même parfois connectées à un réseau internet public, ce qui peut constituer un risque grave pour la sécurité. Les pirates peuvent ainsi facilement utiliser les terminaux compromis pour s'introduire dans le reste du réseau de l'entreprise. Le besoin de connectivité mobile, avec des applications sans fil et cloud, accentue encore ces menaces.

L' **architecture du réseau Zero Trust** est efficace, facile à gérer et extrêmement évolutive. Elle vise à promouvoir la sécurité au-delà du périmètre du réseau et s'appuie sur une approche multicouche pour sécuriser l'ensemble du réseau, y compris les différents terminaux. Elle part du principe que les agresseurs sont déjà présents et toujours prêts à frapper. Aucune confiance implicite n'est accordée. Ces mêmes niveaux élevés de protection sont appliqués à chaque personne, système, sous-système, application et terminal interne et externe, tentant d'accéder au réseau. L'accès est strictement limité aux ressources requises au moment de la demande, et toutes les ressources du réseau sont en permanence analysées pour détecter toute activité inhabituelle ou malveillante.

Un réseau Zero Trust protége contre les menaces de cybersécurité afin de maintenir l'intégrité des systèmes de l'énergie et des services d'utilité publique tout en maintenant des capacités opérationnelles complètes. Il permet de protéger toutes les ressources de l'organisation, et non pas seulement le réseau, en mettant l'accent sur la protection de l'accès aux ressources.

eBook
Trois piliers pour relever les défis actuels du secteur de l'énergie et des services d'utilité publique

Une architecture de réseau Zero Trust

Parmi les attributs d'une architecture Zero Trust, figurent des politiques de sécurité avancées, l'authentification des terminaux, l'identification, la segmentation et la micro-segmentation. En outre, il convient de prendre en considération les éléments suivants :

- Des éléments de sécurité intégrés dans l'architecture
- Un chiffrement natif afin de maintenir l'intégrité du système
- De meilleures pratiques pour l'authentification interne et externe
- Des audits réguliers des systèmes et politiques de mots de passe
- Des capacités de support logiciel qui permettent de mettre à jour le code en cas d'attaque ou de vulnérabilité détectée
- Certification ISO 27001 pour la gestion de la sécurité de l'information
- Des commutateurs industriels dont la sécurité est renforcée et qui intègrent des technologies de sécurité perfectionnées, vérifiées et validées par des organismes tiers
- Un système d'exploitation unique et sécurisé pour réduire la surface d'attaque de l'organisation, atténuer les risques et permettre une remédiation ciblée
- Des solutions qui intègrent des technologies de sécurité clés telles que Wi-Fi Protected Access 3 (WPA3), Shortest Path Bridging (SPB), MACsec, Address Space Layout Randomisation (ASLR) et role-based network access control

2. Augmenter l’efficacité opérationnelle

Les opérations dans le domaine de l’énergie et des services d’utilité publique couvrent généralement de vastes zones géographiques dans des environnements complexes, avec des ressources humaines et techniques limitées pour les gérer. Sans connectivité ni communications, l’énergie et les services ne peuvent être produits ou distribuée, ce qui signifie que les services rendus au public risquent d’être perturbés ou interrompus. La technologie et l’innovation permettent de mettre en place des modèles opérationnels agiles pour répondre à ces exigences.

Le CCO, le cerveau des activités opérationnelles

Le centre de contrôle des opérations (CCO) gère le contrôle quotidien, la direction et la coordination des activités opérationnelles dans le domaine de l’énergie et des services d’utilité publique afin de garantir la qualité des services. Il apporte une assistance à la maintenance à distance permettant d’identifier et de répondre à des situations inattendues qui exigent une attention, une coordination et des actions spécifiques, immédiates et efficaces.

Ces actions sont nécessaires pour éviter les interruptions opérationnelles, afin de minimiser les impacts négatifs sur le service client, les coûts et la sécurité. Un CCO intelligent repose sur la connectivité, la numérisation, les communications en temps réel et la collaboration.

Pour relever les principaux défis du CCO, il faut tenir compte de trois principaux domaines, à savoir :

- **Un espace de travail numérique efficace** permettant d'une part aux agents de l’OCC de gérer et distribuer les appels efficacement, et facilitant d'autre part le travail quotidien des personnels, sur le terrain et dans l’administratif.
- **Une protection complète du personnel et des équipements** grâce à des capacités d’enregistrement et à des solutions de gestion des urgences
- **Des services innovants et efficaces** connectant à la fois les personnes, les objets et les applications

Efficacité dans la gestion et la maintenance

Les technologies modernes, telles que l'IoT et la numérisation, possèdent un grand nombre d'applications qui contribuent à l'efficacité opérationnelle. Tous les terminaux, capteurs et actionneurs nécessitent une maintenance de la part des équipes de gestion informatique et d'exploitation. Cependant, pour que les composants restent en état de fonctionner, il faut que la connectivité réseau soit toujours assurée et que les capacités de contrôle et de réponse à distance soient immédiates. Les outils de gestion centralisée et de maintenance préventive aident les opérateurs du secteur de l'énergie et des services d'utilité publique à gagner du temps et à réduire les temps d'interruption du réseau.

Gestion centralisée : cet outil permet la gestion du WLAN et du LAN, et simplifie les opérations. L'analyse centralisée permet également de prendre des décisions proactives et préventives afin de maintenir la santé du réseau, d'améliorer le temps de fonctionnement et de réduire les coûts. L'interopérabilité et une architecture ouverte (API) avec d'autres systèmes (SCADA, par exemple) permettent d'assurer la qualité de service, la sécurité et l'évolutivité et jettent les bases de la convergence IT/OT.

Maintenance prédictive : cet autre outil est un compagnon d'exploitation du réseau basé sur l'IA qui permet d'assurer une surveillance du réseau en temps réel, d'envoyer des alertes sur les risques potentiels et de résoudre les problèmes de réseau, optimisant ainsi la qualité de l'expérience (QoE). La maintenance préventive d'un réseau consiste à prévoir des correctifs, à détecter les problèmes avant qu'ils n'apparaissent et à prendre soin de votre réseau de manière proactive.

eBook
Trois piliers pour relever les défis actuels du secteur de l'énergie et des services d'utilité publique

3. Améliorer l’engagement des clients

Aujourd’hui, les clients veulent bénéficier d’une expérience personnalisée, de données détaillées sur leur consommation, ainsi que des informations sur la mise à jour ou la modification de leur contrat. Les entreprises du secteur de l’énergie et des services d’utilité publique doivent digitaliser leurs processus pour renforcer leur service client et réduire leurs temps de réponse, la satisfaction des besoins de leurs clients constituant leur priorité absolue. Les solutions suivantes apportent aux clients d’aujourd’hui l’expérience qu’ils attendent :

- **Accueil automatisé :** une opératrice automatique offre un accueil téléphonique professionnel 24h/24 et 7j/7, c'est-à-dire une réponse de qualité en toutes circonstances. Une bonne expérience de service commence par un accueil courtois et permet d’orienter les appelants directement vers les employés et les services concernés, voire la messagerie vocale. L’interface visuelle de programmation est intuitive et flexible, avec des paramètres facilement personnalisables et des règles de routage des appels s’adaptant instantanément aux nouveaux besoins de l’entreprise.
- **Centre de contact multimédia :** aujourd’hui, les utilisateurs finaux veulent pouvoir contacter leurs opérateurs par le canal de leur choix, qu’il s’agisse de la voix, du courrier électronique, du chat depuis le site web de l’opérateur ou des réseaux sociaux. Un centre de contact multimédia optimise les interactions omnicanales par le biais de canaux vocaux et numériques, avec qualité, disponibilité et efficacité. Le centre de contact multimédia est basé sur une solution de "centre de contact en tant que service" (CCaaS) qui permet aux entreprises d’exploiter la puissance du cloud tout en tirant parti de leurs investissements en équipements de communication. Le centre de contact multimédia offre également une assistance basée sur l’IA pour obtenir des réponses rapides et précises, ce qui permet d’améliorer la résolution des problèmes dès le premier contact ainsi que l’expérience client.
- **Connecteurs et applications dans le cloud :** améliorer les interactions avec les clients en intégrant les communications dans les applications professionnelles existantes, telles que les outils de gestion de la relation client (CRM) et de gestion des services informatiques. Les fonctionnalités « click-to-call » permettent à l’utilisateur de passer facilement des appels vers son service d’assistance à la clientèle. L’intégration de CPaaS sur le site web ou l’application mobile de l’opérateur lui permet aussi d’interagir avec un agent par le biais d’un chatbot, de messages textuels, de communications vocales et vidéo.

ALE répond aux besoins du secteur de l’énergie et des services d’utilité publique

Des services disponibles pour vous à chaque étape

Les services Alcatel-Lucent Enterprise accompagnent votre Business Partner ALE ou intégrateur système, à chaque phase de votre déploiement. Notre gamme de services est disponible prête à l’emploi ou peut être adaptée à des besoins spécifiques, délivrée sur site ou à distance. Elle comprend les éléments suivants :

- **Des services professionnels** disponibles, sur site et à distance, de la conception du projet à sa mise en œuvre, en collaboration avec votre Business Partner ALE ou intégrateur système
- **Des services de formation** pour vous aider à développer vos compétences, adopter de nouvelles technologies et devenir autonome
- **Des services gérés** qui offrent à votre Business Partner des prestations flexibles pour la prise en charge des opérations de réseau 24h/24 et 7j/7, avec un accord de niveau de service garanti et une surveillance améliorée
- **Des services d’assistance** assurant la continuité des activités 24h/24 et 7j/7
- **Des services de personnalisation** offrant l’opportunité à votre équipe de développer les applications spécifiques dont vous avez besoin à partir de notre base technologique
- **Des services de gestion du succès** permettant d’accompagner vos utilisateurs finaux dans leur transformation numérique, avec l’adoption des solutions et de leurs avantages, telle que définie par des critères de réussite.

eBook
Trois piliers pour relever les défis actuels du secteur de l'énergie et des services d'utilité publique

Étude de cas client

Ocala Fiber Network

La volonté de mettre à disposition des services à large bande a permis de réaliser des économies et de délivrer une connectivité vitale aux clients des secteurs de l'éducation et de la santé en période de crise.

Ocala Fiber Network (OFN), située en Floride, est issue de la compagnie d'électricité de la ville d'Ocala, fondée il y a vingt ans. Son objectif : mettre à disposition une gamme de services internet à large bande basés sur la mise en place d'un réseau 100 % fibre pour les agences municipales et les citoyens. Le réseau a été modernisé avec des commutateurs Alcatel-Lucent Enterprise pour offrir des vitesses plus élevées avec une meilleure gestion du réseau et des performances accrues.

« Les commutateurs OmniSwitch constituent la partie du cerveau qui nous permet de fonctionner. Tous nos commutateurs Alcatel-Lucent Enterprise sont essentiels pour l'ensemble des connexions et la fourniture des services au sein de notre réseau. Alcatel-Lucent Enterprise propose un ensemble d'équipements d'excellence. Mes ingénieurs me disent qu'ils aiment sa simplicité et surtout la qualité du support qu'ils reçoivent. »

MEL POOLE, DIRECTEUR D'OCALA FIBER NETWORK

Parmi les avantages d'aujourd'hui, on peut citer :

- La rationalisation du réseau qui permet à OFN de fournir des services plus étendus et une plus grande bande passante à ses clients
- Le portefeuille OmniSwitch® d'Alcatel-Lucent Enterprise qui permet à OFN d'augmenter l'utilisation des ressources de manière transparente en temps de crise.
- Des commutateurs ALE à l'épreuve du temps, 5 à 10 fois plus rapides que les commutateurs d'autres fournisseurs

Lire l'étude de cas complète

eBook
Trois piliers pour relever les défis actuels du secteur de l'énergie et des services d'utilité publique

Des solutions pour aujourd'hui et demain

Les solutions Alcatel-Lucent Enterprise pour l'énergie et les services d'utilité publique répondent aux défis auxquels les entreprises sont confrontées chaque jour, notamment en matière de sécurité, d'efficacité opérationnelle et d'engagement des clients. Nous connectons tous les sous-systèmes pour proposer des services plus intelligents et plus écologiques, avec des modèles « as a Service » (aaS) . Les solutions ALE permettent de minimiser l'impact sur l'environnement avant, pendant et après le déploiement grâce aux éléments suivants :

- Conception de produits éco-énergétiques moins énergivores, qui réduisent la consommation et la dissipation thermique
- Réduction de la taille du matériel, miniaturisation des composants et densification des ports
- Technologies de virtualisation afin d'éliminer complètement le recours à certains matériels
- Solutions cloud réduisant les besoins en espace et en énergie
- Architectures et cycles de vie des produits optimisés en vue de maximiser la longévité
- Matériaux d'emballage respectueux de l'environnement
- Conformité aux directives environnementales pour la fin de vie et l'élimination des produits.
- Notre programme Go Green combine nos efforts avec ceux de nos fournisseurs, partenaires et clients afin de réduire la pollution numérique, d'améliorer la gestion des déchets et de diminuer la consommation d'énergie sur toute la chaîne de valeur

Des solutions ALE pour relever les défis de l'énergie et des services d'utilité publique

Les solutions innovantes d'ALE, incluant notre famille de commutateurs industriels, nos capacités de communication et de cloud ainsi que nos application spécifiques pour les centres de contrôle, aident les opérateurs du secteur de l'énergie et des services d'utilité publique du monde entier à accroître leur sécurité, à améliorer leur efficacité et à renforcer leurs interactions avec les clients :

1. **Connectivité grâce à nos solutions de réseau :**

- Infrastructure de réseau et de communication stratégiques robustes et fiables
- Commutateurs industriels avec un niveau de protection élevée pour les environnements difficiles
- Vidéosurveillance et capteurs IoT pour la protection des personnes et des équipements

  Réseau Zero Trust afin de réduire les vulnérabilités liées aux cyber-menaces
- Plateformes de maintenance prédictive intégrant l'IA
- Gestion centralisée connectant tous les sous-systèmes de gestion comme par exemple le système SCADA
- Interopérabilité avec d'autres applications fonctionnelles
- Validation ANSI et DOD
- Zéro émission : certification et conformité en matière de responsabilité sociale des entreprises (RSE)
- Services d'assistance de plus de 10 ans

2. **Solutions de communication et de collaboration :**

- Centres de contrôle des opérations intelligents dotés d'un système de communication enrichie
- Assistance visuelle à distance entre le technicien sur site et les experts à distance
- Accueil automatisé et centre de contact multimédia afin d'améliorer les interactions clients

3. **Solutions Cloud :**

- Connecteurs API Rainbow et CPaaS pour intégrer les communications
- Solution cloud Rainbow™ proposée par Alcatel-Lucent Enterprise et déployée sur site grâce à Rainbow Edge.
- API et SDK pour les déploiements cloud

Découvrez comment les solutions Alcatel-Lucent Enterprise aident le secteur de l'énergie et des services d'utilité publique à relever les défis d'aujourd'hui.

© 2023 ALE International, ALE USA Inc. Tous droits réservés pour tous pays. Le nom et le logo d'Alcatel-Lucent sont des marques commerciales de Nokia utilisées sous licence par ALE. Pour voir la liste des marques de commerce d'ALE, veuillez consulter : www.al-enterprise.com/fr-fr/documentation-juridique/marques-copyright. DID23033101FR (octobre 2023)

Alcatel·Lucent Enterprise