

LOISIRS & CULTURE

Énergie,
Mobilité,
NUMÉRIQUE

Environnement, **HABITAT**,
Santé et bien-être, **SÉCURITÉ**

Alimentation

► **Correspond à
une technologie clé 2015**

MOTS CLÉS

communications radio privées,
Private Mobile Radio, PMR, LTE,
GSM, 3G, 4G, 5G, 3GPP, résilience,
régalien, réseaux dédiés, réseaux
virtuels, MVNO, cyberprotection



Définition et périmètre

Les systèmes de « communications sécurisées » permettent la réalisation d'un échange de type voix ou données (selon les cas), garantissant un certain niveau de protection vis-à-vis des menaces prises en compte. Parmi ceux-ci, on trouve les solutions de radiocommunications sécurisées communément regroupées sous l'acronyme PMR (Professional Mobile Radio – on emploie parfois aussi Private Mobile Radio).

Nota : La sécurité des communications des systèmes embarqués, et la sécurité des objets connectés sont respectivement abordées dans les technologies clés « Systèmes embarqués et distribués sécurisés et sûrs » et « Internet des objets ».

Mis en œuvre pour répondre à des besoins professionnels, avec une grande diversité d'utilisateurs, les réseaux PMR correspondent historiquement à des réseaux indépendants fonctionnant sur des bandes de fréquences spécifiques, souvent distincts des réseaux de téléphonie mobiles classiques ouverts au public ; une tendance d'avenir est de mutualiser les infrastructures sans pour autant transiger sur les spécifications des PMR. Leur couverture est le plus souvent locale ou régionale ; les communications point à multipoint sont une de leurs caractéristiques clés (les réseaux de téléphonie mobile pour le grand public sont point à point).

Les réseaux de PMR comportent par ailleurs un certain nombre de spécificités qui les distinguent des réseaux de communication classiques : disponibilité, permanence du service, confidentialité renforcée, chiffrement, préemption d'appel, établissement de la connexion instantanée (Push to talk), appel de groupe, mode direct, etc.

On distingue deux grands types d'usages, pour lesquels la disponibilité du réseau et la confidentialité des échanges sont bien souvent des exigences critiques :

- les usages régaliens et gouvernementaux. Les communications sécurisées permettent aux services publics (police, gendarmerie, pompiers, sécurité civile, etc.) de maintenir un niveau élevé et durable de sécurité et de protection publique, notamment dans le cadre d'évènements rassemblant de nombreuses personnes (rencontres sportives, commémorations, manifestations, etc.) ou lors d'opérations de secours (suite à des catastrophes naturelles ou industrielles, des accidents, des attentats, etc.) ;

- les usages professionnels. De nombreux secteurs d'activités sont concernés, tels que les transports (transports routiers, sociétés de bus, de taxis, services aéroportuaires, sociétés d'autoroutes, ambulanciers...), la sécurité et le gardiennage, le bâtiment et les travaux publics, l'énergie, l'industrie, les infrastructures.

Pourquoi cette technologie est-elle clé ?

- Enjeu de souveraineté nationale

À date, les acteurs français maîtrisent la totalité de la chaîne de valeur des PMR, hormis quelques composants élémentaires (semi-conducteurs, capteurs, etc.), notamment grâce à Airbus Group, Thales ou encore Alcatel-Lucent ; il est important que cette maîtrise perdure et se renforce. La solution « Confiance Numérique » de la Nouvelle France Industrielle constitue également un cadre structurant qui permet aux acteurs français de conforter leur excellence et maîtrise technologique.

- Dimension économique importante

Avec un taux de croissance élevé (marché qui doublera en moins de 10 ans), maîtriser les solutions de communications sécurisées de demain permettra aux acteurs français de renforcer leur position face aux grands américains (Motorola) et acteurs asiatiques conquérants (comme Huawei).

Liens avec d'autres technologies clés

- Les technologies clés qui influencent les communications sécurisées sont :

| | |
|----|--|
| 6 | Infrastructures de 5 ^{ème} génération |
| 34 | Authentification forte |

- Les technologies influencées par les communications sécurisées sont :

| | |
|---|---|
| 3 | Valorisation et intelligence des données massives |
| 7 | Systèmes embarqués distribués, sécurisés et sûrs |

Les marchés

IMS Resarch évalue le marché mondial à 8 Md\$ et estime qu'il doublera à horizon 2023 pour atteindre 15 Md.

Le marché des PMR numériques est aujourd'hui dominé par 3 technologies : TETRAPOL, standard international d'origine française, conçu par Matra et dont Airbus est le fournisseur principal, TETRA, norme soutenue au niveau européen par l'ETSI et P25 (radio portable de combat) son équivalent américain utilisé par Motorola (et tous les acteurs majeurs proposant des solutions au trois standards).

En France le marché des PMR est composé d'environ 55 entreprises et représentait 1 800 emplois en 2014. Le marché est, et sera, fortement tiré par les usages régaliens au niveau national mais également par les grands industriels au travers de leurs activités au niveau national et à l'export. Il est également important de souligner qu'il s'agit d'un marché de renouvellement et de modernisation des infrastructures qui ont été déployées dans les années 1990.

Le secteur évolue vers un « réseau unique » (mutualisation des infrastructures) pour les applications privées et professionnelles, où les infrastructures LTE constitueront le cœur du réseau. Ce réseau unique comprendra toutes les architectures réseaux qui devront coexister et être disponibles selon les besoins : réseaux publics, privés, ad-hoc, bulles tactiques, etc.

Les défis technologiques à relever

Le marché, en renouvellement, laisse place à une forte mutation technologique : les PMR de demain ne seront plus uniquement sur des réseaux spécifiques mais partageront les réseaux LTE auxquels ils devront s'adapter. Dans une ère où les *smartphones* sont aujourd'hui démocratisés au sein du grand public mais également dans la sphère professionnelle et régaliennne, il y a un réel enjeu de sécurisation et d'adaptation des échanges privés et critiques sur les réseaux publics.

■ Développer les réseaux LTE

Les PMR de demain n'emprunteront plus uniquement des réseaux privés mais partageront les réseaux LTE (4G, puis 5G) publics très haut débit. Adapter les réseaux LTE aux PMR devient une nécessité pour répondre aux attentes des usagers des PMR : ils offrent un meilleur débit et permettront aux PMR de s'ouvrir dans de nombreux domaines, notamment industriels (en lien avec l'arrivée de l'internet des objets plus sécurisés).



■ Des réseaux LTE adaptées aux PMR sûrs, résilients et durcis

Outre le développement des infrastructures, il est essentiel d'aligner les caractéristiques des réseaux LTE et les normes et spécifications des PMR, notamment :

Services spécifiques : conversation groupée, messagerie instantanée (*Short Message Service, SMS*), transmission de données instantanées (*Short Data Service, SDS*), gestion des priorités (préemption, un *lead* qui est prioritaire dans une conversation groupée) et communications entre groupes de terminaux.

Systèmes résilients : même en mode dégradé, les systèmes continueront à fonctionner, notamment pour des opérations de maintien de l'ordre, de secours ou militaires.

Systèmes sécurisés : chiffrement, « surchiffrement », cryptographie et cyberprotection.

Développée par Thales en 2013, Nexium Wireless est une première solution vers les nouvelles solutions LTE adaptées aux PMR pour les applications liées à la sécurité civile ou militaire.

■ Améliorer l'ergonomie des PMR

Les PMR sont aujourd'hui basiques (petit écran, uniquement communication directe, pas d'autres fonctionnalités), une approche peut être de développer un terminal PMR de type Smartphone, qui utilise une bande passante LTE : l'ajout de fonctionnalités multimédia améliorera l'ergonomie et l'expérience utilisateur (mais en conservant la sécurité et la résilience). Nexium, de Thales, intègre TeSquad, un nouveau « *smartphone durci* » sous Android.

Les défis commerciaux et d'usage à relever

■ Maintenir des prix compétitifs.

Bien qu'il soit pressenti à 15 Md\$ d'ici à 2023, le marché des PMR reste un segment d'ultraniche en comparaison avec le marché global des *smartphones* publics, estimé à 870 Md\$ (selon IDC).

Les commandes de PMR seront bien plus mesurées et le risque d'augmentation du prix unitaire d'un système est alors élevé. En adaptant les PMR aux réseaux LTE et au design de smartphones, il est essentiel que les prix restent comparables à ceux des smartphones, compte tenu de leurs spécificités augmentées.

Les enjeux réglementaires

■ Normalisation 3GPP : adapter les PMR aux usages publics et les bandes de fréquences LTE

Actuellement en cours de réflexion au niveau des instances européennes, il y a un fort enjeu de normalisation autour des standards techniques et des bandes de fréquences utilisables par les PMR pour les réseaux dits de services de protection publique et de secours en cas de catastrophe (*Public Protection on Disaster Relief*, PPDR). Cette normalisation doit se faire notamment au niveau de la coopération 3GPP (*Third Generation Partnership Project*) entre organismes de standardisation des télécommunications mondiales.

Analyse AFOM

ATOUTS

Base installée forte dans le monde

Maîtrise de toute la chaîne (infra, terminaux, réseaux dédiés, S-MVNO)

Laboratoires académiques et enseignement supérieur

Présence dans les instances de normalisation

Comité de filière des industries de sécurité (CoFIS) mobilisé sur ces sujets

FAIBLESSES

Dispersion des grands acteurs

Investissement sur LTE 4G insuffisants

OPPORTUNITÉS

Marché national structuré

Le marché international va se renouveler

Opérateurs nationaux forts

Secteur des utilities exportateur qui peut porter l'offre

MENACES

Concurrence directe avec Motorola

Nouveaux entrants asiatiques très agressifs

Consolidation du secteur en cours

Besoins forts d'investir dans la LTE

Facteurs clés de succès et recommandations

■ Maintenir les efforts de R&D sur la thématique

Notre position de leader nous permet de répondre à de forts enjeux de souveraineté dans les télécommunications à l'exemple des projets de démonstrateurs lancés dans le cadre du plan « Souveraineté Télécoms » : travaux de recherche sur la 5G (consortium projets européens 5GPP), démonstrateur d'un réseau 4G permettant d'offrir un réseau haut-débit et sécurisé, dédiés aux services de secours et aux opérateurs d'importance vitales (respectivement Airbus Group et Thales) labellisé par le CoFIS.

■ Dynamisme dans les groupes de normalisation

Il est essentiel que les acteurs français participent aux groupes de normalisation et d'évolution des réglementations, particulièrement en ce qui concerne l'allocation de bandes de fréquences publiques. Un groupe de réflexion piloté par l'ANSSI et dans le cadre du plan « Souveraineté Télécoms » a été lancé mi-2014, qui consiste

à émettre des recommandations concernant l'évolution de la réglementation sur la sécurité des réseaux.

■ Favoriser le rôle des startups innovantes pour redynamiser l'écosystème français

Il est important de permettre aux startups et PME, qui ont des moyens de R&D limités malgré un fort savoir technique, d'avoir accès à tous les outils, plateformes, accompagnement nécessaires à leur développement technologique et commercial en France et à leur expansion à l'international. L'exploitation par ces entreprises des moyens de R&D externalisés et collaboratifs serait un levier considérable vers la souveraineté de la France dans les communications numériques et sécurisées : projet européens collaboratifs, SATT, subventions, etc.

À ce titre, une action du plan « Souveraineté Télécoms » pilotée par EBLink est de redynamiser le développement économique des startups et PME en renforçant leur participation afin de recréer un écosystème en France.

Acteurs clés

| | |
|---|--|
| Entreprises | Airbus Defence and space - Centre d'Excellence Electronique, Airlynx, Alcatel-Lucent, Eolane, Etelm, Expway, Hub One, Ibelem, Logic Instrument, Luceor, Orange, Prescom, Sequans Communication, Sentryo, Sigfox, Sysoco, Thales Communications & Security, Wiko... |
| IRT, ITE, IHU | B-COM, SystemX... |
| Instituts Carnot | INRIA, M.I.N.E.S., TSN... |
| Autres centres de recherches | ESIEE, Mines Telecoms... |
| Pôles de compétitivité | CapDigital, Images et Réseaux, SCS, Systematic, TES... |
| Autres (clusters, associations, fédérations professionnelles, réseaux d'entreprises) | Lora... |

Position des acteurs français

| Position des entreprises françaises dans la compétition mondiale | |
|--|---|
| En position de leadership | ● |
| Dans la moyenne | |
| En retard | |

| Position des acteurs académiques français dans la compétition mondiale | |
|--|---|
| En position de leadership | |
| Dans la moyenne | ● |
| En retard | |