RADIO COMS PRO ALLIANCE

JOURNÉE

Réseaux radio professionnels :
réussir la convergence PMR, 4G/5G et IP



SPEAKER

Makara ANG

ARCHITECTE TELECOM
COGISYS

SECURISER VOS RESEAUX PMR

Des réseaux plus sûrs
pour un monde en mouvement



15 OCTOBRE 2026

Espace Saint Germain
Paris 7e

RADIO COMS PRO ALLIANCE

SECURISER VOS RESEAUX PMR

1 POURQUOI SECURISER VOS RESEAUX PMR

2 COMMENT SECURISER VOS RESEAUX PMR

3 3 CAS PRATIQUES DE SECURISATION



RADIO COMS PRO ALLIANCE

1 POURQUOI SECURISER VOS RESEAUX PMR ?



RADIO COMS PRO ALLIANCE

POURQUOI SECURISER VOS RESEAUX PMR

› LA NATURE CRITIQUE DES RESEAUX PMR

Mission & Business Critical: Les réseaux PMR soutiennent des operations vitales telles que les interventions d'urgence ou la protection de sites sensibles. Assurer leur continuité et fiabilité est une priorité absolue.



› LES OBLIGATIONS IMPOSEES AUX CLIENTS DES RESEAUX PMR

La majorité des clients des réseaux PMR sont soumis à des obligations strictes de protection de la donnée (***RGPD*** pour l'ensemble des entreprises, ***directive Police-Justice*** pour la Police, Administration Pénitentiaire, etc.) ou de protection du service (***LPM*** pour les Opérateurs d'Importance Vitale).

L'ANSSI et la CNIL sont mandatés pour veiller au respect de ces exigences, sous peine de ***sanctions financières***.



› L'EVOLUTION DES MENACES ET L'OUVERTURE PROGRESSIVE AU MONDE IP

Les outils de piratage, notamment pour l'interception radio, sont devenus simples et largement accessibles. Ce phénomène est accentué par l'ouverture au protocole IP: s'il apporte une meilleure standardisation, il introduit également des failles qui incitent au recours d'outils de piratage.



RADIO COMS PRO ALLIANCE

POURQUOI SECURISER VOS RESEAUX PMR

› LE DEVOIR DE CONSEIL DES ACTEURS DE LA PMR

Sensibiliser les clients aux vulnérabilités, les accompagner dans la mise en conformité règlementaire, renforcent le positionnement d'expert pour les acteurs de la DMR.



› UNE OPPORTUNITE COMMERCIALE A SAISIR

La sécurisation des réseaux PMR est rémunératrice : vente de licences, vente de produits durcis, prestation de sensibilisation/formation, conduite du changement cyber, etc. La sécurisation devient une opportunité commerciale.



› LA SECURISATION DES RESEAUX : UN IMPERATIF CONCURRENTIEL

Sans offre de sécurité face aux menaces et exigences règlementaires, de plus en plus fortes, les clients se tourneront inévitablement vers la concurrence.



RADIO COMS PRO ALLIANCE

2 COMMENT SECURISER VOS RESEAUX PMR ?

LE COMMENT



RADIO COMS PRO ALLIANCE

COMMENT SECURISER VOS RESEAUX PMR

Des failles existent dans toutes les technologies PMR
Appliquer ces principes de securisation est une réponse necessaire à ces faiblesses

› CONTROLER L'ACCES AUX SERVICES



Une authentification forte (côté utilisateur et côté réseau) permet de lutter contre les intrusions → ***Principe du ZTNA*** (Zero Trust Network Access).
La gestion centralisée des droits permet une réactivité forte face aux pertes, vols ou compromissions d'identités.

› GARANTIR LA CONFIDENTIALITE DES COMMUNICATIONS



Le chiffrement des données est primordial pour assurer la ***confidentialité et l'intégrité*** des échanges. Celui-ci peut-être réalisé sur l'interface radio, mais également de bout-en-bout (E2E).

› GARANTIR LA DISPONIBILITE DES SERVICES



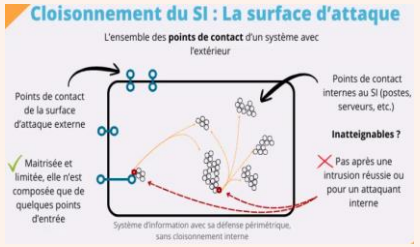
La redondance des équipements critiques doit être prise en compte dans la conception des réseaux, ainsi que l' implementation de mécanismes contre le déni de service.
Le RSSI du client doit être accompagné dans la redaction des Plan de Continuité d'Activité (PCA) et Plan de Reprise d'Activité (PRA).

RADIO COMS PRO ALLIANCE

COMMENT SECURISER VOS RESEAUX PMR

› CLOISONNER & FILTRER LES FLUX

Le cloisonnement des flux & leur filtrage permettent d'éviter la propagation de la compromission et réduisent la surface d'attaque. Le cloisonnement physique est privilégié par l'ANSSI, mais le cloisonnement logiciel reste possible.



› OUTILLER POUR SURVEILLER LES RESEAUX

Un réseau critique doit être surveillé, audité, testé. Ces actions permettent d'anticiper les attaques, et le cas d'échéant, de les analyser pour augmenter la robustesse des réseaux.



› ACCOMPAGNER LA GOUVERNANCE & METTRE EN PLACE DES BONNES PRATIQUES

Le RSSI du client met en place une gouvernance, permettant de maintenir la sensibilisation sur le sujet de la sécurisation.
Elle définit entre autres les protocoles à suivre en cas d'incident critique, désigne les interlocuteurs à contacter, garantit que les bonnes pratiques seront bien appliquées (gestion des mots de passe, verrouillage du parc informatique, politique d'antivirus, startégie de sauvegarde, etc.), s'assure de la sécurité de la supply chain, etc.



RADIO COMS PRO ALLIANCE

3 3 CAS PRATIQUES DE SECURISATION







SECURISATION DU RESEAU DMR

› AUTHENTIFIER LES TERMINAUX

- Implémenter la fonctionnalité ***Link Layer Authentication*** *qui* vérifie l'identité d'un terminal radio avant de lui autoriser l'accès au réseau → ***protection anti-spoofing***

- Activer les fonctions de blocage à distance, temporaire (***Stun***) ou definitive (***Kill***), pour la gestion des terminaux perdus ou volés

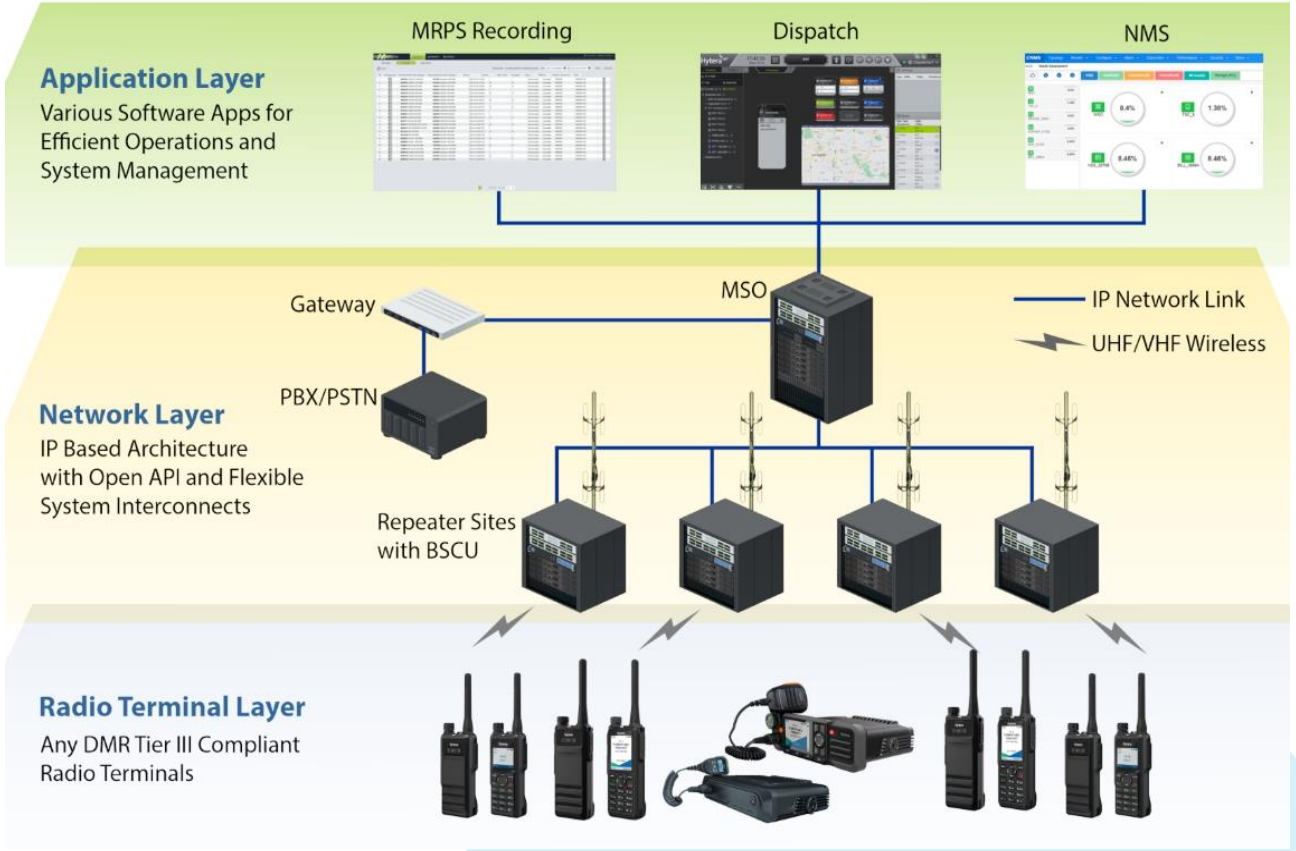
› CHIFFRER LES COMMUNICATIONS

- 3 modes de chiffrement E2E (de terminal à terminal) disponibles : Basic Privacy, Enhanced privacy et Chiffrement AES
- Activer de preference le chiffrement AES car recommandé par l'ANSSI
- Les autres modes de chiffrement sont plus vulnérables

› GERER VOS CLES

- Activer le mécanisme ***OTAR*** (Over The Air Re-keying) qui permet de distribuer et de mettre à jour les clés de chiffrement

- Privilégier les terminaux équipés d'éléments sécurisés pour stocker les clés



Architecture TIER III

Pour plus d'informations: ETSI TS 102 361-4 - V1.10.1

SECURISATION DU RESEAU DMR

› PROTEGER LE COEUR DE RESEAU ET SON INFRASTRUCTURE DE RACCORDEMENT

Le réseau de collecte relie les sites radios, le Coeur de réseau et les applicatifs centralisés (enregistreur, Dispatcher, etc).
Vous devez:

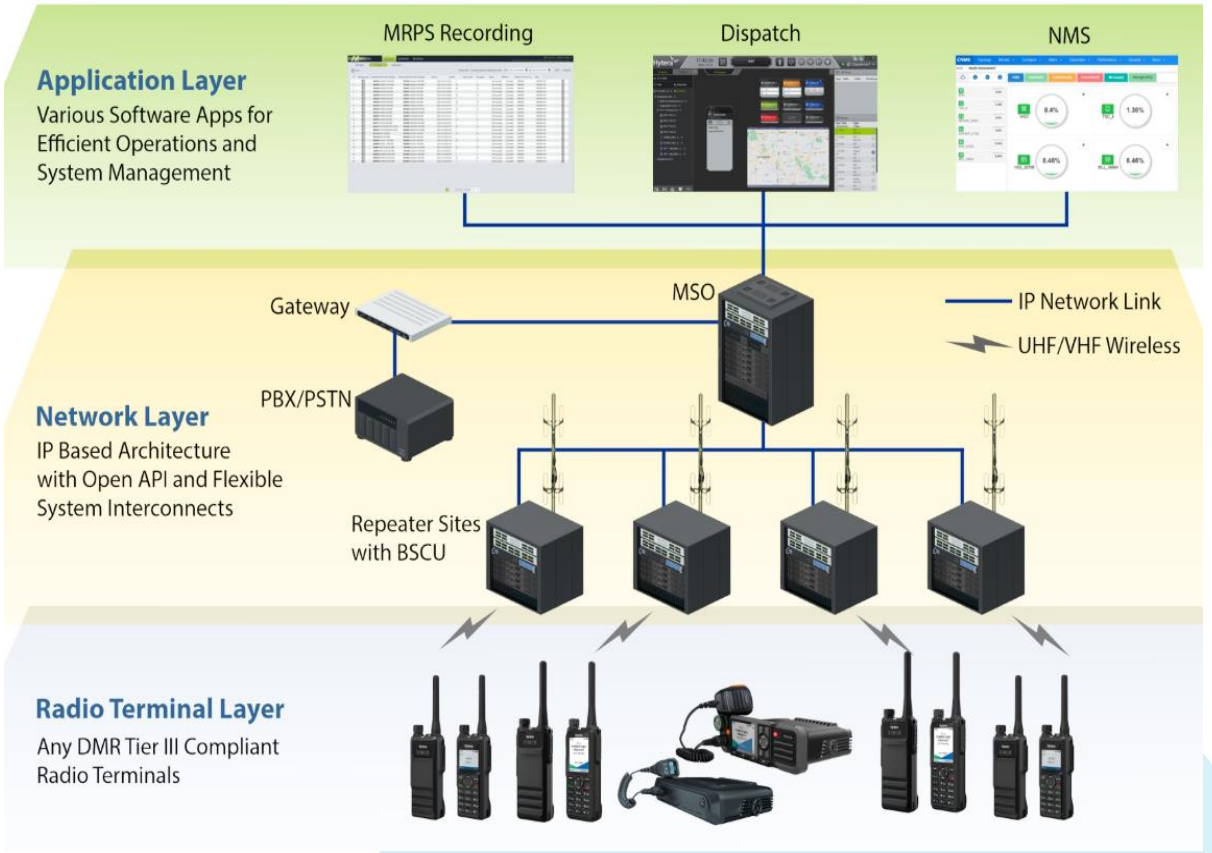
- Activer des mécanismes de chiffrement largement déployés dans le monde IP (IPSEC, TLS, etc.) pour protéger les liaisons généralement en IP
- Redonder vos équipements les plus critiques côté Coeur et applicatifs
- Mettre en place des barrières (mise en place de firewalls pour le filtrage)
- Etc.

› RESILIENCE FONCTIONNELLE INTRINSEQUE

- Les fonctionnalités ***DMO*** (Direct Mode) et ***DMR Gateway*** sont des solutions de resilience

- Elles permettent une certaine autonomie en cas de coupure avec les infrastructures DMR





Architecture TIER III

Pour plus d'informations: ETSI TS 102 361-4 - V1.10.1

SECURISATION DU RESEAU TETRA

› AUTHENTIFIER LES TERMINAUX ET LE RESEAU

- Activer l'authentification mutuelle: le terminal et le réseau s'identifient tour à tour ⟶ Protection ***anti-spoofing*** et ***anti-antenne pirate***

- Activer les fonctions de blocage à distance, temporaire (***Stun***) ou definitive (***Kill***), pour la gestion des terminaux perdus ou volés

› CHIFFRER LES COMMUNICATIONS

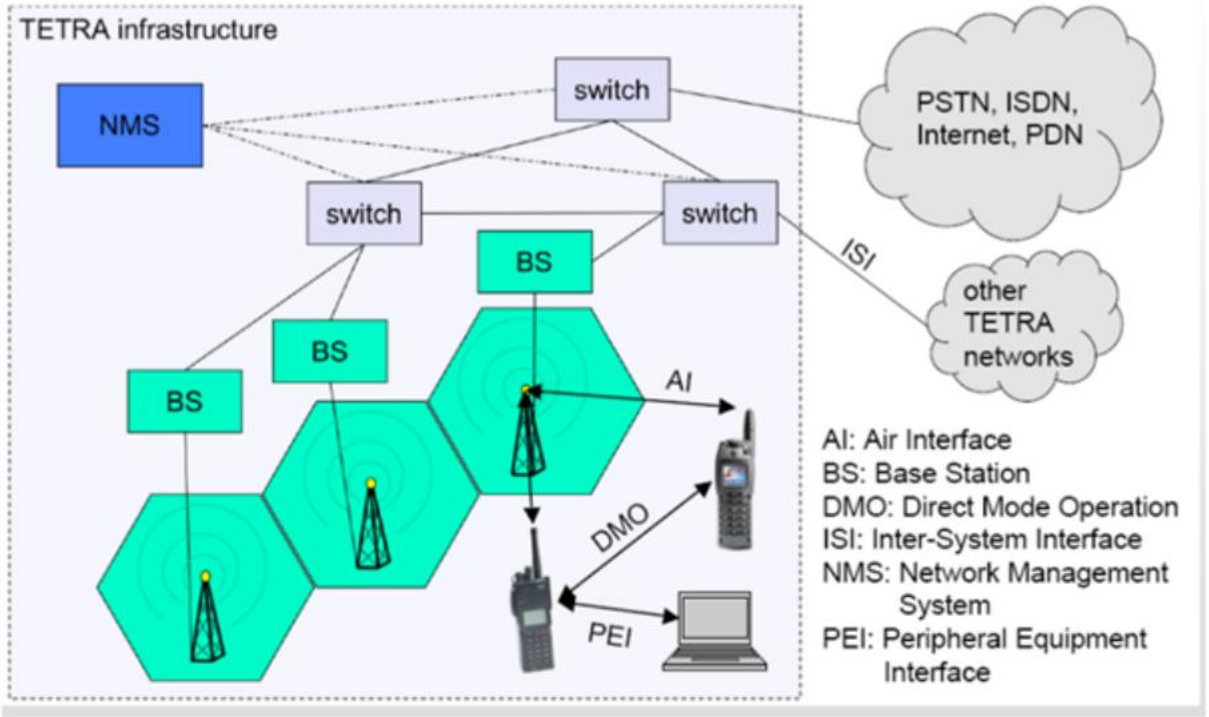
Chiffrement radio: Suite à des publications révélant la faiblesse des algorithmes historiques de chiffrement TETRA, l'ETSI a répondu en sortant 3 nouveaux algorithmes, plus robustes et avec une taille de clé plus grande (80 à 192 bits).

Activer ce chiffrement selon le domaine de vos clients et leur usage :

- Algorithme TEA 7 pour un usage industriel
- Algorithme TEA 5 pour les forces de secours en UE
- Algorithme TEA 6 pour des forces de secours extra UE

Au contraire de la DMR, la signalisation est également chiffrée (protection maximale sur la radio).

Chiffrement de bout-en-bout E2E: Utiliser les algorithmes AES 128 mis à disposition par les constructeurs, voire AES 256 si disponible



› GERER VOS CLES

- Activer le mécanisme ***OTAR*** (Over The Air Re-keying) qui permet de distribuer et de mettre à jour les clés de chiffrement

- Privilégier les terminaux équipés d'éléments sécurisés pour stocker les clés

SECURISATION DU RESEAU TETRA

› PROTEGER LE RESEAU DE COLLECTE ET LE COEUR DE RESEAU

Le réseau de collecte relie les sites radios, le Coeur de réseau et les applicatifs centralisés (enregistreur, Dispatcher, etc).
Vous devez:

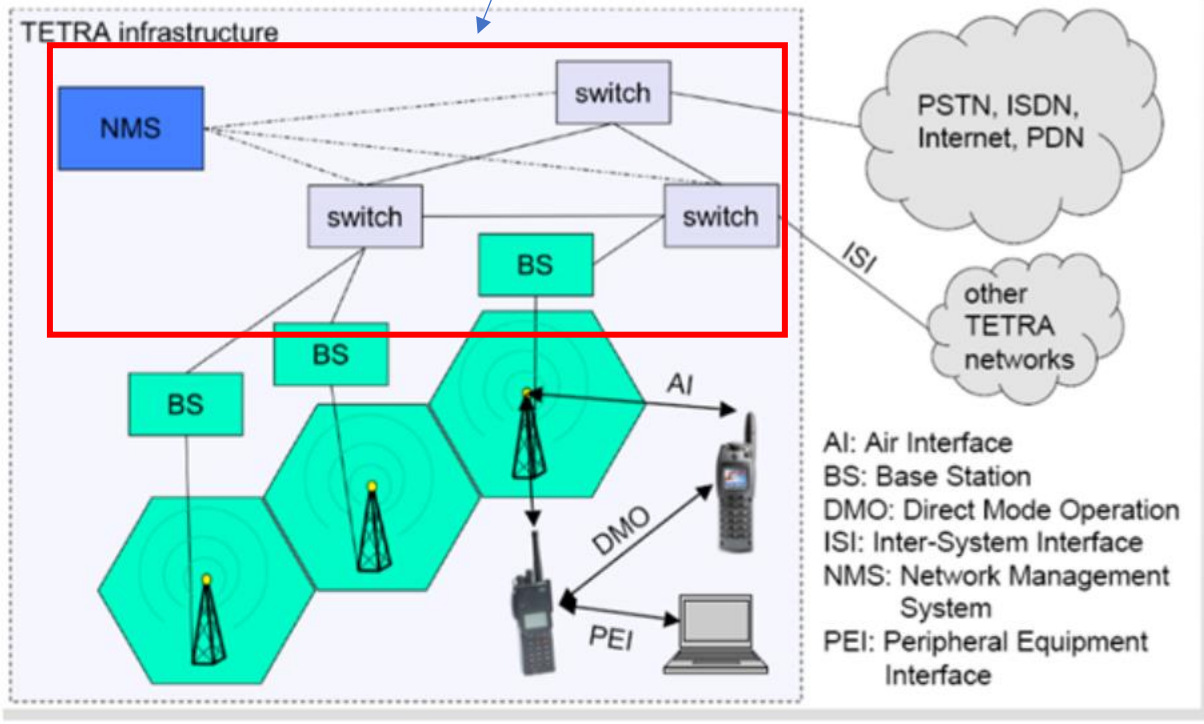
- Activer des mécanismes de chiffrement largement déployés dans le monde IP (IPSEC, TLS, etc.) pour protéger les liaisons généralement en IP
- Redonder vos équipements les plus critiques côté Coeur et applicatifs
- Mettre en place des barrières (mise en place de firewalls pour le filtrage)
- Etc.

› RESILIENCE FONCTIONNELLE INTRINSEQUE

- Les fonctionnalités ***DMO*** (Direct Mode) et ***TETRA Gateway*** sont des solutions de resilience
- Elles permettent une certaine autonomie en cas de coupure avec les infrastructures TETRA



Sécurisation du réseau de collecte et du cœur



RADIO COMS PRO ALLIANCE

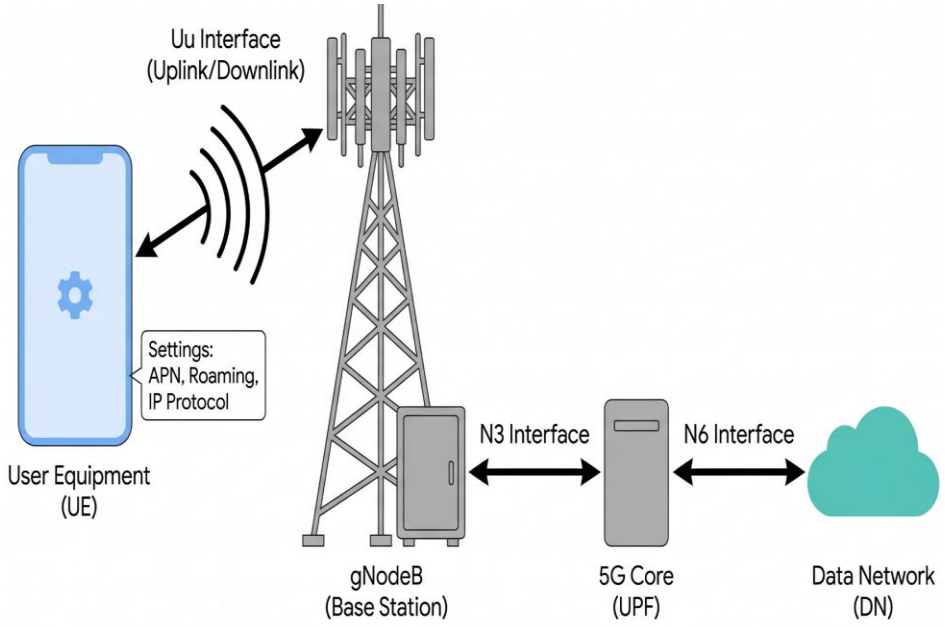
SECURISATION DU RESEAU PMR 5G

› AUTHENTIFIER LES TERMINAUX ET LE RESEAU

- Activer l'authentification mutuelle: le terminal et le réseau s'identifient tour à tour → Protection ***anti-spoofing*** et ***anti-antenne pirate***
- Désactiver les sims et les terminaux perdus ou volés via des fonctions natives de la 5G

› CHIFFRER & PROTEGER LES FLUX A TOUS LES NIVEAUX

- Activer le chiffrement sur la radio avec les algorithmes NEA2 et NIA2 (basés sur AES 128)
- Activer les mécanismes de chiffrement du monde IP (IPSEC, TLS, etc.) pour protéger le réseau de collecte et le coeur de réseau (à redonder)
- Utiliser des logiciels de communication (type Mission Critical) qui apportent une couche de chiffrement supplémentaire → chiffrement au niveau applicatif
- Privilégier pour les usages ultra-critiques, des terminaux avec des OS durcis et customisés
- Etc.



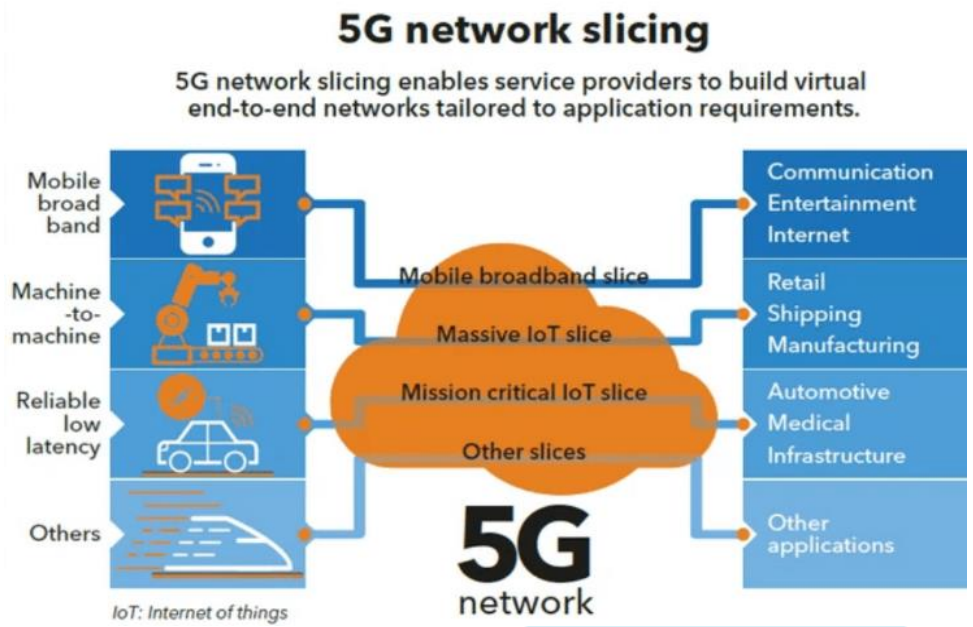
L'écosystème 5G, étant très lié au monde IP et donc à ses vulnérabilités, propose en contrepartie de nombreux mécanismes de sécurité E2E et multi-couches

SECURISATION DU RESEAU PMR 5G

› CLOISONNER LES USAGES

Diviser une infrastructure 5G physique en plusieurs réseaux virtuels (slices ou tranches) dédiés à des usages spécifiques ⟶ Network Slicing

- Le Network Slicing permet une réservation des ressources afin de garantir un niveau de qualité de service défini, pour un usage ou un client donné
- Une tranche de réseau attaquée ne compromettra pas l'ensemble de l'infrastructure → le risque est confiné
- A l'intérieur d'une même slice, des mécanismes de priorisation/préemption sont toujours possibles pour privilégier des utilisateurs en particuliers



RADIO COMS PRO ALLIANCE

CONCLUSION

- La protection des réseaux PMR s’impose désormais comme une nécessité et une opportunité de développement

- *Les règles fondamentales de sécurité sont déjà applicables à la majorité des technologies PMR, toutes générations confondues*