



Les besoins fonctionnels des sapeurs-pompiers dans le cadre du Réseau Radio du Futur (RRF)

Mémoire en vue de l'obtention de la formation de commandant des systèmes d'information et de communication

Commandant Vincent BERGONHE
Brigade des Sapeurs-Pompiers de Paris

Commandant Jean-Albert LAMA
Service départemental d'incendie et de secours de Guyane

Capitaine Frédéric ROOMS
Service départemental d'incendie et de secours de la Moselle

Promotion 2018/01
Directeur de mémoire : Colonel de gendarmerie Bruno CHAPUIS

« Les opinions exprimées dans ce mémoire sont propres à leurs auteurs et n'engagent pas l'École Nationale Supérieure des Officiers de Sapeurs-Pompiers »

Remerciements

Les rédacteurs, pendant leur travail de recherche nécessaire à la rédaction de ce mémoire, tiennent à remercier les acteurs tant locaux que nationaux qui ont permis d'orienter la recherche documentaire des participants à ce mémoire.

Au niveau national, la Mission de Préfiguration du Réseau Radio du Futur (MPRRF) a été en permanence à l'écoute des rédacteurs et s'est investie sans compter pour guider et transmettre les documents pertinents dans l'élaboration de ce document.

C'est pourquoi nous tenons à remercier ce service et en particulier :

- Monsieur Guy DUPLAQUET, chef de la MPRRF ;
- Monsieur le colonel de gendarmerie Bruno CHAPUIS ;
- Monsieur le commandant des sapeurs-pompiers Alain ALBAREZ.

Par ailleurs, nous tenons également à remercier l'ensemble des participants locaux et, en particulier, au sein du SDIS de la Moselle, les agents qui ont contribué par leurs idées et l'expression de leurs besoins à la rédaction de ce mémoire.

Tableau des abréviations

3GPP	:	3rd Generation Partnership Project
ANSSI	:	Agence Nationale de la Sécurité des Systèmes d'Information
BSS	:	Basic Set Service (dans le contexte Wi-Fi)
CODIS	:	Centre Opérationnel Départemental d'Incendie et de Secours
COS	:	Commandant des Opérations de Secours
DGSCGC	:	Direction Générale de la Sécurité Civile et de la Gestion des Crises
EPA	:	Établissement Public Administratif
ERP	:	Établissement Recevant du Public
GED	:	Gestion Électronique des Documents
ESS	:	Extended Set Service
IBSS	:	Independent Basic Set Service
IMS	:	IP Multimedia Subsystems
INPT	:	Infrastructure Nationale Partagée des Transmissions
LTE	:	Long Term Evolution
MBMS	:	Multimedia Broadcast / Multicast Services
MDM	:	Mobile Device Management
MCPTT	:	Mission Critical Push-to-talk
MMS	:	Multi-media Message Services
MVNO	:	Mobile Virtual Network Operator
NFC	:	Near Field Communication
OCT	:	Ordre Complémentaire des Transmissions
OPT	:	Ordre Particulier des Transmissions
OMA	:	Open Mobile Alliance
PMR	:	Professional Mobile Radio
PPDR	:	Public Protection & Disaster Relief
QoS	:	Quality of Service
RIP	:	Relais Indépendant Portable
RRF	:	Réseau Radio du Futur
SCN	:	Service à Compétence Nationale
SMS	:	Short Message Services
ST(SI) ²	:	Service des Technologies et des Systèmes d'Information de la Sécurité Intérieure
TWP	:	Tactical Working Position
VPW	:	VePeaWay
VSAV	:	Véhicule de Secours et d'Assistance aux Victimes
UMTS	:	Universal Mobile Telecommunication Systems

Table des Matières

1	Présentation.....	7
2	Introduction aux réseaux de télécommunication	8
2.1	Les différentes composantes d'un réseau de télécommunication.....	8
2.2	Évolutions technologiques.....	8
2.3	ANTARES et INPT	17
2.4	Présentation du Réseau Radio du Futur.....	25
2.5	Neopol/Neogend : le futur selon la police nationale et la gendarmerie.....	30
3	Besoins fonctionnels des sapeurs-pompiers.....	33
3.1	Préambule	33
3.2	Méthodologie d'identifications.....	33
3.3	Personnels interrogés	34
3.4	Besoins des utilisateurs.....	35
3.5	Description du terminal idéal	43
4	Besoins des administrateurs fonctionnels	47
5	Contraintes d'implémentations	52
5.1	Zones fortement urbanisées : exemple à Paris.....	52
5.2	Guyane.....	55
5.3	Zones frontalières	57
6	Présentation de PC Storm : première brique du RRF	58
6.1	Préambule	58
6.2	Articulation.....	58
6.3	Services offerts	64
6.4	Présentation des lots composants l'offre PC STORM.....	67
7	Perspectives : impacts du Réseau Radio du Futur	71
7.1	D'un point de vue opérationnel	71
7.2	D'un point de vue organisationnel.....	73
7.3	D'un point de vue du développement d'applications	74
7.4	D'un point de vue de la formation.....	74
7.5	D'un point de vue de l'acquisition et de la maintenance.....	75
7.6	D'un point de vue de la structure porteuse	75
8	Conclusion	77
9	Annexes.....	78

9.1	Cartes mentales	78
9.2	Cartes de couverture par les opérateurs commerciaux en Guyane	81
10	Bibliographie	83

1 Présentation

L'Infrastructure Nationale Partagée des Transmissions (INPT) arrive en fin de vie avec un remplacement étalé entre 2023 et 2030. Par conséquent, il est important d'identifier les besoins des sapeurs-pompiers afin que le réseau du futur corresponde à ceux-ci.

Ainsi, au-delà de la présentation du Réseau Radio du Futur et des technologies sous-jacentes, ce mémoire présente les besoins fonctionnels des services d'incendie et de secours dans le cadre du remplacement de l'INPT et vient appuyer le travail réalisé par le commandant ALBAREZ en tant que « Responsable Métier Sapeurs-Pompiers » au sein de la mission de préfiguration du RRF. Ces besoins fonctionnels ont été identifiés par trois sapeurs-pompiers professionnels provenant de trois environnements différents: un environnement urbain très dense (Paris et sa couronne), un département de catégorie A situé en métropole (Moselle) et un département d'Outre-Mer (Guyane).

Les auteurs de ce mémoire ont cherché à se libérer de toute contrainte technique pour imaginer le réseau rêvé. Il en ressort des besoins de communication et des besoins d'administration. Toutefois, il est du devoir des auteurs de signaler qu'il est difficile de se projeter sur des usages et des besoins à horizon de cinq à dix ans car les usages et le monde des télécommunications évolue extrêmement rapidement. En outre, il est important de noter que les besoins identifiés correspondent aux besoins identifiés par les auteurs et n'engagent nullement leur autorité d'emploi ni l'ENSOSP.

En préambule, et afin de mettre en perspective les besoins identifiés, un premier chapitre portant sur la présentation d'un réseau et sur les évolutions technologiques au cours de ces vingt dernières années est présenté. Il comporte également une section de présentation technique du Réseau Radio du Futur tel qu'imaginée au moment de la rédaction.

Les chapitres deux à quatre sont quant à eux consacrés à l'expression des besoins tels que recensés.

Enfin, dans une dernière partie, ce mémoire présente l'état de l'art de la bulle tactique « PC STORM ». Il a paru effectivement opportun de présenter cette solution afin d'illustrer ce qui sera la première brique fonctionnelle du réseau radio du futur.

La notion de « sécurité civile » utilisée dans le cadre de ce mémoire s'entend au sens large et n'est en aucun cas rattachée à la Direction Générale de la Sécurité Civile et de la Gestion des Crises.

2 Introduction aux réseaux de télécommunication

2.1 Les différentes composantes d'un réseau de télécommunication

Le mot « télécommunication » vient du préfixe grec *tele-* (τηλε-), signifiant *loin*, et du latin *communicare*, signifiant *partager*. Par conséquent, nous proposons la définition suivante du réseau de télécommunication :

Ensemble de moyens techniques permettant d'échanger de l'information sous n'importe quelle forme (voix, image, vidéo, document, hologramme, etc.) par l'intermédiaire de services entre un ou plusieurs interlocuteurs (humains ou non) au moyen de dispositifs techniques dédiés appelés terminaux.

Les moyens utilisés par plusieurs interlocuteurs sont généralement regroupés sous l'appellation d'infrastructure. Il est intéressant de noter que les capacités et les services offerts par les terminaux ont évolué concomitamment avec les infrastructures.

2.2 Évolutions technologiques

Les principales caractéristiques des réseaux et des services sont présentés ici pour illustrer la trajectoire avec laquelle ceux-ci évoluent afin de mettre en perspective les avancées possibles au cours des prochaines années.

2.2.1 Réseaux mobiles de 1^{ère} génération

Les réseaux mobiles de 1^{ère} génération fournissaient principalement un service de téléphonie analogique. Pour diverses raisons dont des problèmes de coût et de miniaturisation, ces réseaux ont connu un faible succès commercial [Pujolle2011].

2.2.2 Réseaux mobiles de 2^{ème} génération

2.2.2.1 Réseaux « 2G »

Les services offerts se sont étoffés avec l'apparition des réseaux dits de « 2^{ème} génération / 2G » :

- la voix ;
- les échanges de messages courts appelés *short message services*.

Apparus au début des années 90, ils ont permis le développement des communications mobiles. À cette époque, il existait une différenciation entre les réseaux sans fils (ex : DECT en entreprise et domicile) et les réseaux de couverture nationale. Ces derniers sont appelés réseaux de télécommunications *cellulaires*. En effet, le territoire est divisé en cellules dans lesquelles se trouvent une *station de base* (appelée *Base Transceiver Station, BTS*) comportant des équipements électroniques et une ou plusieurs antennes. Ces différentes cellules sont regroupées entre elles par l'intermédiaire d'un contrôleur de station de base (appelé *Base Station Controller, BSC*). Ces *Base Station Controller* sont eux-mêmes regroupés à des commutateurs appelés *Mobile service Switching Center*). La figure ci-dessous représente l'architecture d'un réseau cellulaire de deuxième génération.

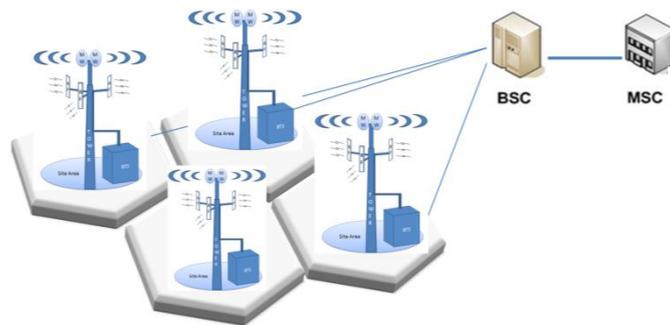


Figure 1: infrastructure d'un réseau de deuxième génération (représentation basée sur des illustrations provenant de)

La mobilité des usagers d'une cellule repose sur deux principes :

- la connaissance de la localisation de l'utilisateur ;
- le transfert d'une cellule appelé *handover*.

À ce titre, le réseau de l'*Infrastructure Nationale Partagée des Transmissions (INPT)* est typiquement un réseau de deuxième génération même si des protocoles propriétaires et des méthodes de modulations spécifiques ont été mises en œuvre par le fournisseur. En outre, comme indiqué, ci-dessous, il dispose de services spécifiques aux forces de sécurité civile.

L'infrastructure des réseaux est prévue initialement pour véhiculer de la voix sous forme numérique. Dès lors, l'infrastructure des réseaux 2G est basée sur des circuits commutés à l'image des réseaux téléphoniques filaires classiques. Par conséquent, lorsqu'une communication est établie entre deux terminaux, le circuit est connu et spécifique aux deux utilisateurs. Il en ressort des difficultés pour dimensionner le réseau et gérer les congestions (i.e. les saturations du réseau).

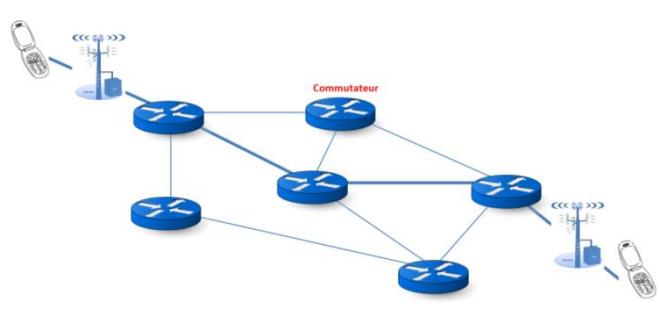


Figure 2: Principe d'un réseau commuté : l'ensemble de la communication suit le chemin établi tout au long de la communication (ici en gras).

2.2.2.2 Réseaux « 2.5G »

Les réseaux dits « 2.5G » ont permis de réaliser une transition vers la 3G en introduisant des services supplémentaires de transport de données. Cette amélioration est connue en Europe sous le nom de *General Packet Radio Services (GPRS)*.

À la différence des réseaux 2G dont le cœur est dédié à la voix, les réseaux 2.5G possèdent un double cœur :

- un premier réseau dédié aux communications téléphoniques classiques ;
- un deuxième réseau dédié aux communications de données.

Le terminal de l'utilisateur est chargé d'émettre des paquets de données sur des intervalles de temps bien précis.

2.2.2.3 Terminaux « 2G » et « 2.5G »

Les terminaux "2G" présentaient des fonctionnalités assez basiques eues égard aux avancées actuelles. Ils permettaient :

- l'émission/réception d'appels téléphoniques ;
- la transmission de messages SMS écrits au moyen d'un clavier "T9" ;
- des clients "mail" basiques.

Par contre, ils consommaient peu de batteries et présentaient des autonomies beaucoup plus importantes que nos smartphones actuels (typiquement quelques jours contre 24h aujourd'hui).

2.2.3 Réseaux mobiles de 3^{ème} génération

2.2.3.1 Réseaux « 3G »

Plusieurs technologies ont été proposées pour réaliser les réseaux de troisième génération dont le déploiement s'est fortement développé à partir de 2005. L'*Universal Mobile Telecommunication Systems* (UMTS) est la solution actuellement dominante et est originaire d'un groupe de travail dénommé *3rd Generation Partnership Project* (3GPP). Les réseaux de troisième génération ont permis un développement important des services :

- transport de la voix ;
- transport de données (image, vidéo, Internet, etc.).

Les débits offerts par l'UMTS sont théoriquement de 2Mbits/s pour une mobilité faible et des conditions radio favorables, 384kbits/s pour une mobilité moyenne et dans un environnement urbain et 144kbits/s dans un environnement rural.

Ces réseaux « 3G » sont également des réseaux cellulaires. De nombreuses similitudes avec les réseaux « 2G » peuvent être observées mêmes si les appellations des équipements ont évolué (ces évolutions s'accompagnant parfois de nouvelles fonctionnalités).

Contrairement aux réseaux « 2G », les réseaux UMTS permettent aux opérateurs de service de développer des services destinés aux utilisateurs en y associant, pour la première fois en téléphonie mobile, la notion de qualité de services (*Quality of Services, QoS*). Cette QoS est basée sur deux critères : la tolérance aux délais de transmission et la tolérance aux erreurs.

2.2.3.2 Réseaux 3G+ et Long Term Evolution (LTE)

La génération « 3G+ » a débuté avec la *release 5* de l'UMTS. L'enjeu est d'assurer une intégration des réseaux mobiles dans le monde IP. À terme, rien ne permettra à un utilisateur de distinguer une connexion téléphonique d'un service classique, ni de distinguer une connexion fixe d'une connexion mobile.

Ainsi, plusieurs évolutions ont été proposées dans ces dernières évolutions :

- l'augmentation des débits (tant montants que descendants) dans la *release 5* de l'UMTS ;
- la possibilité pour un utilisateur d'ouvrir une session multimédia vers un serveur qu'il soit connecté depuis un terminal fixe ou mobile grâce à la notion d'*IP Multimedia Subsystem (IMS)*. Ces sessions peuvent être des communications téléphoniques, des conférences, etc. Pour l'utilisateur, cela se traduit par la possibilité (à long terme) d'un identifiant unique quelle que soit la manière d'accéder au réseau. En outre, les solutions de nomadisme et de continuité de session sont améliorées ;
- la possibilité de diffuser des contenus à plusieurs utilisateurs simultanés tout en économisant les ressources (évitant ainsi la congestion) à l'aide de la notion de *Multimedia Broadcast/Multicast services (MBMS)* ;
- amélioration de la qualité de service (QoS) ;
- l'introduction des services de proximité par l'intermédiaire du *Near Field Communication (NFC)*. Ce standard est aujourd'hui utilisé dans diverses applications telles que le paiement sans contact, le transfert de fichier, l'impression depuis un smartphone, etc.

La version 8 de l'UMTS introduit la notion de *Long Term Evolution (LTE)* sur laquelle s'appuie le projet *Réseau Radio du Futur (RRF)*. Cette version 8 se caractérise par un changement d'utilisation des ressources spectrales et d'un réseau tout IP (sauf pour la partie téléphonique). Il ne s'agit pas encore de « 4G » car la téléphonie n'est pas encore véhiculée en mode IP.

2.2.3.3 Terminaux « 3G »

Ces terminaux sont devenus de véritables ordinateurs. Ils permettent non seulement d'établir des communications téléphoniques classiques mais permettent également d'exécuter des applications complexes telles que la visio-conférence, visualisation de vidéos, traitement de textes, visionnage de fichiers, etc.

Ces applications sont généralement téléchargeables depuis un magasin d'application après approbation préalable de la mise en ligne par le produit de la plate-forme (Google et Apple ayant une position très dominante dans ce domaine). Même s'il est possible d'installer un magasin d'applications alternatif, cette installation est peu aisée et peu d'utilisateurs le font. Il s'agit, dès lors, d'un modèle économique fermé pour lequel des services innovants peuvent être retardés ou ne pas voir le jour à cause du gestionnaire d'applications.

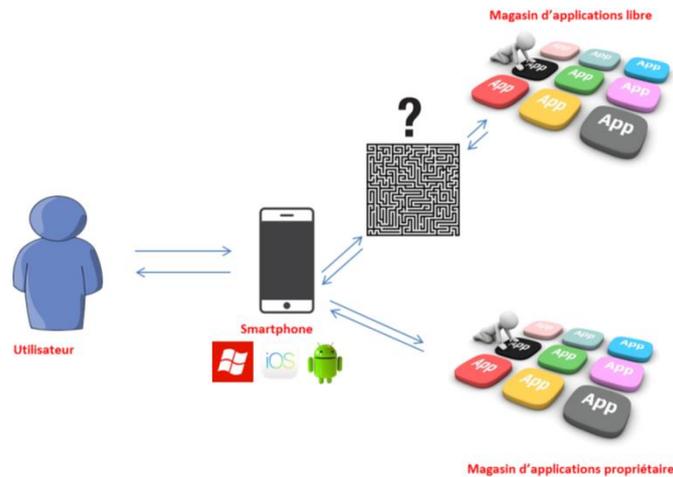


Figure 3: téléchargement et magasin d'applications

Cependant, l'apparition des magasins d'application a très fortement démocratisé l'installation de logiciels, installation qui était généralement l'affaire de spécialistes. À ce titre, tout système d'exploitation installé sur le smartphone doit s'accompagner d'un magasin d'applications avec un catalogue bien fourni. En outre, les utilisateurs ont *de facto* délégué la responsabilité de vérifier l'innocuité des applications au gestionnaire d'applications.

2.2.4 Réseaux mobiles de 4^{ème} génération / LTE Advanced

Les réseaux « 4G » apparaissent avec la *release 10* correspondant au LTE Advanced. Cette génération efface totalement les différences entre les réseaux mobiles et les réseaux fixes avec une compatibilité totale avec le monde IP. La téléphonie est ainsi traitée avec le protocole IP.

D'autre part, la « 4G » introduit une nouvelle technique appelée « *multi-homing* » permettant à un terminal d'être connecté à plusieurs réseaux simultanément (voir Figure 4) sans que ces réseaux soient au courant de la connexion multiple. Bien que cette technique (notamment dans le cas de réseaux hétérogènes) soit identifiée comme une des clefs de la mobilité et de performances pour la « 5G » (Karimi & Al, 2017), les améliorations pour l'utilisateur final ne sont visibles que dans certaines conditions (Finley & Al, 2017).

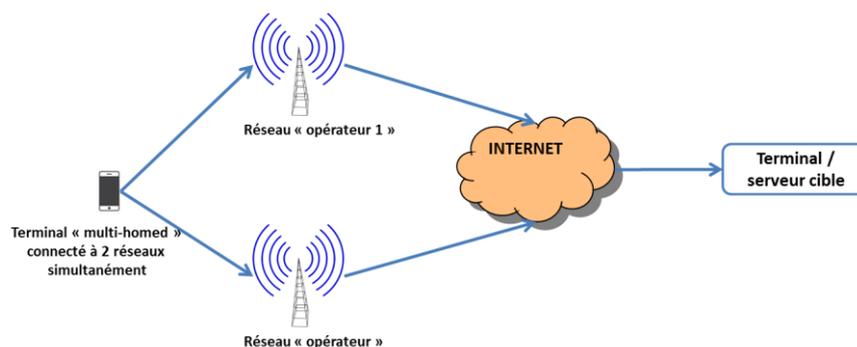


Figure 4 : connexions simultanées sur différents réseaux (*multi-homing*) afin d'améliorer les performances. Une partie des flux est transportée par le réseau « opérateur 1 » et le deuxième par le réseau « opérateur 2 ».

2.2.5 Réseaux mobiles de 5^{ème} génération / LTE Advanced Pro

Même si les réseaux « 5G » ne seront normalisés qu'en 2020, plusieurs grands concepts semblent se dégager :

- l'augmentation des débits grâce notamment à une partie du spectre non utilisée jusqu'à présent et l'augmentation du nombre d'antennes ; chaque antenne étant très directive ;
- le développement des réseaux de type *mesh*. Une explication de ces réseaux est indiquée à la section 2.2.7 ;
- la communication à haut débit d'équipement à équipement ;
- la généralisation des *femtocells* ;
- la virtualisation des équipements réseaux à l'intérieur d'un même opérateur et la possibilité de mutualiser des équipements entre différents opérateurs ;
- le déploiement de *datacenters* à proximité des antennes (*datacenters* appelés dans ce cas *Mobile Edge Computing*) ;
- l'interconnexion massive d'objet (*Internet of Things*).

Parmi ces différents points, il est particulièrement intéressant de noter dans le cadre de ce mémoire que les réseaux hors infrastructures vont se développer de façon importante. Certains chercheurs et visionnaires prévoient même une *ubérisation* des acteurs des télécommunications avec une disparation de ces opérateurs au profit de réseaux ne dépendant plus de leur architecture. A contrario, les opérateurs de télécommunication cherchent à conserver la relation avec leur client et déploient des *datacenters* à proximité des antennes afin de fournir les meilleures performances possibles.

D'autre part, la 5G étend la notion de « missions critiques » ; missions pour lesquelles les performances doivent être garanties.

2.2.6 Prise en compte de la sécurité civile à travers les différentes générations de réseaux mobiles

Depuis 2011 et les travaux de l'*Open Mobile Alliance (OMA)*, différentes fonctionnalités à destination des forces de sécurité civile se sont ajoutées aux réseaux mobiles « grands publics ». Le groupe « 3GPP » s'est servi des travaux de l'OMA pour définir les spécifications techniques connues, depuis la release 13 (publiée en 2016), sous le nom de *Mission Critical Push-to-talk (MCPTT)*.

Parmi ces principales fonctions développées, et disponibles sur tout réseau respectant ces normes :

- les services de proximité (appelé en anglais *ProSe* pour *Proximity Services*) qui permettent à un terminal de découvrir d'autres terminaux à proximité et d'établir des communications de terminal à terminal sans passer par l'infrastructure du réseau. Il convient de noter que la portée de ce mode de communication est limitée à cause de la faible puissance des émetteurs. En outre, une puce spéciale (qui n'est pas disponible dans tous les terminaux) est nécessaire. À ce jour, un seul fabricant propose cette puce à destination des constructeurs de téléphone mobile ;

- les communications de groupe qui permettent la communication d'une personne vers plusieurs destinataires ;
- mission critical PTT (MCPTT) qui proposent un ensemble de services d'administration et de flux (possibilité de prioriser les flux de la sécurité civile, préemption, management de groupes, usage hors réseau, etc.) ;
- Multimedia Broadcast / Multicast Services (MBMS) qui permet de mettre en place des services (notamment dans des groupes de communication) tout en économisant la bande passante ;
- Isolated E-UTRAN Operation for Public Safety (IOPS) qui permet de mettre en place un réseau fournissant les services MCPTT sans dépendre de l'infrastructure.

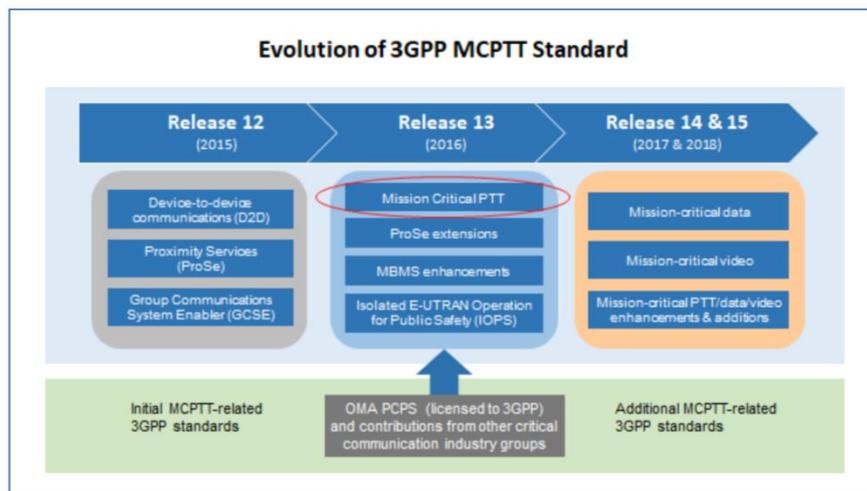


Figure 5 : évolution du MCPTT (voir (Kodiak, 2017))

2.2.7 Réseaux sans fils

2.2.7.1 Réseaux personnels Bluetooth

Issu à la base d'un consortium industriel, le standard *Bluetooth* a fortement évolué au cours du temps. Le développement du standard *Bluetooth* a suivi deux axes différents :

- l'amélioration des performances avec une augmentation des débits passant de 721kbits/s dans la version 1.2 (publiée en 2005) à 2 Mbits/s dans la version 5 (publiée en 2016), une amélioration de la sécurisation (au niveau applicatif et/ou au niveau de la liaison), la découverte de l'environnement ;
- l'apparition d'une version extrêmement économe en énergie avec des performances moindres.

Alors que le standard *Bluetooth* était initialement prévu pour réaliser un appairage entre deux terminaux, il permet aujourd'hui de réaliser de petits réseaux de télécommunication de quelques mètres carrés. Pour ce faire, un terminal devient maître du réseau auxquels les autres terminaux, dits esclaves, se connectent. Une distance d'une dizaine de mètres peut être atteinte en émettant une centaine de milliwatts.

La première méthode pour réaliser un réseau personnel *Bluetooth* consiste à réaliser un *piconet*. Celui-ci est composé d'un terminal maître et jusqu'à huit terminaux esclaves. La communication à l'intérieur d'un *piconet* peut atteindre 1Mbits/s. À noter toutefois que le débit est fonction du nombre de terminaux connectés à l'intérieur du réseau.

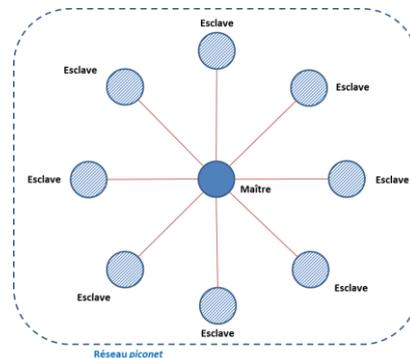


Figure 6: topologie d'un réseau piconet

Plusieurs réseaux de type *piconet* peuvent être assemblés pour constituer un réseau plus étendu (un esclave peut appartenir à deux *piconets* ; un maître dans un *piconet* peut être esclave dans un deuxième). Ces réseaux s'appellent alors *scatternet* (Pujolle, Les réseaux - édition 2011, 2011).

2.2.7.2 Réseaux personnels Wi-Fi

Les réseaux Wi-Fi sont issus d'un ensemble de normes « IEEE 802.11 » issus du groupe de travail éponyme. Les réseaux WI-FI peuvent fonctionner selon deux modes :

- en mode *infrastructure* via un point d'accès ;
- en mode *ad hoc* caractérisé par des liaisons point-à-point.

Le mode *infrastructure* est représenté à la Figure 7. Les terminaux se connectent à un point d'accès dans une cellule qui est appelée dans ce mode *Basic Set Service*. À l'image des réseaux cellulaires, plusieurs cellules peuvent être reliées entre elles pour réaliser un réseau étendu. On parle alors d'*Extended Set Service*. Le système de distribution peut être réalisé de différentes manières.

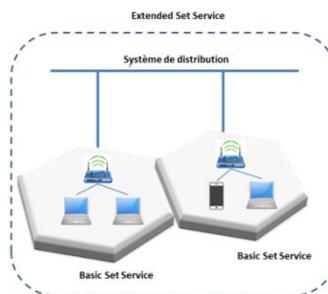


Figure 7: mode infrastructure d'un réseau Wi-Fi

À l'inverse, le mode *ad hoc* ne nécessite pas d'infrastructure : chaque terminal peut communiquer avec un autre. L'ensemble des terminaux regroupés dans la même cellule font

partie d'une cellule appelée *Independent Basic Set Service*. La figure ci-dessous illustre un réseau WI-FI *ad hoc* (appelé aussi parfois appelé *mesh*).

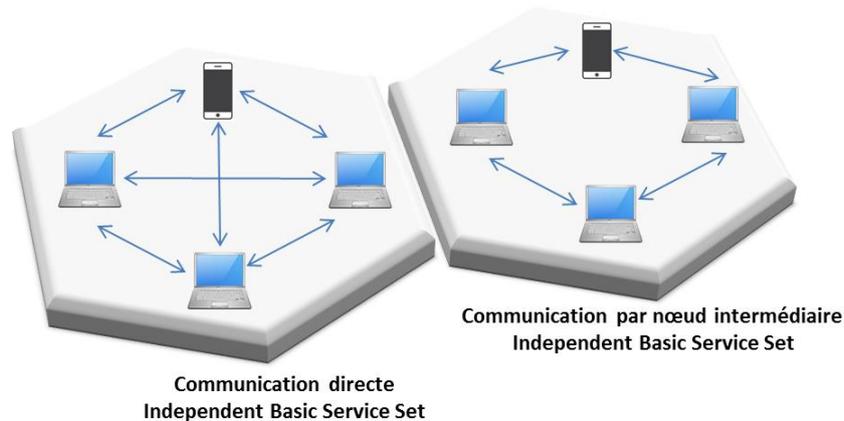


Figure 8: mode *ad hoc* d'un réseau Wi-Fi. A gauche : communication directe entre tous les terminaux. A droite : communication par le biais de terminaux intermédiaires

La qualité de service est un enjeu majeur des réseaux WI-FI. En effet, le débit (et donc les services) se dégradent avec la distance. Malheureusement, les terminaux situés dans une même cellule doivent attendre que les trames aient été émises par le terminal ayant le plus faible débit. Autrement dit, le débit utile de l'ensemble des terminaux est déterminé par le terminal ayant le débit le plus faible.

2.2.7.3 Exemple d'applications dans le monde de la sécurité civile

Les réseaux personnels permettent d'établir très rapidement des réseaux temporaires sans déployer d'infrastructures (comme le montre l'exemple à la Figure 9).

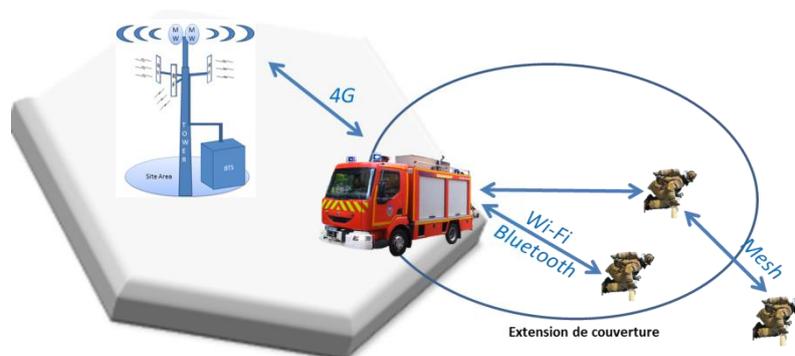


Figure 9: Exemples de communications possibles. Un engin se connecte en tant que client dans une cellule d'un réseau « 4G » et relaie le réseau vers les sapeurs-pompiers à l'avant. Les sapeurs-pompiers situés à l'extérieur de l'extension de couverture peuvent bénéficier de services de télécommunications en se connectant à des sapeurs-pompiers situés à l'intérieur de la couverture.

Toutefois, le contexte des applications de sécurité civile et la nécessité d'une continuité des télécommunications soulèvent quelques questions :

- comment gérer la mobilité et la continuité des communications (ex : entrer ou sortir d'une cellule alors qu'une communication est en cours ?) ?
- quelle autonomie pour les dispositifs communicants ?

- à qui affecter la priorité de communication dans le cas où le terminal est à la fois émetteur (pour ses propres besoins) et relais pour un tiers ?
- comment faire et avertir un sapeur-pompier en dehors de couverture si son relais tombe en panne ?

2.2.8 Conclusion sur les évolutions technologiques des réseaux « grand public »

Les évolutions technologiques illustrent une volonté de convergence et d'unification des usages. Ainsi, cette convergence des services et des réseaux mobiles et fixes se constate quotidiennement. Il est, aujourd'hui, possible d'utiliser un ordinateur portable (connecté à Internet via un point d'accès WI-FI d'une « box » Internet) pour initier une communication par vidéo qui se poursuit sur un téléphone portable relié au réseau Internet par l'intermédiaire d'une connexion 4G sans aucune discontinuité.

L'enjeu des prochaines années est donc d'assurer une continuité des usages quelles que soient les conditions d'accès au réseau (fixe ou mobile, statique ou en déplacement dans un véhicule ou un avion, ordinateur ou smartphone, etc.). Cette continuité des usages devra être assurée quelle que soit la position sur le territoire et quelles que soient les conditions, et tout particulièrement, pendant une crise de sécurité civile. En outre, les évolutions technologiques montrent que tout l'enjeu sera d'utiliser efficacement différents réseaux hétérogènes afin de véhiculer les services souhaités par les utilisateurs.

Alors que le monde de la sécurité civile a, par le passé, construit ses systèmes de télécommunication de manière autonome et indépendant des services grands publics (les usages étatiques étant parfois en avance sur le grand public), il apparaît utopique de vouloir construire un réseau *ex nihilo* totalement déconnecté des autres supports de transmissions.

En effet, les évolutions technologiques et l'importance que revêtent aujourd'hui les télécommunications dans la société civile et l'économie associées au développement de fonctions importantes pour les forces de sécurité civile (MCPTT) montrent que les systèmes commerciaux sont à même de fournir la meilleure solution en termes de performances, résilience et coûts pour autant que quelques précautions et adaptation soient prises.

2.3 ANTARES et INPT

ANTARES (Adaptation Nationale des Transmissions aux Risques Et aux Secours) est le réseau numérique utilisé par la sécurité civile pour communiquer. Il se base sur une infrastructure de deuxième génération partagé par plusieurs services (police, gendarmerie, sapeurs-pompiers, etc.). Basé sur le standard *Professional Mobile Radio (PMR)*, il utilise des technologies et des protocoles propriétaires de la société Airbus afin d'assurer la confidentialité des communications.

Le réseau servant de base à ANTARES s'appelle *Infrastructure Nationale Partagée des Transmissions*. Cette infrastructure est le résultat d'une interconnexion d'une multitude de réseaux départementaux appelés *réseaux de base (RB)*. Le maintien en condition opérationnelle et les évolutions du réseau sont gérés par l'État.

Il est important de noter que ce réseau est réservé à des organisations après approbation par le gestionnaire de réseau. Il en résulte que le réseau (et notamment les capacités des relais, le nombre de relais et d'éléments de commutation, etc.) est défini après que chaque organisation ait défini ses besoins par l'intermédiaire d'un document appelé *Expression du Besoin Opérationnel et Technique (EBOT)*. Par conséquent, la congestion du réseau est très peu probable. Ce point est particulièrement important pour les services d'incendie et de secours qui pourraient être craintifs à l'idée de rejoindre un réseau grand public dans lequel les services ne seraient pas garantis.

2.3.1 Services fournis par l'infrastructure

Ce paragraphe détaille les services proposés par l'architecture. Les fonctionnalités des terminaux (qu'ils soient situés dans un centre opérationnel ou sur le terrain) sont abordées dans la section consacrée aux terminaux. La liste non exhaustive a pour but de mettre en évidence soit des particularités du réseau actualisé, soit des points importants pour les services d'incendie et de secours.

2.3.1.1 Services fournis aux utilisateurs

Pour les utilisateurs, l'infrastructure permet les services suivants :

ANTARES_SERV1	transport de la voix (avec une « commutation de circuit ») : <ul style="list-style-type: none"> • communication à plusieurs audibles par tous les abonnés (ex : <i>talkgroup</i>) ; • communication d'une à quatre personnes en mode privé (ex : appel privé) ; • communication privée vers un interlocuteur situé en dehors de l'INPT ; • capacité de suivre plusieurs communications simultanément avec bascule automatique sur la communication active.
ANTARES_SERV2	transport de données permettant les services suivants : <ul style="list-style-type: none"> • transport des données de géolocalisation ; • transport de status ; • transport de <i>Short Message Service (SMS)</i>.
ANTARES_SERV3	transport prioritaire des appels de détresse (reconfiguration automatique du réseau garantissant la priorité de l'appel de détresse au détriment des communications non urgentes).
ANTARES_SERV4	possibilité aux utilisateurs prioritaires (ex : terminaux des centres opérationnels) de couper une communication et de prendre la parole.

Tableau 1 : liste des services offerts aux utilisateurs par l'infrastructure. A noter que le mode « DIR » n'est pas repris dans ce tableau (mais bien dans la partie « Terminal ») car il est indépendant de l'infrastructure de l'INPT.

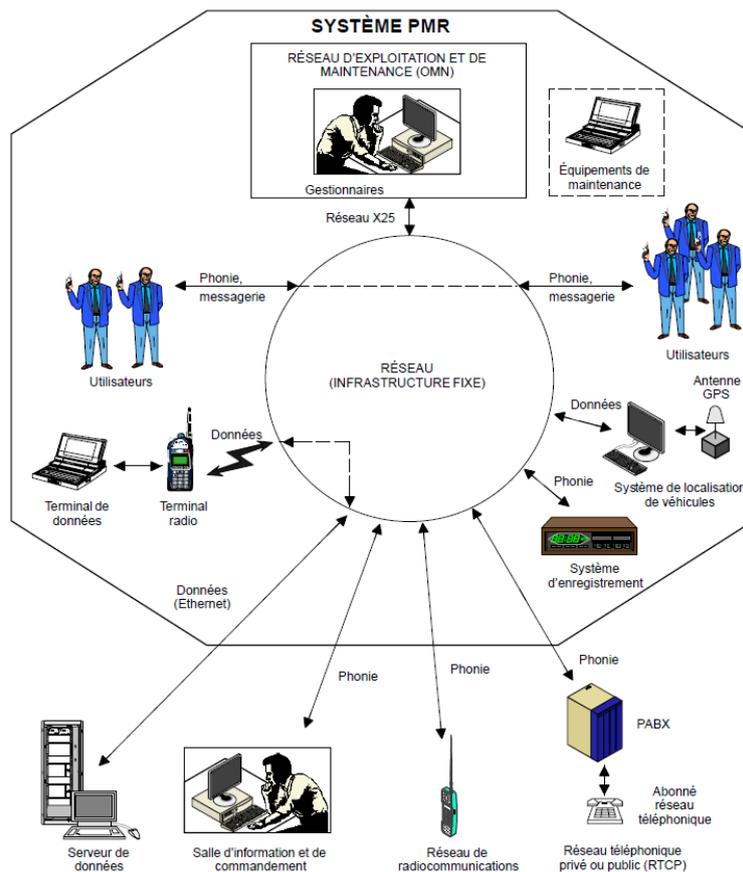


Figure 10: services fournis par le réseau INPT et interconnexions avec le monde extérieur (source : Système PMR – Présentation générale, AIRBUS)

L'infrastructure permet la mobilité des abonnés terrestres (et non celle des moyens aériens).

2.3.1.2 Services fournis aux administrateurs fonctionnels

L'infrastructure offre de nombreux moyens de configuration, de supervision et de sécurisation. Les tableaux ci-dessous listent les principales fonctionnalités utilisées par les services d'incendie et de secours.

Supervision

La supervision peut se faire à différents niveaux par l'intermédiaire d'une station de travail dédiée appelée « TWP ».

ANTARES_SUP1	Supervision de l'état de chacun des relais et des commutateurs.
ANTARES_SUP2	Supervision de l'état des liaisons entre les relais.
ANTARES_SUP3	Supervision des terminaux inscrits sur un relais.
ANTARES_SUP4	Supervision des communications d'un terminal.
ANTARES_SUP5	Supervision de la base de données des terminaux.
ANTARES_SUP6	Supervision de l'activité (en direct et archivée) des terminaux.

Tableau 2 : liste de quelques fonctionnalités de supervision.

Configuration

ANTARES_CONF1	Gestion dynamique des « conférences/talkgroups » à différentes échelles (de quelques relais d'un département, à un réseau de base voire à une échelle supra-départementale). Il est important de noter que la gestion des « conférences/talkgroup » n'est pas aisée et n'est pas aussi dynamique qu'avec des systèmes de visio-conférences/chats actuels.
ANTARES_CONF2	Gestion dynamique des canaux autorisés.
ANTARES_CONF3	Adaptation des droits aux fonctions détenues par l'agent (si dotation individuelle).
ANTARES_CONF4	Configuration de l'interface homme-machine du terminal.
ANTARES_CONF5	Gestion du temps de parole (fonction anti-bavard).
ANTARES_CONF6	Subdivision de la flotte de terminaux en différentes catégories permettant à l'abonné de s'inscrire ou non à une « conférence/talkgroup ».
ANTARES_CONF7	Association de droits spécifiques d'un terminal.

Tableau 3 : quelques fonctionnalités de gestion de l'INPT

Sécurisation et résilience

ANTARES_SEC1	Activer/Désactiver l'accès d'un terminal à des communications à distance.
ANTARES_SEC2	Autoriser/Empêcher l'accès d'un terminal au réseau.
ANTARES_SEC3	Autorisation d'inscription d'un terminal par une clef cryptographique.
ANTARES_SEC4	Fonctionnement à l'intérieur d'une cellule radio en cas de perte de la liaison entre le relais et son commutateur de raccordement
ANTARES_SEC5	Fonctionnement à l'intérieur d'une zone isolée en cas de perte de la liaison entre le commutateur secondaire et le commutateur de gestion.
ANTARES_SEC6	Fonctionnement à l'intérieur du réseau de base en cas de perte de liaison entre le commutateur de gestion et la station de raccordement.
ANTARES_SEC7	Fonctionnement en « relais ouvert » en cas de perte entre l'étage de commande et l'étage « radio » (Herreman & al, 2009).
ANTARES_SEC8	Possibilité de pallier à certaines défaillances du réseau en utilisant des éléments projetables tels qu'un <i>Relais Indépendant Portable (RIP)</i> et/ou une <i>Gatepro</i> (voir 2.3.3).

Tableau 4 : quelques fonctionnalités de sécurisation et de résilience du réseau ANTARES

La confidentialité des échanges (possibilité de cryptage d'une communication de bout en bout) et la sécurisation (authentification des terminaux) est un des points forts d'ANTARES. Toutefois, l'allocation d'une bande de fréquence spécifique diminue la furtivité des forces de l'ordre : l'observation du niveau de puissance émis dans cette gamme de fréquences est un

indice de leur présence à proximité. À ce titre, l'utilisation d'une gamme de fréquences grand public serait un élément d'amélioration.

2.3.2 Infrastructure

2.3.2.1 Généralités

La figure ci-dessous représente les principales caractéristiques du réseau de l'INPT.

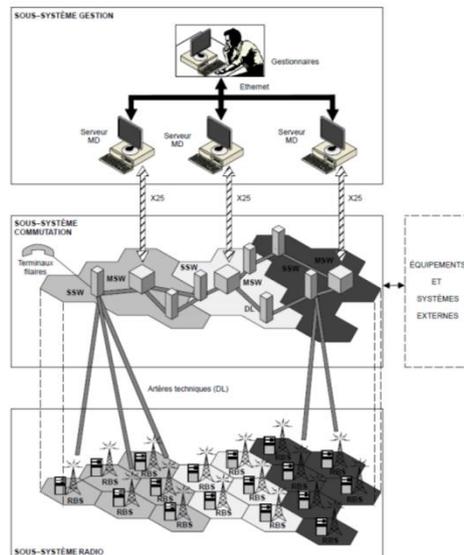


Figure 11 : présentation succincte du réseau de base INPT. À noter que l'évolution en « IP » a eu pour conséquence de modifier cette architecture (Système PMR – Présentation générale, AIRBUS)

Les principales caractéristiques d'un réseau sont (Airbus, 2011) :

- 120 réseaux de base maximum ;
- 20 organisations au maximum ;
- Un réseau de base comprend au maximum :
 - 9 commutateurs dont un commutateur de gestion ;
 - 45 cellules radio ;
 - 20 000 terminaux ;
 - 15 000 terminaux locaux ;
 - 10 000 terminaux de passage.
- Bande de fréquences allouée (380 MHz – 430 MHz et 440 MHz – 490 MHz) ;
- 100 communications de groupe maximum peuvent être établies à un instant donné dans un même réseau de base.

Selon la documentation de la société Airbus (Airbus, 2011),

Le système est entièrement numérique : la phonie est numérisée par un vocodeur interne au terminal avant d'être émise, et reste codée sous forme numérique à chaque étape de la transmission, sur l'interface air entre les terminaux et les relais radio, et sur le réseau fixe (relais radio, artères techniques, commutateur).

Les communications sont réalisées à l'alternat : un seul participant à une communication parle à la fois. Le terminal en émission utilise la voie de trafic et ne peut l'utiliser pour la réception. Par contre, sa voie balise est toujours disponible pour recevoir la signalisation.

2.3.2.2 Relais Radio Indépendant Portable (RIP)

Le relais radio indépendant portable a pour fonction d'établir des communications entre des terminaux radios placés sous sa couverture radioélectrique, appelée cellule. La cellule est fonction de l'antenne, de la puissance d'émission et de la fréquence utilisées.



Figure 12 : valise RIP (source : <http://www.fasstransmissions.com/real/antaresnhc/antaresnhc.php>)

2.3.3 Terminaux

2.3.3.1 Types de terminaux

- **Terminaux portatifs (TPH700, TPH700 ATEX et TPH900)**

Les terminaux portatifs sont des terminaux mobiles autonomes qui permettent à un utilisateur d'accéder à l'ensemble des services offerts par le système TETRAPOL. Il existe différentes générations de terminaux dont la plus répandue au sein des services d'incendie et de secours est le TPH700. Il en existe une déclinaison dite « ATEX » afin d'intervenir en milieu explosif.

Ces terminaux sont associés à une gamme d'accessoires permettant de l'utiliser dans des conditions opérationnelles variées.



Figure 13 : portatif TPH700 de la société AIRBUS (source : manuel utilisateur du TPH700, société AIRBUS)

Ces terminaux permettent de communiquer en se raccordant à une infrastructure mais également en mode *talkie-walkie* sans aucun relais. Un large bouton sur le côté (appelé pédale d'alternat) permet de communiquer aisément (même avec des gants). Il en va de même pour signaler une détresse via un bouton dédié accessible en face avant.

La batterie est facilement remplaçable. En outre, il permet de connecter des accessoires à l'arrière et en *bluetooth*.

Il est important de noter que ces terminaux émettent jusqu'à 2W et qu'ils peuvent être insérés dans un dispositif d'accueil d'une voiture afin d'émettre jusqu'à 10W tout en rajoutant une antenne (gain de réception par conséquence). Il en résulte une portée importante notamment en mode *talkie-walkie* sans avoir à utiliser d'infrastructure permanente ou temporaire.

- **Terminaux mobiles (TPM700)**

Le TPM700 est un terminal mobile autonome relié au réseau INPT par une liaison radio. Ce terminal est prévu pour être installé dans un véhicule et permet d'exploiter le terminal aussi bien à l'arrêt qu'en roulant. Les principales composantes de ce terminal sont :

- un BER (Boîtier Émission Réception) ;
- un organe de commande nommé CH (Control Head) ;
- une antenne de la gamme de fréquence du système (fournie localement ou par le constructeur) ;
- un ensemble d'accessoires audio.



Figure 14 : BER – Modem Radio de la société AIRBUS (source : manuel technique, société AIRBUS)

Ces terminaux émettent jusqu'à 10W. Ils peuvent fonctionner aussi bien en mode relayé (utilisation des relais de l'INPT) qu'en mode *talkie-walkie*.

- **VePeaWay**

Selon la notice utilisateur, « le VePeaWay » réalise une extension de la couverture radio d'un terminal mobile au bénéfice de terminaux radios situés dans une zone mal ou non couverte. Le rôle du VePeaWay est d'établir les communications entre les terminaux situés dans la zone de couverture locale, l'opérateur VePeaWay » et les terminaux participant à la communication situés dans le réseau PMR.

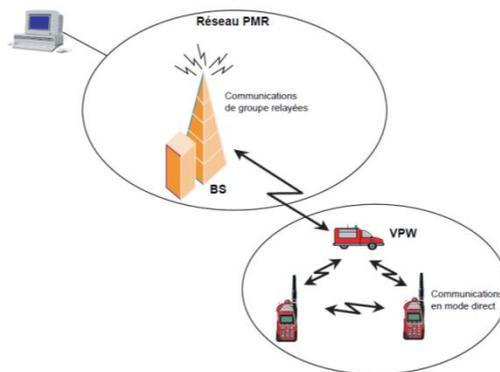


Figure 15 : extension de couverture réalisée par un boîtier VePeaWay (VPW). Source : Manuel Utilisateur VEPEAWAY, Airbus.

- **Gatepro**

La GATEPRO est une passerelle radio entre deux groupes d'interlocuteur (sur un seul réseau ou entre deux réseaux différents). La GATEPRO est un élément mobile pouvant être utilisé sur le terrain de façon totalement autonome (alimentation par batterie, par groupe électrogène et allume-cigare) pour établir des liaisons temporaires ou permanentes.

Elle permet d'étendre une couverture réseau mais aussi de faire le pont entre deux zones isolées renforçant ainsi la résilience du service offert aux utilisateurs. En outre, elle permet de créer des liens entre des utilisateurs situés dans deux réseaux différents. Enfin, elle permet d'interconnecter une communication de type *talkie-walkie* avec une communication relayée.



Figure 16 : extension de couverture réalisée par un boîtier VePeaWay (VPW). Source : Manuel Utilisateur VEPEAWAY, Airbus.

2.3.3.2 Fonctionnalités des terminaux

- **Fonctionnalités des terminaux portatifs (TPH700, TPH700 ATEX et TPH900) et du BER**

Le but de cette section est de mettre en évidence les fonctionnalités qui distinguent ces terminaux d'un « téléphone » classique.

ANTARES_TER1	Accès aux communications via une pédale d'alternat.
ANTARES_TER2	Bouton dédié pour les appels de détresse.
ANTARES_TER3	Rotacteur simplifiant la navigation (notamment avec les gants).
ANTARES_TER4	Géolocalisation via un GPS intégré (TPH900) ou externe (TPH700).

ANTARES_TER5	Détection de la perte de verticalité et fonction « homme mort » (TPH900).
ANTARES_TER6	Annuaire statique (non modifiable à distance).
ANTARES_TER7	Possibilité de crypter les communications.
ANTARES_TER8	Possibilité de rajouter des accessoires soit par un connecteur dédié, soit par <i>Bluetooth</i> .
ANTARES_TER9	Communication de terminal à terminal(-aux) en mode talkie-walkie sans passer par une infrastructure réseaux.

Tableau 5 : fonctionnalités particulières des terminaux ANTARES de type portatifs ou mobiles

Les fonctionnalités des stations mobiles aussi appelées « BER » sont sensiblement identiques.

- **Fonctionnalités des terminaux filaires (*Line Connected Terminal, LCT*)**

ANTARES_TER10	Possibilité d'écouter une conversation à distance sans que l'interlocuteur réalise une action (écoute d'ambiance).
ANTARES_TER11	Possibilité de préempter la parole pour un opérateur radio (mode station directrice).

Tableau 6 : fonctionnalités particulières des terminaux LCT

2.4 Présentation du Réseau Radio du Futur

2.4.1 Introduction

La notion de « RRF » comprend plusieurs éléments différents[RRF2018] :

- la structure juridique portant le projet et qui exploitera les futurs services et réseaux ;
- les réseaux de télécommunication au sens de l'infrastructure ;
- les services offerts par l'infrastructure.

2.4.2 Du point de vue administratif et financier

Le projet « Réseau Radio du Futur » sera porté par une structure porteuse non définie à la date de rédaction de ce mémoire. Il s'agira soit d'un Établissement Public Administratif (EPA) ou bien d'un Service à Compétence Nationale (SCN).

En ce qui concerne l'EPA, il est « une personne morale de droit public gérant un service public spécialisé, distincte de l'État, et des collectivités territoriales, mais rattachée à eux» (définition du Professeur Pierre-Laurent Frier à la fin du XXe siècle). Ils sont soumis à trois principes :

- ils sont autonomes et disposent à ce titre d'un budget et d'une organisation propres ;
- ils sont rattachés à un niveau de l'administration (État, région, département ou commune) ;
- ils sont spécialisés *i.e.* les compétences sont clairement énumérées et délimitées.

La catégorie des Services à Compétence Nationale a, quant à elle, été créée par le décret n°97-464 relatif à la création et à l'organisation des services à compétence nationale. La circulaire de monsieur le Premier Ministre du 9 mai 1997 précise, qu'« *il existe dans de nombreux ministères des missions de gestion, d'études techniques, de production de biens ou de prestation de services, ainsi que d'autres missions à caractère opérationnel, qui n'entrent*

pas dans le rôle des administrations centrales tel qu'il est défini par le décret no 92-604 du 1er juillet 1992 (b) modifié portant charte de la déconcentration. Or, il s'agit de missions qui présentent un caractère national et ne peuvent être, par conséquent, déconcentrées au niveau territorial » (Juppé, 1997).

Ces services « *peuvent se voir confier des fonctions (...) correspondant aux attributions du ministre sous l'autorité duquel ils sont placés* ». Ils sont créés soit par décret ou arrêté suivant l'autorité à laquelle ils sont rattachés. Ce décret ou cet arrêté de création « *fixe les missions et l'organisation générale de celui-ci* » (Juppé, 1997).

L'échéancier de la création de la structure porteuse est le suivant :

- 2017 : démarrage des travaux ;
- 2018 : nomination du préfigurateur, création et montée en charge de la structure porteuse ;
- 2019 : montée en charge de la structure porteuse ;
- 2020 : fin de la montée en charge.

Comme le déclare Mme Villebrun (Villebrun, 2018), « *la gestion du RRF sera ainsi assurée par une structure porteuse dédiée, qui proposera aux diverses directions et services utilisateurs éligibles de bénéficier de l'offre de service que représente le RRF en contrepartie d'une contribution financière* ». Ces utilisateurs pourraient ainsi être la DGSCGC, les services d'incendie et de secours, etc.

Les missions envisagées du RRF sont les suivantes :

- fournir un service de télécommunication haut débit basé sur des technologies standardisées, utilisant des infrastructures opérées par des opérateurs commerciaux et par le RRF lui-même ;
- assurer et participer à la définition des normes techniques relatives aux équipements du réseau de radiocommunication, au contrôle et à l'évaluation de leur application, la contribution à leur évolution et à la surveillance de l'interopérabilité des dispositifs techniques correspondants ;
- assurer et animer la veille technologique, de la recherche et du développement, de la normalisation dans le domaine des réseaux de radiocommunication, PMR et communications sans fil ;
- coordonner des activités d'hébergement et de déploiement des services ;
- assurer la cohérence du système de communication associé aux réseaux radio de l'État, dans le cadre plus général des orientations du Système d'Information d'État ;
- assurer l'urbanisation, l'architecture et l'ingénierie du réseau de radiocommunication de sécurité et de secours de l'État ;
- élaborer des conventions de service avec l'ensemble des entités utilisatrices ;
- élaborer et assurer un catalogue d'offres de services recommandés par le réseau de radiocommunication.

La gouvernance de la structure reste à définir selon qu'il s'agit d'un EPA ou d'un SCN.

D'autre part, le modèle organisationnel de l'EPA prévoit une mutualisation des ressources et compétences (recours aux services/directions du ministère pour assurer des fonctions du RRF).

M. Guy Duplaquet est le responsable de la mission de préfiguration du RRF. Celui-ci a estimé ce projet à 1,5 milliards d'euros sur 20 ans.

2.4.3 Du point de vue technologique

Le RRF est conçu comme un réseau mixte (une partie dépendant de l'État et une partie opérée par un ou plusieurs opérateurs commerciaux) basé sur une stratégie de résilience à deux axes complémentaires (MI, 2018) :

- un appui massif sur les infrastructures des opérateurs commerciaux. Ainsi un terminal peut se connecter à plusieurs opérateurs (augmentation de la résilience en se connectant à plusieurs réseaux) ;
- des réseaux tactiques projetables opérés directement par les équipes du ministère de l'Intérieur en complément de couverture et/ou de capacité, y compris en dernier recours (crise de sécurité civile).

La figure ci-dessous représente les 4 scenarii envisagés pour fournir des services aux utilisateurs.

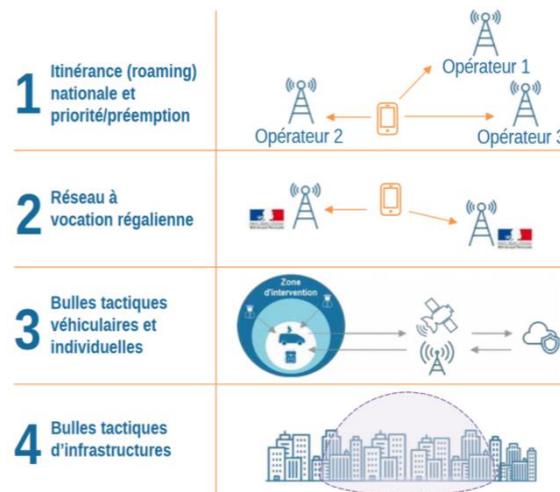


Figure 17 : cas de figures envisagés par la mission de préfiguration pour assurer la couverture.

Comme indiqué à la section 2.2.6, dans le cas où un réseau opérateur commercial est utilisé (scénario 1 de la Figure 17), il est nécessaire de rajouter les fonctions *MCPTT* pour assurer notamment la préemption et la priorisation. Cela sera réalisé à travers un serveur *MCPTT* hébergé par des infrastructures étatiques redondantes et sécurisées.

En outre, dans les zones qui auront été définies comme sensibles (scénario 2), les réseaux opérateurs seront complétés par un réseau étatique afin de garantir la résilience. Les fréquences dites «*Public Protection & Disaster Relief / PPDR* » dédiées au ministère de

l'Intérieur seront préférentiellement utilisées même si les fréquences opérateurs pourront être utilisées.

Des équipements pourront être installés dans les véhicules afin de créer des bulles tactiques véhiculaires et individuelles (scénario 3). Les fréquences *PPDR* seront utilisées (même si la mission de préfiguration n'exclut pas l'utilisation de fréquences opérateurs). Ces bulles tactiques permettront de communiquer autour d'un engin (avec un rayon d'action dépendant des conditions environnementales). A ce jour, la fourniture des services *MCPTT* est sujette au résultat de l'étude sur les coûts de l'*IOPS* (voir section 2.2.6). Ces bulles tactiques véhiculaires correspondent peu ou prou aux équipements *VePeaWay ANTARES* (voir section 2.3.3).

Les bulles tactiques d'infrastructures (scénario 4) utiliseront également les fréquences *PPDR* et disposeront des services *MCPTT* en intégrant les fonctionnalités *IOPS*. Elles seront donc totalement indépendantes d'un accès en cœur de réseau (qu'il soit opéré ou régalién).

Ces bulles tactiques d'infrastructure seront déployées grâce aux solutions retenues dans le marché « *PC STORM* » en cours de notification et sont décrites à la section 6. Même si ces réseaux tactiques sont initialement prévus pour être utilisés en cas de crise de la sécurité civile (réseau tactique projetable), ils pourront être utilisés pour compléter et ou sécuriser les réseaux commerciaux.

À noter que les modalités de mise en œuvre des communications tactiques est actuellement à l'étude et que des solutions de type « mode directe » en mode *ProSe* (voir 2.2.6) ou en mode *mesh* (voir 2.2.7) sont également à l'étude.

2.4.3.1 Terminaux

Le choix des réseaux de télécommunications « standards » permettra d'acheter des terminaux grands publics (« *smartphones* » ou non selon les besoins et fonctions). Les services d'incendie et de secours pourront ainsi réduire les coûts en évitant l'achat d'un matériel fabriqué en petite série par un unique fournisseur.

Le choix actuel de la mission de préfiguration porte sur des terminaux exécutant le système d'exploitation *Android* dans sa version standard. À la différence d'autres services (principalement police et gendarmerie), les terminaux des services d'incendies et de secours n'utiliseront pas la version sécurisée d'*Android* appelée *secdroid* et développée par le *Service des Technologies et des Systèmes d'Information de la Sécurité intérieure (ST(SI)²*. La sécurisation de cette version *secdroid* est étudiée par l'*Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI)*.

Toutefois, si le service *ProSe* devait être retenu pour les communications de terminal à terminal (sans passer par l'infrastructure réseau), cela limiterait le nombre de marché car ces téléphones nécessitent une puce spéciale qui n'est disponible que dans certains terminaux. Des solutions sont actuellement à l'étude pour communiquer de terminal à terminal sans utiliser le service *ProSe* et bénéficier ainsi du plus grand choix possible.

Les services d'incendie et de secours pourront développer une stratégie de différenciation des équipements en fonction de l'engin et des fonctions des personnels.

2.4.4 Du point de vue des services et des fonctionnalités

Le RRF se distingue par le choix d'un système grand public renforcé pour remplir les besoins de la sécurité civile. Par conséquent, et à l'opposé du système ANTARES actuel, il sera potentiellement possible de développer un nombre infini d'applications disponible au téléchargement par l'intermédiaire d'un magasin d'application sans être contraint et/ou nécessiter une prestation de la part d'un industriel maîtrisant de bout en bout un environnement fermé. L'EPA en charge du RRF pourra ainsi avoir le contrôle d'un magasin dédié et de superviser le développement d'applications dédiées.

Au-delà des traditionnels services d'un système de communications, la souplesse et les performances laissent entrevoir de nombreux services :

- outils d'aides à la décision ;
- applications métiers embarquées.

L'usage sera également simplifié par le choix de smartphone grand public déjà utilisé et connu par une grande majorité de la population. *A contrario* de la situation actuelle, nous pouvons supposer que les utilisateurs s'approprient plus fortement leurs terminaux.

D'autre part, la liberté dans le choix du matériel laisse supposer le développement de services complémentaires en fonction des capacités des terminaux (notamment en termes d'écosystème de composants, de capteurs et d'outils connexes).

Les limites du RRF ne semblent donc plus se situer au niveau technique mais bien dans l'imagination et la capacité à développer (et/ou faire développer) les services répondant à nos besoins.

Ces services pourraient être accessibles directement depuis Internet ou par l'intermédiaire d'applications (modalités définies par la suite). Ces applications, développées par diverses entités, pourraient être validées par la structure porteuse avant d'être publiées dans le magasin d'application. Elles seraient ensuite téléchargeables par toute personne en ayant les droits. Les services d'incendie et de secours pourront déterminer librement les applications installées suivant l'utilisation faite des terminaux (ex : applications différentes pour un chef d'agrès et un chef de colonne).

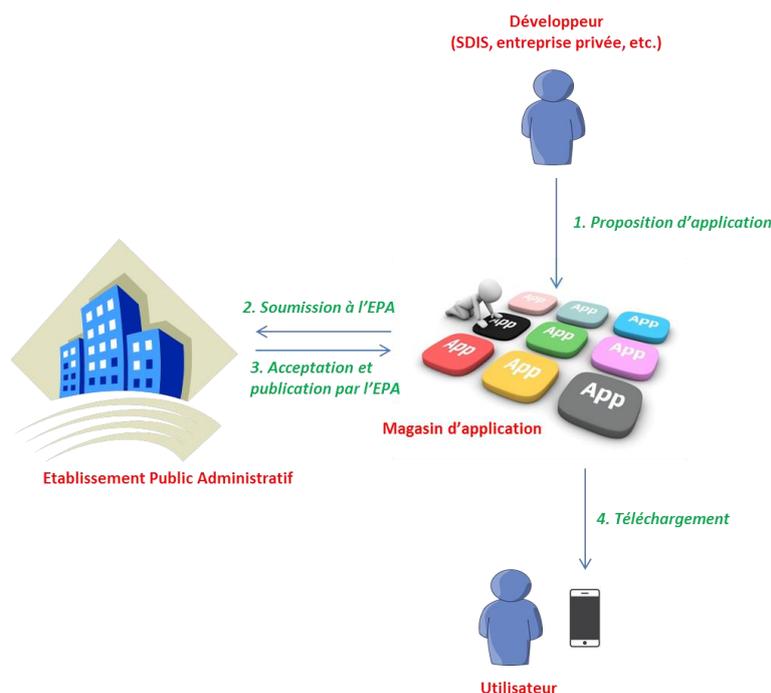


Figure 18 : exemple de principe du développement d'applications et de téléchargements (une solution parmi d'autres envisagée pour répondre aux besoins des utilisateurs)

L'objet de ce mémoire consiste à identifier les besoins fonctionnels. Une véritable rupture se situe dans la manière même de préparer l'avenir : il est nécessaire de penser et de définir les usages ainsi qui seront satisfaits par des applications fonctionnant sur un terminal versatile et simple d'utilisation.

2.5 Neopol/Neogend : le futur selon la police nationale et la gendarmerie

2.5.1 Présentation générale

La police nationale et la gendarmerie, appuyées par le ST(SI)², ont initié cette démarche. Dans le cadre de ce mémoire, nous avons assisté à une réunion de présentation du projet « Neopol » par la préfecture de police de Paris.

Ce projet consiste à fournir à fournir un poste de travail mobile sous forme d'applications accessibles via un smartphone ou tablette en utilisant une version sécurisée d'Android appelée *secdroid*. Le terminal se connecte à un réseau de télécommunications soit en 4G, soit via un point d'accès WI-FI. Il préfigure ce que permettra le futur RRF sans bénéficier de la résilience ni des bulles tactiques (voir section 2.4.3). À ce titre, ces terminaux ne se substituent pas à l'utilisation du réseau ACROPOL pour les communications opérationnelles.

Étant connectés à un réseau commercial, le service est disponible sous formes d'abonnements :

- pour les smartphones :
 - 1,55 € hors taxe/mois pour 5 h ;
 - 10,80 € hors taxe/mois pour 5 Go à haut débit, débit réduit au-delà.
- pour les tablettes :
 - 11,00 € hors taxe/mois pour 6 Go à haut débit, débit réduit au-delà.

La flotte composée de 13 000 terminaux grand public (smartphone SONY EXPERIA X et tablette SONY EXPERIA Z4) d'ici fin 2018 est distribuée de manière individuelle et collective. Dans le cas d'une dotation individuelle, le policier peut le conserver sur lui à tout moment sous réserve d'autorisation par sa direction d'emploi.

La maintenance en conditions opérationnelles est assurée par le CESAR. Cette maintenance porte sur les points suivants :

- casse et panne matérielle ;
- difficultés d'accès aux services ;
- changement d'affectation d'un terminal ;
- carte SiM téléphonique défectueuse ;
- perte ou vol de terminal ;
- déblocage du terminal en cas de multiples saisies erronées des codes d'accès.

2.5.2 Services disponibles

2.5.2.1 Pour les utilisateurs

Afin d'identifier les besoins, toutes les directions ont émis leur besoin. Il en a résulté une feuille de route mise en œuvre en collaboration avec le ST(SI)².

La préfecture de police a ainsi identifié besoins et différents services ont été fournis :

- applicatifs génériques tels que :
 - partage de fichier sur le *cloud* ;
 - messagerie instantanée ;
 - géolocalisation ;
 - etc.
- applicatifs métiers tels qu'interrogations de fichiers et de base de données, rédaction de comptes-rendus, outils d'aides à la décision inter-actifs (ex : identification d'armes à feu) ;
- applicatifs techniques tels que des notifications de type *push*, de la reconnaissance vocale, des systèmes de dictée, etc. ;
- travaux afin de renforcer l'ergonomie.

2.5.2.2 Pour les administrateurs

Un outil spécifique, appelée *NEOPARC*, a été développé avec le soutien du ST(SI)². Cette application permet de connaître précisément l'état du parc (IMEI, modèles, quantités, affectations, statut opérationnel ou *spare*, etc.).

Cette application offre des indicateurs tels que :

- la fréquence d'utilisation des applications ;
- les types de réseaux utilisés (3G, 4G, etc.) ;
- les volumes de données échangées sur des bases de données métiers (indicateurs de l'interrogation globale de celles-ci) ;
- le nombre d'interrogations des bases de données métiers ;
- le nombre d'interrogations par services.

2.5.3 **Retours d'expériences**

Le groupe de rédaction a pu échanger avec des utilisateurs et des gestionnaires de la préfecture de police en charge de Neopol. Les premiers retours sont principalement positifs :

- une appropriation très aisée par les utilisateurs ne nécessitant pas de formation grâce au choix d'un système d'exploitation intuitif et très proche de la version « grand public » d'Android ;
- une simplicité appréciée par tous les utilisateurs ;
- un véritable engouement du personnel qui y voit un moyen d'accéder à de la documentation contextuelle et un gain de temps.

Toutefois, le choix d'un réseau grand public n'offrant aucune résilience a été pointé. En effet, le service n'est pas garanti en cas de saturation du réseau. Transporter ces outils et informations via le réseau radio du futur permettra de remédier à ce point faible.

3 Besoins fonctionnels des sapeurs-pompiers

3.1 Préambule

Les besoins identifiés ci-dessous résultent de réunions des personnels en tête-en-tête et d'analyse par les services compétents (opérationnels et techniques). Cette liste de besoins se veut la plus complète possible même si elle ne prétend pas être exhaustive ; ambition qui requiert un travail plus important. En outre, ce travail devrait être continuellement réactualisé pour tenir compte des évolutions des usages et des possibilités techniques.

Les besoins identifiés par le personnel ayant participé à ce travail n'engage nullement les services d'incendie et de secours pour lesquels les auteurs de ce mémoire travaillent. Ce document ne constitue en aucun cas une expression de besoin ou une position officielle de la part de ces services.

3.2 Méthodologie d'identifications

Une partie des besoins fonctionnels résulte de réunions soit en tête-à-tête, soit en groupes. Les participants à la réunion ont été soumis à trois grandes catégories de questions:

- « *Comment et avec qui imaginez-vous communiquer demain en tant que...* » où la personne interrogée est positionnée le cas échéant en tant que chef d'agrès, chef de groupe, chef de colonne, officier CODIS, officier d'astreinte direction, etc. afin de faire émerger les besoins fonctionnels des utilisateurs.
- « *Si vous aviez une baguette magique, quel serait, selon vous, le terminal idéal ?* » afin de faire émerger les besoins fonctionnels des terminaux.
- « *Si demain, vous deviez gérer une flotte de terminaux pour le SDIS, quelles seraient les fonctions que vous pensez nécessaires et qui vous permettraient d'effectuer votre mission efficacement ?* » afin de faire émerger les besoins des administrateurs fonctionnels.

À partir de ces questions, d'autres (non préparées préalablement et en lien direct avec les affirmations/propositions de la personne interrogée) ont été posées afin de développer les pistes évoquées. Afin de contourner les difficultés qu'ont éprouvées certaines personnes, les questions ont été reformulées de la manière suivante :

- « *Que voudriez-vous faire demain et que vous ne pouvez pas faire aujourd'hui ?* » ;
- « *Quelles sont vos frustrations actuelles ?* » ;
- « *Comment pourrait améliorer le système actuel ?* ».

Au préalable, il a été rappelé aux participants les règles suivantes :

- liberté totale d'imagination (« aucune mauvaise idée ») ;
- se projeter dans le futur et ne pas penser au système actuel ;
- penser « fonctionnalité » et non pas « technique » ;
- toute remarque est bonne à dire ;
- aucun jugement sur la pertinence de la proposition ;

- aucun filtre de la part de la personne menant l'entretien ;
- possibilité au menant de reformuler une affirmation/proposition de la personne interrogée pour s'assurer de la bonne compréhension de l'affirmation/proposition.

À ces réponses, les besoins identifiés par les auteurs du mémoire ont été ajoutés.

L'ensemble des réponses a ensuite été collecté et traité afin de les présenter de manière synthétique dans ce document.

3.3 Personnels interrogés

Au sein du SDIS de la Moselle, les personnels suivants ont été interrogés :

- le directeur départemental, chef de corps ;
- un officier supérieur responsable chargé de la recherche et du développement ;
- un officier supérieur responsable occupant les fonctions « astreinte de direction » ;
- un officier supérieur responsable du Département des Systèmes d'Information ;
- deux chefs de groupes ;
- 4 chefs d'agrès « tout engin » ;
- 2 chefs d'agrès « une équipe » ;
- le responsable des systèmes de radiocommunications du SDIS de la Moselle (ingénieur).

Emploi opérationnel	Nombre de personnes interrogées
Chefs d'agrès « une équipe »	2
Chefs d'agrès « tout engin »	4
Chefs de groupes	2
Chefs de colonne	1
Chefs de site	4

Tableau 7 : nombre de personnes interrogées par catégorie d'emploi

3.4 Besoins des utilisateurs

Les besoins des utilisateurs identifiés par le personnel interrogé sont représentés à la figure ci-dessous.

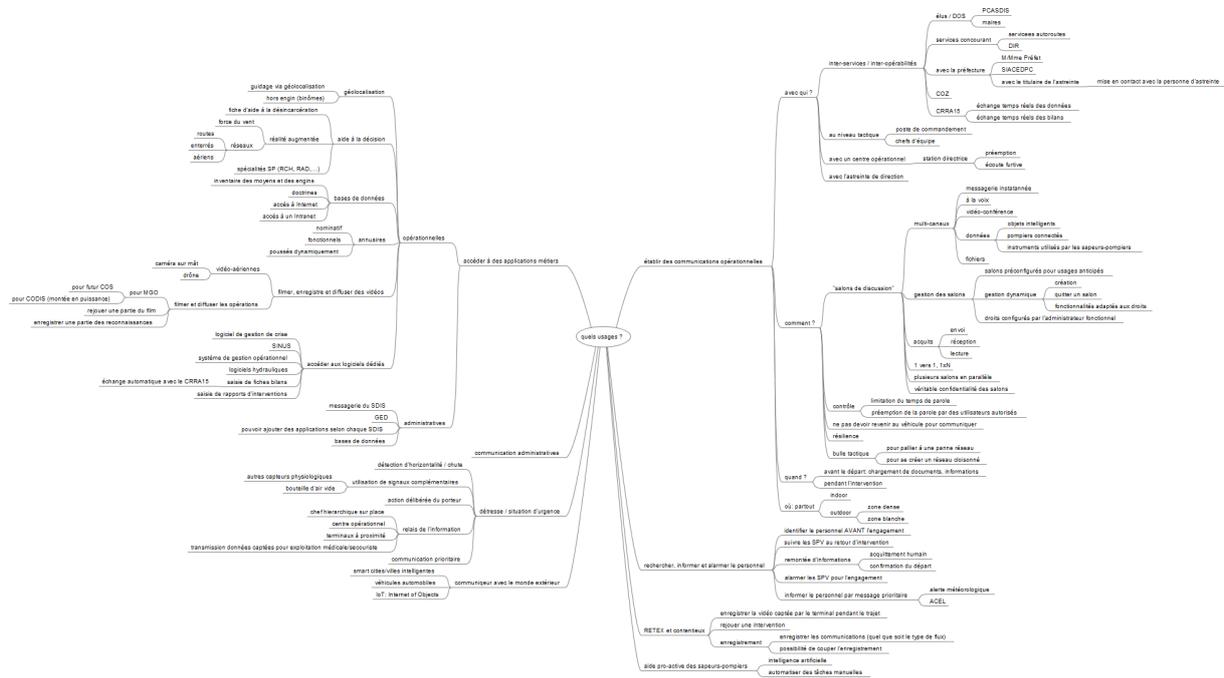


Figure 19 : carte mentale des besoins exprimés par les personnes interrogées. Les points mentionnés sur cette carte mentale sont développés ci-dessous. La carte mentale est mise en annexe pour plus de lisibilité.

57_FON_01	Établir des communications opérationnelles	1
<p>Remarques</p>	<p>Les communications opérationnelles devront pouvoir être établies facilement entre les sapeurs-pompiers et les différents intervenants concourant aux missions de sécurité civile :</p> <ul style="list-style-type: none"> • les directeurs des opérations de secours (maires et préfets) ; • les services tels que la DIR et les concessionnaires des autoroutes ; • les services des préfectures (SIACEDPC) ; • l'État-Major de Zone ; • le CRRA15. 	
	<p>En outre, les communications opérationnelles suivantes et internes aux services d'incendies doivent pouvoir être établies :</p> <ul style="list-style-type: none"> • au niveau tactique avec un poste de commandement et l'ensemble des moyens et des personnels engagés (chef de site, chef de colonne, chef de groupe, chef d'agrès, chefs d'équipe, équipiers) ; • avec le centre opérationnel (CODIS) ; • avec la chaîne de commandement d'astreinte. 	

Les communications opérationnelles devront pouvoir être établies sous forme de « salons de discussions » multi-canaux :

- échange d'information à la voix (en temps réel et en lecture différée) ;
- en vidéo-conférence ;
- sous forme de messagerie instantanée ;
- échange de fichiers ;
- échange de données issues d'objets connectés, d'instruments/outils utilisés par les sapeurs-pompiers, etc.

Les différents « salons de discussion » doivent pouvoir travailler en parallèle quelle que soit la forme de l'échange (donnée, voix, etc.). Ainsi, il paraît intéressant de pouvoir établir en parallèle des salons avec « l'avant » et « l'arrière » depuis le niveau chef d'équipe jusqu'au niveau chef de site.

À chaque échange le nécessitant, des acquits doivent être disponibles. Ces acquits indiqueront :

- l'envoi de l'information ;
- la bonne réception par les différents destinataires ;
- l'accusé de lecture (manuel ou automatique).

La gestion des « salons de discussion » devra être souple et dynamique :

- des salons dynamiques pré configurés par l'administrateur fonctionnel ;
- des salons inter-services ou non pouvant être créés, modifiés ou supprimer en temps réel suivant les droits des utilisateurs.

Les utilisateurs qui pourraient être rajoutés à un « salon » devraient être identifiés par le nom mais également par leur fonction à l'instant t (exemple : il est souhaité qu'on puisse rajouter le/la sous-préfet(e) d'astreinte en choisissant cette fonction et non pas en le choisissant dans une liste nominative qui présuppose la connaissance du nom du titulaire à l'instant t).

Ces salons seront soit de type :

- 1 vers 1 : un interlocuteur échange de l'information avec un autre interlocuteur ;
- N vers N : plusieurs interlocuteurs échangent dans le cadre d'un groupe où toutes les informations échangées sont vues par l'ensemble des membres participant au salon.

Un utilisateur doit pouvoir faire partie de plusieurs « salons de discussion » (ex : un COS fait partie d'un salon de niveau tactique et d'un salon d'information avec le CODIS).

L'envoi de messages courts, modifiables par l'utilisateur, doit pouvoir être réalisé (ex : transmission d'un bilan simplifié au CODIS).

La confidentialité des échanges devra être totale entre chaque « salon ». Actuellement, la solution n'est pas totalement confidentielle car il est possible d'écouter des messages s'ils sont émis sur un talkgroup de portée départemental.

Des utilisateurs (tels que le CODIS) devront disposer de fonctionnalités spéciales telles que la préemption des échanges afin de jouer un rôle de station directrice ainsi que l'écoute *furtive* pour assurer la sécurité des personnels dans le cas où la sécurité de celui-ci serait compromise.

Des limites devront pouvoir être fixées afin de limiter les temps de parole.

D'autre part, ces salons de communications devront être faciles d'utilisation et accessibles sans devoir retourner à l'engin afin que le COS ne doive pas s'éloigner du théâtre d'intervention.

Ces communications opérationnelles devront être accessibles tant à l'extérieur (y compris dans une zone blanche non couverte par un opérateur de télécommunications) qu'à l'intérieur de bâtiments (immeubles d'habitations et bâtiments industriels).

Des bulles tactiques devront pouvoir être mises en place soit pour pallier à une défaillance de couverture ou panne mais également pour créer un espace totalement cloisonné du monde extérieur.

D'autre part, des échanges d'informations entre le personnel engagé et le service incendie devront avoir lieu non seulement pendant l'intervention mais également en transit et au moment du départ (envoi d'informations et documents pouvant faciliter la conduite de l'opération).

L'identification du personnel et/ou de l'engin doit être souple afin de pouvoir gérer des engins polyvalents (et ne pas être limitée par des groupes statiques prédéfinis).

57_FON_02	Rechercher, informer, sonder et alarmer le personnel	2
Remarques	Le Réseau Radio du Futur peut ainsi se substituer à un système de déclenchement (type réseau départemental d'alerte) pour : <ul style="list-style-type: none">• alarmer les sapeurs-pompiers et les engager sur une opération ;• se faire confirmer la disponibilité du personnel pour partir en intervention (remontée d'acquit manuel) ;	

	<ul style="list-style-type: none"> • suivre le personnel (l'ayant accepté) depuis le moment de l'alarme jusqu'au retour à domicile. Le service incendie est ainsi en capacité de secourir un sapeur-pompier ayant un accident de circulation ; • géolocaliser (sous réserve d'acceptation par le personnel) dans le cadre d'une recherche de personnel (exemple : demande d'activation du partage de la position demandée par le CODIS, acceptation par le sapeur-pompier et identification du personnel disponible par le CODIS) ; • informer le personnel par message opérationnel (ex : alerte météorologique, recherche de personnel dans le cadre d'une catastrophe,...) ; • sonder le personnel (ex : « Êtes-vous disponible pour un départ en colonne de renforts sous 24 heures ? »). <p><u>NB</u> : la mutualisation avec la fonction de l'alarme du personnel permettrait de réaliser des économies.</p>
--	--

57_FON_03	Pratiquer des RETEX	2
Remarques	<p>Pouvoir enregistrer et « rejouer » toute une intervention en reprenant l'ensemble des informations échangées et captées par les sapeurs-pompier (images, vidéos, flux issus de capteurs, etc.).</p> <p>L'enregistrement doit couvrir tous les flux.</p>	

57_FON_04	Justifier en cas de contentieux	2
Remarques	<p>En plus des fonctionnalités entrant dans le cadre des pratiques du « RETEX », il est demandé de pouvoir embarquer une caméra enregistrant et transmettant les flux vidéo en cas d'accident (caméra appelée <i>dashcam</i>).</p> <p>L'enregistrement doit couvrir tous les flux quel que soit le format.</p>	

57_FON_05	Renforcer la sécurité du personnel	1
Remarques	<p>Une application dédiée à la gestion des détresses doit être disponible. Cette communication opérationnelle particulière doit être prioritaire vis-à-vis des autres communications.</p> <p>Elle doit pouvoir être déclenchée :</p> <ul style="list-style-type: none"> • par une action délibérée du porteur du terminal ; 	

	<ul style="list-style-type: none"> • par détection d'horizontalité et d'absence de mouvements du porteur ; • par suite d'informations provenant de capteurs (ex : capteurs physiologiques). <p>L'information d'un personnel en détresse doit être relayée vers :</p> <ul style="list-style-type: none"> • le chef hiérarchique sur place ; • le centre opérationnel ; • les terminaux à proximité. <p>L'ensemble des données physiologiques et de géolocalisation captées par le terminal de la personne en détresse devront être communiquées aux logiciels métiers concernés et partagées avec le personnel et services <i>ad hoc</i> afin d'assurer la meilleure prise en charge médicale possible.</p>
--	---

57_FON_06	Supporter les communications administratives	2
	<p>Dans l'optique de mutualiser les flottes opérationnelles et administratives, idéalement, le Réseau Radio du Futur transporte à la fois les communications opérationnelles et administratives afin d'éviter le doublement de la flotte et éviter que l'utilisateur ait besoin de deux terminaux. Ce dernier point est l'une des raisons pour lesquelles certains utilisateurs n'utilisent plus le terminal ANTARES et passent, sauf problème, leurs communications via le réseau téléphonique grand public.</p>	

57_FON_07	Accéder à des applications métiers « opérationnelles »	1
	<p>Le Réseau Radio du Futur doit offrir les capacités permettant d'accéder à diverses applications opérationnelles :</p> <ul style="list-style-type: none"> • des logiciels d'aide à la décision : <ul style="list-style-type: none"> ○ aide à la désincarcération ; ○ aide à la décision dans le cadre du secours d'urgence à la personne ; ○ aide dans l'identification de matières dangereuses (risque chimique et radiologique) ; ○ applications météorologiques ; ○ utilisation de la réalité augmentée (ex : affichage de l'ensemble des réseaux aériens et enterrés) ; • des bases de données : <ul style="list-style-type: none"> ○ moteur de gestion documentaire ; ○ documents <i>pdf</i> (inventaires des moyens, doctrines, etc.) • accès à Internet ; 	

	<ul style="list-style-type: none"> • accès à l'intranet du service d'incendie et de secours ; • accès à un annuaire nominatif et fonctionnel (les fonctions sont mises à jour notamment pour les personnels d'astreinte). Ils doivent pouvoir être mis à jour à distance sur l'ensemble de la flotte de terminaux. • visualisation de l'ensemble des engins et des personnels (même en dehors de l'engin) ; • système de gestion opérationnelle ; • SINUS ; • logiciel de gestion de crises ; • logiciel de calculs hydrauliques ; • logiciel de saisie de bilan secouriste ; • logiciel de saisie des comptes rendus de sortie ; • logiciel « caméra embarquée » permettant à un personnel de voir au travers d'un terminal embarqué par un autre personnel (ex : chef d'équipe CMIC visualisant la vidéo captée par une équipe de reconnaissance). Ce logiciel doit permettre d'enregistrer les vidéos et de diffuser les flux. L'enregistrement local doit permettre de rejouer ce qui a été vu pour faciliter la conduite des opérations (ex : un premier COS montre les reconnaissances réalisées afin que l'échelon supérieur puisse prendre en compte des informations jugées importantes par le premier COS) ou pour permettre au CODIS de bénéficier d'une vue d'ambiance afin de préparer une montée en puissance (si nécessaire). Il peut être envisagé de positionner cette caméra sur un drone de reconnaissance ainsi que sur un mât d'un poste de commandement.
--	--

57_FON_08	Accéder à des applications métiers « administratives »	2
	<p>Dans l'optique de mutualiser les flottes opérationnelles et administratives, idéalement, le Réseau Radio du Futur permet d'accéder aux applications métiers de type « administratives » telles que, par exemple:</p> <ul style="list-style-type: none"> • base de données ; • intranet. 	

57_FON_09	Accéder à un outil de gestion électronique des documents (GED)	2
	<p><u>Définition d'une GED :</u></p> <p>La GED est un procédé faisant intervenir des moyens électroniques pour prendre en charge la gestion des documents, à savoir les opérations et actions destinées à traiter et à exploiter les documents, par exemple la capture, l'acquisition, la numérisation, la validation, la diffusion, le</p>	

classement, l'indexation, l'archivage, etc.

Le déploiement d'une GED permet donc de consulter et de gérer à distance une base de données compilant tous les plans de secours, les textes réglementaires, de faire remonter au CO les différents comptes rendus écrits avec ou sans pièces jointes. Ces dernières peuvent être de toutes natures (photos, vidéos, textes ...).

Chaque COS dispose ainsi d'un « fond de sac » documentaire lui permettant d'accomplir sa mission avec toutes les informations nécessaires. L'usage de GED est généralisé dans le monde de l'entreprise ainsi que chez la plupart des acteurs institutionnels. Cependant, l'usage de ce service dans un contexte opérationnel dépend en grande partie de la qualité du réseau de transport.

Exigences :

Les informations à durée de validité ponctuelle (relative à un sinistre particulier) ou permanente (doctrine d'emploi) doivent être consultables par le COS en charge du sinistre et sur son terminal.

De plus, et afin de parer une éventuelle perte de réseau, l'accès à la GED devra être associée à un client lourd permettant l'exploitation des données en mode non connecté ou permettre le téléchargement des documents. La possibilité de travailler en mode non connecté pour l'accès à la GED répond à un double impératif :

- compenser une perte ponctuelle du réseau ou une mauvaise qualité de ce dernier tout en permettant au COS de continuer à exploiter en local les documents stockés sur son périphérique.
- en période de congestion du réseau, l'exploitation en mode non-connecté de texte, photos, vidéos, etc., permet de délester ce dernier et de conserver une bonne qualité de service pour les communications opérationnelles en phonie qui sont entièrement dépendantes du mode connecté (connecté à une bulle tactique ou directement au réseau opéré).

Le mode non connecté doit rester pour l'accès à la GED un mode dégradé et temporaire lors d'une intervention.

57_FON_10	Main courante	2
	La main courante est un outil de renseignement indispensable pour tout échelon de commandement.	

Elle permet une plus grande coordination et un suivi des actions en cours plus efficace. Via le RRF, la main courante peut être « extraite » par des formulaires automatiques et ainsi implémenter les différents tableaux de bord du centre opérationnel (cas d'opérations majeures et multi-sites par exemple).

L'intérêt de disposer d'un réseau de transport permettant la transmission de donnée est de limiter les communications phonie entre les postes de commandement et de faire circuler une information au format souhaité impactant le moins possible les personnels alimentant la main courante.

Localement, chaque COS doit disposer des logiciels et matériels permettant l'échange d'information numérique.

Ce type d'organisation permet de collaborer et de partager des informations avec d'autres services qu'ils se trouvent sur place ou à distance via le RRF. De plus, ces outils permettent de mener des recherches efficaces portant sur des personnes, des documents et des données, (= recherche d'information à base de formulaires) et y participer et pour accéder à de grandes quantités de données et les analyser.

Ce service pourrait être particulièrement utile dans la mise ne forme des informations présentées à l'échelon politique. À ce jour, cette tâche essentiellement faite manuellement est consommatrice de personnel. La remontée systématique des informations par l'utilisation de formulaires automatiques permet de présenter la « bonne information » en temps réel et selon un format défini à l'avance.

57_FON_11	Aide pro-active des sapeurs-pompiers	2
Remarques	La solution proposée doit permettre la mise en place de fonctionnalités intelligentes (ex : intelligence artificielle). L'envoi automatique de statuts pourrait ainsi, à titre d'exemple, être automatisé sans que le chef d'agrès doive réaliser d'actions manuelles (ex : arrivée sur les lieux, départ en intervention, etc.).	

57_FON_12	Communiquer avec le monde extérieur	2
Remarques	Le développement de l'Internet des objets (<i>IoT : Internet of Objects</i>) ainsi que le développement des outils communicants (<i>smart cities</i> , véhicule intelligent) nécessite que les terminaux puissent exploiter pleinement ses besoins à l'avenir. A titre d'exemple :	

- les fonctionnalités de ville intelligentes permettraient :
 - d'adapter le chemin parcouru et de faciliter le trajet (contrôle des feux de circulation lors du passage d'un engin de secours) ;
 - d'adapter la conduite des opérations en fonction d'informations en temps réel provenant des réseaux (hydrauliques, électriques, etc.)
- l'interconnexion à un ordinateur de bord du véhicule permettrait de connaître les circonstances d'un accident et d'adapter la conduite des opérations de secours ;
- faciliter l'accès à l'intérieur des domiciles dans le cas d'une personne ne répondant pas aux appels.

3.5 Description du terminal idéal

La carte mentale représentée ci-dessous (voir Figure 20) synthétise les réponses à la question suivante : « Si vous aviez une baguette magique, quel serait, selon vous, le terminal idéal ? ». Les notions de « facilement réparable » et « facilement échangeable » sont développées à la section 3.5.

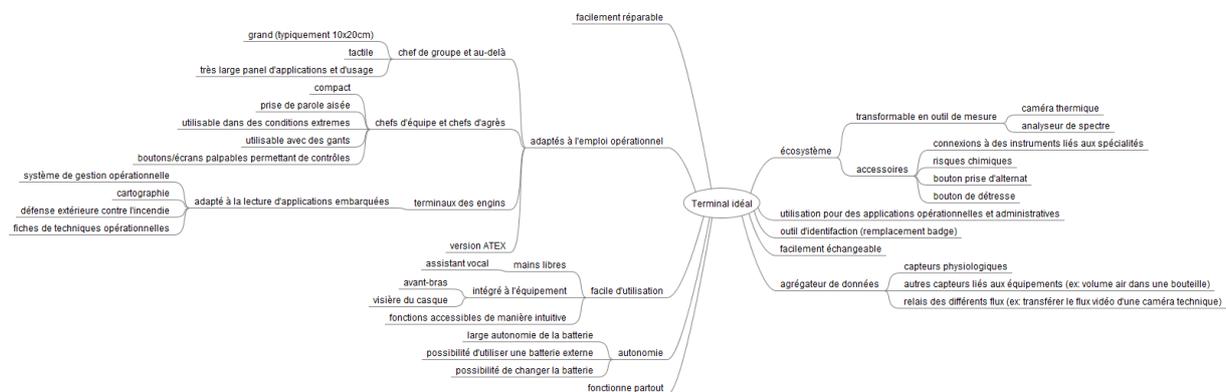


Figure 20 : carte mentale décrivant le terminal idéal

57_TER_01	Terminal adapté à l'emploi opérationnel	1
Remarques	<p>Après prise en compte des besoins émanant de différentes catégories d'utilisateurs, il ressort que trois grandes catégories de terminaux se dégagent :</p> <ul style="list-style-type: none"> • un terminal relativement compact, solide, intégré à l'équipement de base du sapeur-pompier (casque, col, veste, etc.) utilisable avec des gants et robuste pour les sapeurs-pompier susceptibles d'être engagés à l'avant (incendie, équipe de reconnaissance, etc.). Ces terminaux seraient utilisés 	

	<p>pour communiquer à la voix et comme « caméra » afin d'être les yeux de personnels plus éloignés,</p> <ul style="list-style-type: none"> • un terminal plus grand à destination des chefs de groupe, de colonne et de site optimisés pour des applications de type « commandement / S.G.O.». • un terminal plus grand destiné à être mis dans des engins (ex : FPT et VSAV) afin d'y consulter en transit des données relatives à l'opération et/ou remplir des comptes rendus d'intervention lors du retour. <p>En outre, une version « ATEX » doit être disponible afin de pouvoir être utilisé en milieu explosif.</p>
--	---

57_TER_02	Facile d'utilisation	1
Remarques	<p>Le terminal doit être simple d'utilisation :</p> <ul style="list-style-type: none"> - il doit pouvoir être utilisé en mains libres de manière conviviale. Les « assistants vocaux » et « logiciels de reconnaissance de parole et de dictée » semblent particulièrement intéressants dans cette perspective ; - il doit être intégré à l'équipement pour qu'il soit presque « transparent » pour l'utilisateur ; - il doit être intuitif et disposer de menus adaptés. Par conséquent, les applications développées devront être particulièrement soignées. En outre, le choix d'un système d'exploitation ressemblant le plus possible à celui d'un terminal grand public faciliterait l'appropriation par les utilisateurs. 	

57_TER_03	Fonctionne longtemps	1
Remarques	<p>Les terminaux devront avoir une large autonomie (plus de 24 heures en fonctionnement). Parmi les propositions envisagées figurent :</p> <ul style="list-style-type: none"> - la possibilité d'alimenter par l'extérieur (batterie de secours, par l'engin, etc.) ; - la possibilité de remplacer aisément la batterie ; - utiliser une batterie à forte capacité. 	

57_TER_04	Fonctionne « partout »	1
Remarques	Le terminal devra fonctionner « partout » sans zone blanche et sans	

	<p>devoir passer par l'engin.</p> <p>La solution actuelle dans laquelle un portatif est hors couverture et nécessite l'utilisation d'un terminal mobile d'un engin est vécue comme pénalisante dans la conduite des opérations.</p> <p>D'autre part, <u>l'ensemble des services</u> devra être disponible sur une couverture géographique plus élevée que dans la solution actuelle.</p>
--	--

57_TER_05	Dispose d'un écosystème varié et ouvert	1 et 2
Remarques	<p>Le terminal doit pouvoir être associé à un grand nombre d'accessoires tels que :</p> <ul style="list-style-type: none"> • des accessoires transformant le terminal en instrument de mesure (priorité 2) : <ul style="list-style-type: none"> ○ caméra thermique ; ○ analyseur de spectre ; ○ etc. • visualiser le contenu d'instruments situés à distance. Ex : <ul style="list-style-type: none"> ○ permettre à un chef d'agrès de voir les images de la caméra thermique emmenée par un chef d'équipe ; ○ permettre à un chef de cellule « CMIC » de voir les images d'une caméra embarquée sur l'équipe de reconnaissance ; ○ etc. • des outils simplifiant la prise de parole : <ul style="list-style-type: none"> ○ bouton de prise d'alternat ; ○ bouton de détresse ; ○ etc. 	

57_TER_06	Utilisable tant pour des applications administratives qu'opérationnelles	2
Remarques	<p>Le terminal idéal doit pouvoir être utilisé à la fois pour des applications opérationnelles qu'administratives afin que les agents utilisent et améliorent la maîtrise de l'outil. En outre, l'unification de la flotte permettra de réduire les coûts d'acquisition et de maintenance.</p>	

57_TER_07	Un outil d'identification	2

Remarques	Le terminal idéal permet de s'identifier et d'accéder aux bâtiments des services d'incendie et de secours. L'attention devra être portée sur la résilience et la continuité d'activités (notamment dans le cas où le terminal centralise toutes les fonctions).
------------------	---

57_TER_08	Un agrégateur de données relayant les informations captées	1
Remarques	<p>Le terminal idéal est, en quelque sorte, une multiprise sur lequel viennent se connecter l'ensemble de l'écosystème (que ce soit des informations liées aux capteurs du <i>sapeur-pompier connecté</i> que d'instruments externes). Ce multiprise relaie ensuite les informations vers d'autres terminaux soit de manière directe, soit en passant par des serveurs intermédiaires afin que les parties prenantes puissent avoir accès aux informations en temps réel.</p> <p>Le mécanisme d'appairage entre le terminal et un capteur/instrument doit être robuste, rapide et stable. En particulier, il doit pouvoir fonctionner même en présence de plusieurs intervenants situés dans une zone peu étendue.</p>	

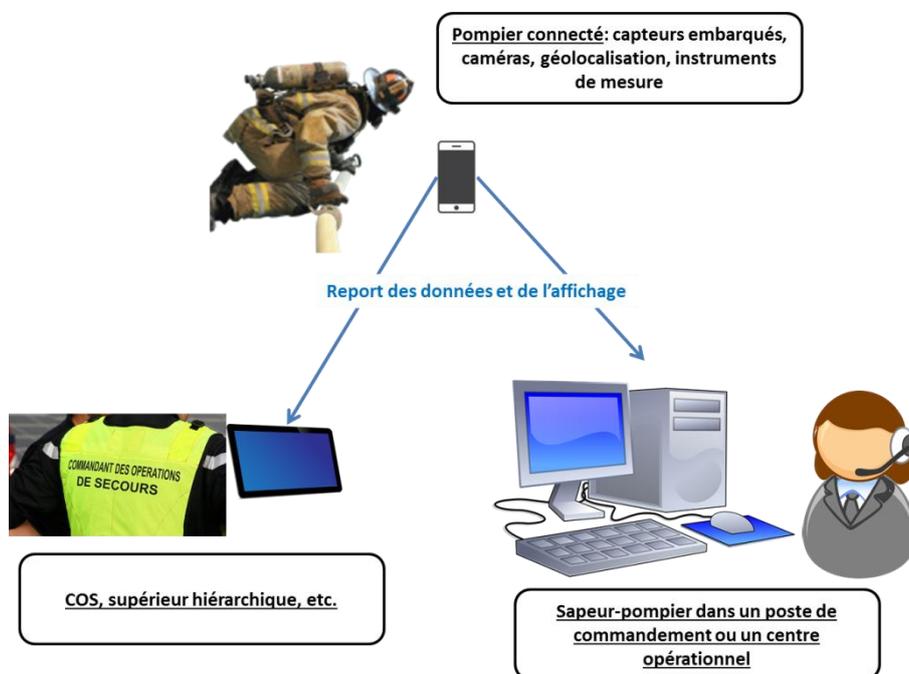


Figure 21 : illustration du rôle du terminal en tant qu'agrégateur de données et de relais d'informations captées

4 Besoins des administrateurs fonctionnels

Les besoins sont décrits à partir d'une carte mentale (voir Figure 22). Chacun de ces besoins est décrit par la suite. Bien que certains besoins ne concernent pas strictement le RRF, il a été jugé utile de les inclure car ils impactent l'organisation et les missions des services d'incendie et de secours. La prise en compte de ces éléments en amont du basculement vers le nouveau réseau permettrait d'adapter la stratégie notamment en termes de mutualisation tant dans les acquisitions que la maintenance.

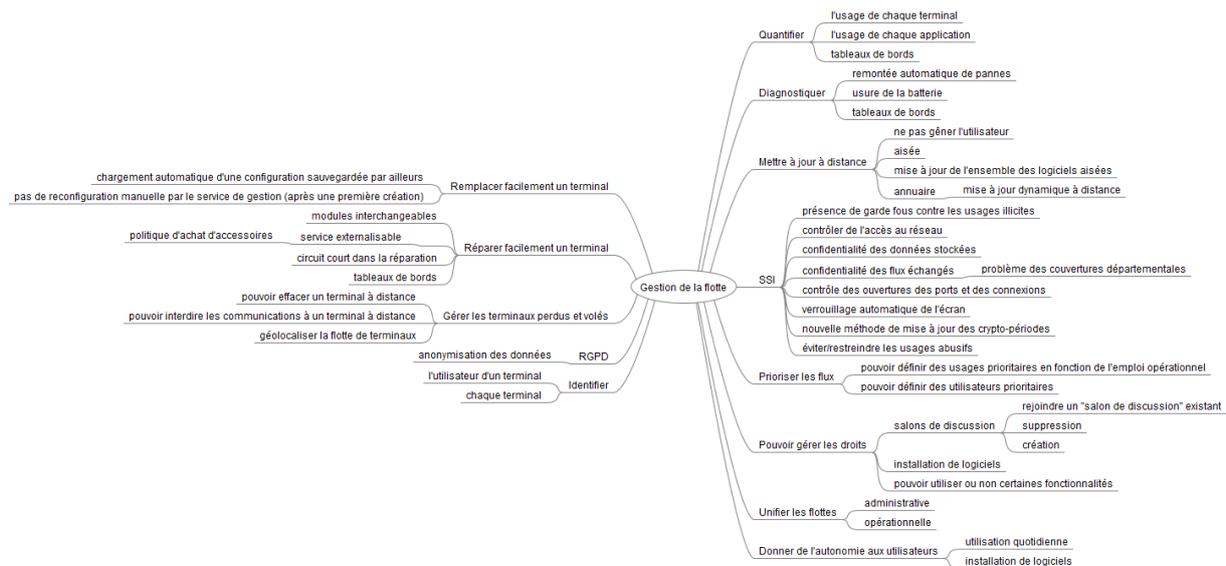


Figure 22 : carte mentale des besoins fonctionnels des administrateurs fonctionnels

57_BAF_01		
	Remplacer facilement un terminal	2
	Il est proposé de stocker une copie de l'ensemble de la configuration, des messages, des fichiers, etc. de l'utilisateur dans le <i>cloud</i> . En cas de nouveau terminal, l'ancienne configuration est <i>poussée</i> vers le nouveau terminal. Il en résulte un gain de temps pour l'administrateur et l'utilisateur.	

Id	Intitulé	Priorité
57_BAF_02	Réparer facilement un terminal	2
Remarques	Il est proposé d'acquérir des terminaux évolutifs et réparables facilement en interne au sein du SDIS. Ainsi, idéalement, les terminaux seraient composés de modules interchangeables et évolutifs. Ainsi, les terminaux dont les batteries sont collées/soudées seraient exclus.	

	D'autre part, un circuit court de réparation devrait pouvoir être mis en œuvre pour réparation de deuxième niveau.
--	--

Id	Intitulé	Priorité
57_BAF_03	Gérer les terminaux perdus ou volés	1
Remarques	Il doit être possible de géolocaliser un terminal perdu ou volé. En outre, les dernières positions connues doivent être accessibles par les administrateurs fonctionnels.	

Id	Intitulé	Priorité
57_BAF_04	Identifier les terminaux	1
Remarques	Chaque terminal doit être doté d'un identifiant unique. Dans le cas d'une dotation collective, il doit être possible d'identifier la personne utilisant/ayant utilisé le terminal (historisation de l'usage).	

Id	Intitulé	Priorité
57_BAF_05	RGPD	1
Remarques	Les outils mis à dispositions des personnels devront respecter le RGPD. À ce titre, et afin de pouvoir exploiter l'ensemble des données, il semble important de pouvoir conserver des données importantes (utilisation d'application, utilisation des terminaux, etc.) après les avoir rendues anonymes afin, par exemple, d'améliorer le service et de réaliser des statistiques.	

Id	Intitulé	Priorité
57_BAF_06	Quantifier	1
Remarques	<p>L'administrateur fonctionnel a besoin de connaître l'usage qui est fait de chaque terminal et de chaque application :</p> <ul style="list-style-type: none"> • nombre d'heures d'utilisation ; • volume de données échangées par chaque application ; • consommation de la batterie par chaque application ; • etc. <p>Sachant que les terminaux peuvent être en dotation collective, ces informations doivent être reliées à l'utilisateur.</p> <p>Ces informations doivent être disponibles à travers des tableaux de</p>	

	bord permettant de naviguer au travers des données globales tout en permettant l'analyse détaillée.
--	---

Id	Intitulé	Priorité
57_BAF_07	Diagnostiquer	2
Remarques	<p>Chaque terminal doit être doté d'un outil interne de diagnostic s'exécutant périodiquement afin que les pannes et dégradation des performances soient signalées avant de constater un problème en intervention.</p> <p>Les performances (ex : capacité de la batterie) sont historisées afin de pouvoir mesurer l'évolution temporelle.</p> <p>Ces informations doivent être accessibles depuis des tableaux de bord.</p>	

Id	Intitulé	Priorité
57_BAF_08	Mise à jour à distance	2
Remarques	<p>Il doit être possible de <i>pousser</i> à distance une mise à jour de tout ou partie de la flotte afin d'avoir des montées de version et de configuration homogènes sur toute la flotte sans que l'utilisateur ait besoin de procéder à des réglages par lui-même (si ce n'est la validation de l'installation des modifications).</p> <p>Parmi les points particuliers, figure l'annuaire nominatif et fonctionnel.</p>	

Id	Intitulé	Priorité
57_BAF_09	Prioriser les flux	1
Remarques	<p>Dans l'hypothèse où les capacités de transmission du réseau sont finies, il doit être possible de prioriser certains flux (ex : flux applicatifs du système de gestion opérationnels en priorité absolue, communications avec les binômes à l'attaque,...) au dépend de certains autres.</p> <p>D'autre part, il doit être possible d'arbitrer la priorité de certains flux en fonction de l'emploi opérationnel de l'utilisateur.</p>	

Id	Intitulé	Priorité
57_BAF_10	Pouvoir gérer les droits des utilisateurs	1

Remarques	<p>Chaque application et le système d'exploitation doivent disposer de paramètres « utilisateurs » :</p> <ul style="list-style-type: none"> • spécifier les droits relatifs aux « salons de discussions » : <ul style="list-style-type: none"> ○ droit ou non de créer dynamiquement un salon ; ○ droit ou non de supprimer un salon ; ○ droit ou non de rejoindre un salon pré-défini. • droit d'installer ou non des applications ; • droit ou de pouvoir utiliser certaines fonctionnalités du terminal ; • etc.
------------------	---

Id	Intitulé	Priorité
57_BAF_11	Unifier les flottes à usage administratif et opérationnel	1
Remarques	Utiliser les mêmes terminaux et tablettes à des fins d'usages administratifs et opérationnels permettraient des économies importantes.	

Id	Intitulé	Priorité
57_BAF_12	Donner de l'autonomie aux utilisateurs	2
Remarques	L'utilisateur doit jouir d'une autonomie afin d'éviter de solliciter les services supports. Cette autonomie est possible si le terminal se rapproche des terminaux « grands publics » (maîtrise de l'outil) et par une liberté encadrée dans la configuration et l'installation d'outils.	

Id	Intitulé	Priorité
57_BAF_13	Sécurité du système d'information	1
Remarques	<p>Le terminal et son utilisation doivent être sécurisés :</p> <ul style="list-style-type: none"> • présence d'un garde-fou embarqué dans le téléphone pour interdire/restreindre les usages illicites ; • assurer la confidentialité des données stockées sur le terminal ; • possibilité d'effacer à distance (ou non) le contenu d'un terminal ; • assurer la confidentialité des flux échangés ; • possibilité de verrouiller automatiquement le terminal. Si un terminal venait à être verrouillé alors qu'il est utilisé en intervention, ce terminal pouvoir être débloqué aisément ; • accès au terminal par l'intermédiaire d'un contrôle d'identité de l'utilisateur (mot de passe, biométrie, etc.) ; • contrôle des connexions et des ports ouverts vers le monde extérieur ; 	

	<ul style="list-style-type: none"> • sécuriser les terminaux connectés avec le monde extérieur (notamment contre les attaques provenant d'une connexion par câble à un ordinateur) ; • mise à jour d'éventuelles clefs de cryptage aisée nécessitant moins de main d'œuvre que dans l'INPT,
--	---

Id	Intitulé	Priorité
57_BAF_14	Adapter l'interface aux missions	1
Remarques	L'administrateur fonctionnel doit pouvoir adapter l'interface d'accueil en fonction des fonctions et des missions afin de proposer un outil simple d'utilisation.	

Id	Intitulé	Priorité
57_BAF_15	Évolutif	1
	Le système proposé doit être évolutif avec le temps afin d'évoluer en phase avec les systèmes grands publics.	

5 Contraintes d'implémentations

Bien que ne portant pas sur les besoins fonctionnels, il est apparu important de présenter des contraintes fortes d'implantations que le groupe a identifié durant la rédaction de ce mémoire.

Le RRF doit respecter le principe de non régression du service de communication qui est proposé par ANTARES. Nous verrons dans ce chapitre que la plaque parisienne, la Guyane et les régions frontalières présentent des problématiques de communication différentes.

5.1 Zones fortement urbanisées : exemple à Paris

Pour les communications « *outdoor* » (à l'extérieur), les zones très denses telle que la plaque parisienne présentent l'avantage de disposer d'un réseau 4G moderne et fiable. Il est raisonnable de penser que les évolutions techniques futures seront déployées à Paris avant les autres zones de défense. La zone « Île de France » reste donc une zone privilégiée puisque les opérateurs ont et auront toujours un intérêt économique fort à moderniser la plaque parisienne. De plus, des événements internationaux tels que la prochaine coupe du monde de rugby en 2023 ou les JO 2024 sont des « accélérateurs » dans ce domaine.

Cependant, l'utilisation des services basés sur le RRF en milieu confiné que nous appellerons « *indoor* » est aussi problématique que les précédents systèmes de communications. Dans ce domaine, le RRF devra répondre aux mêmes défis que ces prédécesseurs à savoir les difficultés de propagation en sous-sol, les tunnels ferroviaires ou les ERP.

Le RRF doit, de par son mode de fonctionnement exclusivement en mode connecté, répondre à une exigence supplémentaire : comment assurer les communications de base (la voix) en mode non connecté ?

Le service « voix », à savoir la transmission d'une conversation appelée service critique (MCPTT) dans le programme RRF est le premier besoin de tout sapeur-pompier sur le terrain. En dernier ressort, il est indispensable que le chef sur le terrain puisse communiquer à la voix avec ses subordonnés et que le COS (commandant des opérations de secours) puisse être contacté par ses propres chefs.

Ce service doit être le successeur du mode relayé et du mode direct que l'on peut retrouver sur l'INPT. Ce service doit présenter une grande souplesse d'emploi car les opérations de secours se caractérisent par une évolution rapide des effectifs sur le terrain, un niveau de coopération inter-service pouvant évoluer rapidement dans le temps et un grand besoin d'adaptabilité dans ces structures de commandement.

Ceci est particulièrement important à Paris où les opérations inter-services sont plus fréquentes et se déroulent aux plus petits niveaux hiérarchiques. Les exemples sont nombreux :

- feux de voitures dans une zone sensible ;
- émeutes urbaines ;
- tuerie de masse.

Même si la création d'un Ordre Particulier des Transmissions (OPT) reste un préalable à toutes opérations, le service voix du RRF devra permettre, sans préavis et, avec la plus grande facilité d'emploi des échanges vocaux inter-services.

D'autre part, ce service devra permettre de communiquer à un grand nombre d'utilisateurs de façon structurée et organisée. Les ressources actuelles d'ANTARES ne permettent pas de disposer du nombre désiré de canaux et leur gestion se révèle très rigide.

En outre, le système de communication devra s'affranchir de la notion de *talkgroup* ou de conférence afin de répondre aux spécificités des missions inter-services telles que l'on peut les rencontrer sur la plaque parisienne.

La possibilité de transmettre via la messagerie vocale des fichiers, photos ou vidéos qui seront nécessaires à renseigner les états-majors et la chaîne politique.

À partir de ce constat, le service voix idéal serait :

- un logiciel client léger permettant de diffuser de la voix en VOIP (*voice over IP*) et des données ;
- un serveur hébergeant un service de messagerie et un service de stockage des données (fichiers, photos et vidéos).

La figure ci-dessous illustre ce propos.

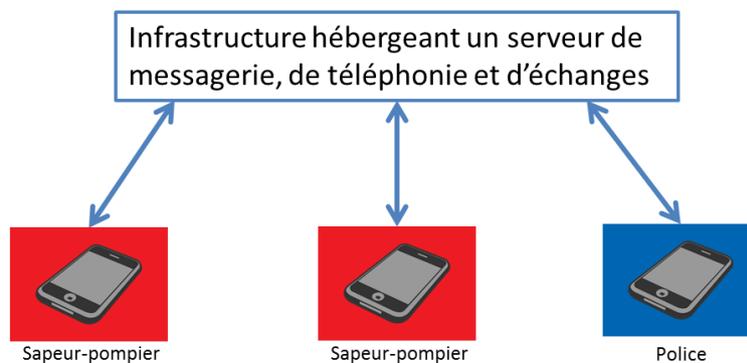


Figure 23 : exemple d'interopérabilité. Dans cet exemple, deux périphériques sapeurs-pompiers (en rouge) communiquent. Un périphérique de la police (en bleu) doit se joindre à l'opération. Pour cela, il doit être en mesure de se connecter au même serveur de messagerie vocale. Afin de permettre une conversation entre ces trois intervenants, il est donc nécessaire que l'infrastructure de communication soit ouverte à tous les intervenants potentiels à une mission de service publique.

L'interopérabilité inter-service s'en trouve grandement facilitée. L'infrastructure permet d'échanger des documents entre les intervenants connectés à un même serveur.

Le COS peut ainsi faire remonter au centre opérationnel une vidéo capturée avec son smartphone si besoin.

Dans ce type de messagerie, la possibilité d'administrer doit répondre aux besoins de souplesse nécessaire à une opération de grande ampleur. La Brigade des Sapeurs-Pompiers de Paris a ainsi imaginé ce que pourrait être le fonctionnement de la messagerie :

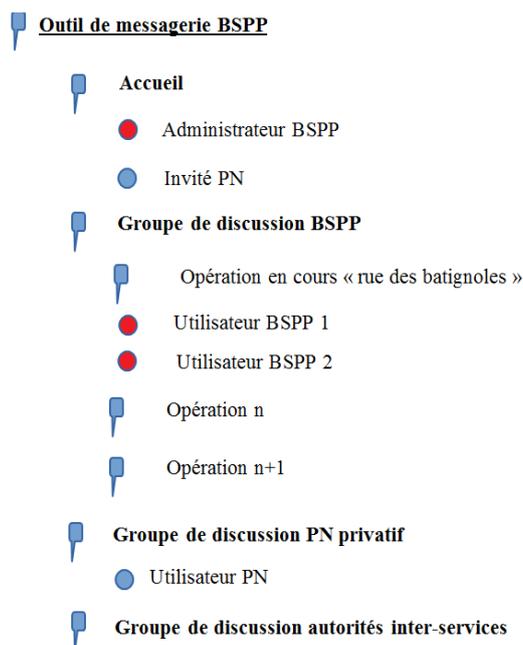


Figure 24 : exemple de messagerie (inter-service, multi-opérations) imaginé par la BSPP

Chaque utilisateur de la messagerie doit pouvoir accéder à des groupes de discussion en fonction de ses prérogatives et de sa fonction opérationnelles. À la connexion, chaque intervenant doit, seul ou avec l'aide de l'administrateur de la messagerie si besoin, pouvoir accéder au groupe de discussion relatif à l'intervention en cours qui motive sa connexion.

Le nombre de groupe de discussion doit être virtuellement illimité afin de pouvoir organiser un grand nombre de salons de conversation.

Chaque groupe de discussion doit donc pouvoir être créé, renommé ou supprimé en temps réel et sans délai.

Chaque intervenant doit pouvoir basculer de groupe en groupe en fonction de la mission. Si, par exemple, les policiers doivent communiquer de façon plus confidentielle, ils doivent pouvoir basculer dans un groupe de discussion privé permettant d'échanger entre eux.

Chaque intervenant doit pouvoir être à l'écoute de deux groupes de discussion au moins. Cela permet au COS de converser avec son détachement dans un groupe dédié mais aussi d'être rappelé par le centre opérationnel pour un point de situation dans le canal « autorités » par exemple.

La transmission de fichier doit suivre la même logique. Chaque intervenant doit pouvoir publier dans un canal donné un document qui ne sera accessible qu'aux autres intervenants ayant accès à ce canal.

Dans cette démarche, la gestion des droits d'accès permet d'assurer l'équilibre entre souplesse d'emploi de la messagerie et sécurité de l'information.

L'infrastructure doit permettre la sauvegarde des données. Enfin, il est indispensable que les conversations puissent être enregistrées afin d'assurer la traçabilité des échanges.

5.2 Guyane

5.2.1 Présentation du département

La Guyane, département-région de 83 853km², est située dans le nord-est de l'Amérique du sud, entre le Surinam et le Brésil. Elle est limitée :

- au nord par la côte qui, dans son ensemble, est plate et marécageuse ;
- à l'est par le fleuve Oyapock séparant la Guyane du Brésil ;
- à l'ouest par le fleuve Maroni séparant la Guyane du Surinam ;
- au sud par la frontière avec le Brésil. Cette frontière est matérialisée par la ligne de partage des eaux avec le bassin de l'Amazon.

Les 252 000 habitants de la Guyane sont situés principalement sur les communes du littoral, le long de la route nationale ainsi qu'au bord des grands cours d'eau.

Tous les textes législatifs nationaux y sont applicables mais peuvent faire l'objet de mesures d'adaptation « nécessités par leur situation particulière », conformément aux dispositions de l'article 73 de la constitution.

Située au sein de l'Amérique du Sud, le contexte réglementaire relatif aux bandes de fréquence est différent de celui applicable en France métropolitaine.

5.2.2 Réseaux de communications

La répartition de la population et les contraintes environnementales expliquent la concentration des services commerciaux principalement le long du littoral et à proximité des quelques agglomérations situées dans les terres.



Figure 25 : Performances mesurées par l'ARCEP au premier semestre 2018, avec des terminaux compatibles 4G. Les points verts représentent les succès et les rouges illustrent les échecs en 4G (source : www.monreseau mobile.fr). Les cartes sont représentées au format A4 en annexe.

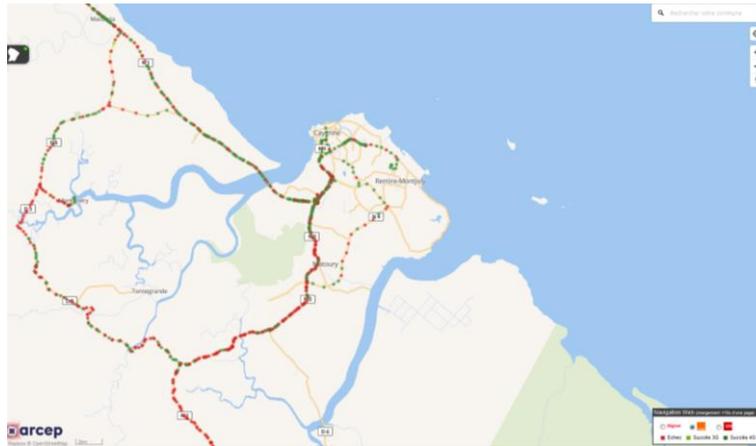


Figure 26 : A titre d'exemple, un zoom a été réalisé autour de Cayenne. Elle représente les tests réalisés par l'ARCEP pour le réseau d'Orange (charte graphique identique à la figure précédente). Ces cartes montrent que les réseaux 4G sont faiblement déployés même à Cayenne.

Dans la ville d'Albina du Surinam, ville frontalière avec la Guyane, la couverture 4G est excellente et fonctionne de manière optimale. Le réseau déborde sur Saint Laurent du Maroni située en Guyane.

Dans la ville d'Oiapoque, ville frontière située au Brésil, deux opérateurs privés présents. Pour autant, les réseaux 4G sont pratiquement inexistant. Des projets d'amélioration sont prévus dans un futur lointain car c'est une ville esulée au milieu de la forêt amazonienne.

Le SDIS973 est, par ailleurs, propriétaire d'un réseau de faisceaux hertziens. Un accès satellitaire est utilisé dans les zones blanches. Les réseaux radio des forces de l'ordre et de la sécurité civile fonctionnent principalement en analogique dans la bande de fréquence des 80 MHz.

5.2.3 Difficultés de réalisation

Dans les départements métropolitains, il est relativement aisé de créer une infrastructure. Ce n'est pas le cas en Guyane notamment par manque de pylônes et de réseaux (énergie et *backbone de télécommunications*).

Les deux tiers de son territoire sont composés de la forêt amazonienne. Cette forêt dense et compacte rend difficile l'établissement de communications fiables. D'autre part, la canopée en Guyane est nettement plus élevée qu'en Europe (~100m contre ~20m) introduisant un surcoût sur les pylônes de communications (hauteur plus élevée).

Ainsi, les difficultés techniques de réalisation des travaux associées aux actes de malveillances et de vols engendrent des coûts extrêmement élevés. En outre, la faible densité de population dans certaines zones et villes n'incitent pas à un développement par les opérateurs commerciaux. La stratégie métropolitaine basée sur une utilisation importante des opérateurs privés devra donc être adaptée.

Toutefois, la décision d'installation d'une trentaine de pylônes, dans le cadre de la mise en place de l'INPT Outre-Mer en Guyane, devrait toutefois améliorer la situation.

5.2.4 Réflexions sur le RRF en Guyane

Le développement d'une infrastructure classique « 4G » (*i.e.* basée sur un nombre élevés de pylônes reliés entre eux par faisceau hertziens et filaire) sur le territoire guyanais semble très difficile. Par conséquent, il semblerait pertinent :

- d'étudier la faisabilité de déployer les services offerts par le RRF à l'aide de quelques pylônes et de bulles tactiques en partie fixes (jusqu'à l'arrivée d'un service commercial), et en partie mobiles ;
- d'étudier la faisabilité du déploiement RRF sur une architecture « 3G », la couverture de cette dernière étant meilleure.

Ces bulles tactiques pourraient être reliées aux *data centers* hébergeant les applications du Réseau Radio du Futur par l'intermédiaire d'une liaison satellitaire. Toutefois, cette solution devra être validée techniquement car certaines applications fonctionnant en « *temps réel* » pourraient ne pas être compatibles avec un temps de latence élevé (temps de propagation jusqu'au satellite). En particulier, le temps nécessaire pour joindre le serveur hébergeant les applications MCPTT pourrait être un obstacle à l'établissement des communications opérationnelles et/ou de certaines fonctionnalités propres aux secours. Sous réserve de faisabilité technique, l'hébergement d'un serveur MCPPT local pourrait résoudre en partie ce problème.

5.3 Zones frontalières

Les zones frontalières présentent des caractéristiques particulières pour deux raisons :

- la réalisation d'interventions en France avec un service d'incendie et de secours étranger ;
- la réalisation d'interventions à l'étranger dans le cadre d'une opération de secours commune ;
- la possibilité pour les équipes françaises travaillant sur le territoire national de se faire « téléporter » sur un réseau d'un opérateur étranger.

Par conséquent, les équipements doivent assurer un fonctionnement sans engendrer de pertes de fonctionnalités dans les zones frontalières (tout en étant en France) ainsi qu'à l'étranger. De même, les solutions proposées devront veiller à réduire les coûts de fonctionnement à leurs stricts minimums.

6 Présentation de PC Storm : première brique du RRF

6.1 Préambule

PC STORM est la réponse du ministère de l'Intérieur aux nouveaux défis des télécommunications de crise. Conçu autour d'une bulle tactique déployable rapidement en fonction de la situation opérationnelle, ce système regroupe toutes les composantes techniques ou fonctionnelles permettant à une unité d'intervention de bénéficier d'un système de télécommunication performant, sécurisé et répondant aux nouveaux besoins du GIGN, BRI, GIPN, RAID, etc.

PC STORM n'a pas vocation à être déployé au profit des SDIS. Cependant, les technologies, les services offerts et l'articulation permettent de présenter ce que pourrait être une bulle tactique de la sécurité civile (inclus dans le programme RRF).

6.2 Articulation

6.2.1 Notion de réseau tactique

Les réseaux tactiques permettent à l'ensemble de leurs utilisateurs de bénéficier de leurs applications métiers (propre à chaque service et qu'il reste à définir pour la sécurité civile) et de communications de groupe multimédia.

Définition d'un réseau tactique : réseau de communications opérationnelles qui permet aux pompiers de communiquer sur le terrain entre eux (localement) ou avec leur hiérarchie (à distance).

Une fois un *backhaul* IP établi, les utilisateurs doivent pouvoir accéder à d'autres applications métier ainsi que joindre les autres membres de leur groupe de communication sur d'autres réseaux inter ou intra services.

Définition du *backhaul* : le *backhaul* est un réseau intermédiaire, permettant par exemple, l'émission et la réception de données entre un centre de radiodiffusion et une station terrestre d'un réseau satellite ou entre les équipements de raccordement d'abonnés.

L'architecture prévoira l'hébergement d'applications en local. Ainsi, l'usage de service dit critique tel que le MCPTT restera opérationnel même en zone peu ou mal couverte par les opérateurs.

Le gestionnaire de communications de groupe se doit de pouvoir être « utilisable » dans le cadre :

- d'une instance locale, (mode non connecté au réseau des opérateurs) par l'utilisation d'une bulle tactique par exemple ;
- d'une instance centrale (mode normal).

Le schéma ci-dessous reprend le principe de fonctionnement décrit précédemment :

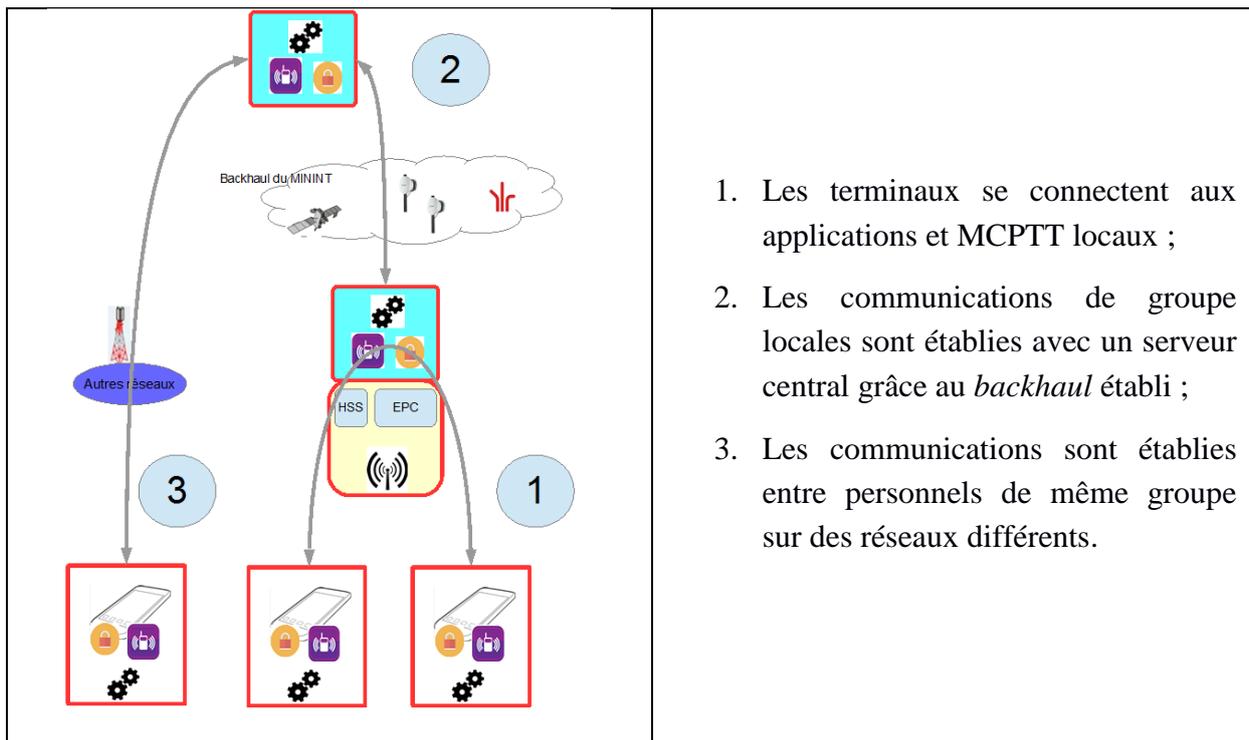


Figure 27 : principe de fonctionnement

Via l'utilisation d'une bulle tactique, les utilisateurs sous couverture de cette bulle communiquent via le MCPTT local même en cas d'intervention en zone blanche.

En zone couverte par les opérateurs, un utilisateur même hors zone de couverture de la bulle tactique peut se connecter au même réseau que les utilisateurs connectés au MCPTT local.

La notion de réseau de base et de plan de communication perd tout son sens puisque même un utilisateur connecté à un MCPTT local 1 et hors de la couverture du MCPTT local 2 pourra si le *backhaul* est établi entre les bulles tactiques communiquer avec ses correspondants distants.

6.2.2 Notion de groupe de recueil

Un utilisateur équipé qui n'est pas nécessairement prévu dans le dispositif initial peut être « recueilli » sur le réseau tactique et pouvoir communiquer avec les utilisateurs en écoute d'une communication dite de « recueil » ou de « repli », particulièrement si l'utilisateur recueilli est en détresse ou en présence d'un péril imminent.

L'architecture du réseau MCPTT est, contrairement à ANTARES, complètement décloisonnée et nativement interopérable. Les contraintes techniques interdisant les communications, tendent à disparaître. Les règles d'accès seront décidées en fonction du besoin d'en connaître, de l'opportunité d'une communication inter-services, etc.

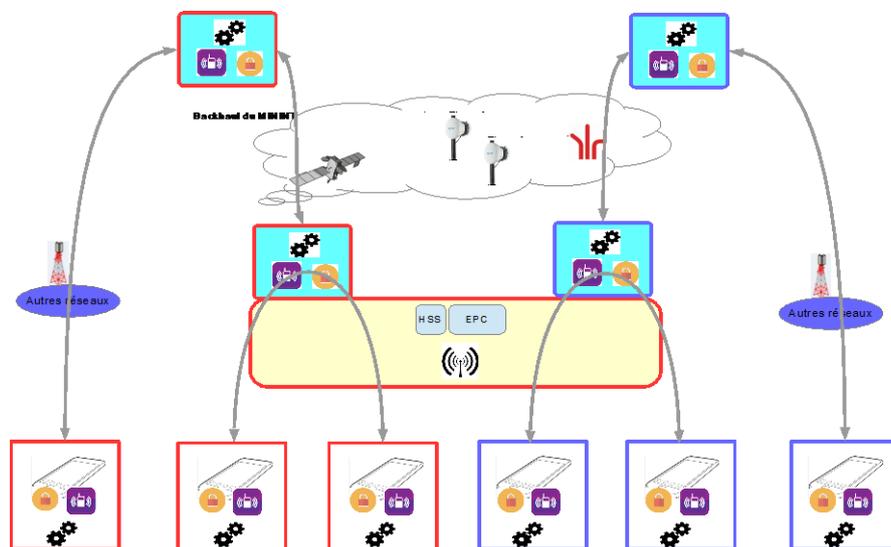
6.2.3 Fédération de réseaux tactiques

Les principes d'intervention des forces de sécurité et de secours répondent au principe du :

- déploiement initial dirigé par un COS, COP ou COG ;
- renforcé, si besoin, par des unités spécialisées.

Ce principe peut être repris par la chaîne technique. Deux scénarios sont proposés :

- un premier dispositif (*MCPTT*, *MCdata*, *Mcvidéo* locaux) est mis en place par le COS, COP ou COG puis les renforts sont rapidement intégrés en hébergeant les applications critiques nécessaires à l'intervention ;
- un premier dispositif mis en place par le « menant » est ensuite complété en capacité et en couverture par les dispositifs techniques renforçant le dispositif initial. Ces derniers joignent leurs propres applications et services.



- 1) L'entité rouge déploie la bulle tactique
- 2) L'administrateur rouge monte l'instance de l'entité bleue. Les communications de groupe locales sont assurées pour l'ensemble des entités
- 3) Une fois le backhaul établi, les communications de groupe sont relayées jusqu'à l'entité centrale « bleue ».
- 4) Les communications sont établies entre personnels de même groupe sur des réseaux différents.

Figure 28 : scénario « réseau tactique seul » et « entité concourante »

En suivant ce mode de déploiement en deux temps, nous pouvons distinguer deux types d'application :

- les applications dites critiques qui sont optimisées pour être opérationnelles sur bulles tactiques. Ces applications comme le MCPTT devront permettre aux primo-intervenants d'être opérationnels même sans activation du *backhaul* vers l'infrastructure du réseau et les serveurs centraux ;
- les applications lourdes qui nécessitent un accès obligatoire aux serveurs centraux et/ou à des serveurs privés (cartographie 3D par exemple). Ces applications ne pourront être hébergées localement du fait des limitations techniques des bulles tactiques et seront accessibles dès que le dispositif technique aura été renforcé (*backhaul* activé).

La fédération de deux réseaux tactiques permettra de mutualiser les applications communes à deux SDIS ou deux services différents (police - démineur de la sécurité civile).

Les interventions communes à deux SDIS s'affranchissent également des limitations liées aux réseaux de base utilisés dans la technologie TETRAPOL.

6.2.4 Réseaux permanents de transports des communications critiques

Le bond technologique initié par la migration entre TETRAPOL et LTE va voir émerger le besoin de protéger les communications des sapeurs-pompier. Les attaques informatiques étaient inexistantes sur le réseau ANTARES du fait de sa technologie propriétaire mais également par l'usage d'un réseau propre à l'État et opéré par lui-même.

Avec l'usage du réseau radio du futur, les communications opérationnelles seront plus vulnérables car :

- la technologie sera commune à ce qui est proposé aux particuliers et aux entreprises ;
- le réseau de transport devient un réseau commercial ;
- ce dernier n'est plus opéré par l'État. Il reste supervisé par les opérateurs privés.

Les solutions LTE supportant les communications critiques aux missions de sécurité publique assurent la confidentialité et la permanence des communications pour les agents.

Le standard 3GPP, à l'instar des solutions NEOGEND et TEOREM IP assure la confidentialité des communications par l'isolement des niveaux applicatifs des réseaux de transports.

Les réseaux de transports doivent se sécuriser afin de préserver la permanence des communications (et lutter contre les interférences, pannes, dénis de services, etc.) et assurer une qualité de service (QoS) qui permet la fluidité des applications.

Le standard 3GPP intègre ce principe en adoptant sur la couche de transport du LTE les fonctions de priorité, préemption, qualité de service, propres aux besoins des services de communications de groupe multimédia critique et en confiant les contenus et les identités « métiers » au seul MCPTT abrité derrière ses barrières d'authentification et de cryptage.

Ainsi, un réseau pouvant transporter des flux critiques est principalement un réseau qui :

- applique les qualités de services adéquats sur les flux, même cryptés, désignés par l'administration publique et dont la supervision est gérée par contrat avec les opérateurs privés ;
- applique, en cas de limitations des ressources réseaux, la mise en priorité de flux, même cryptés désignés par l'administration publique et le reporte aux gestionnaires des flux. Cette mise en priorité des flux concourant à une mission de service publique doit faire l'objet de contrat de service entre les opérateurs et l'État ;
- applique, en cas de limitations des ressources réseaux, la préemption de flux moins prioritaires, même cryptés, désignés préemptables et le reporte aux gestionnaires des flux.

À ce jour, en radio-téléphonie et en IP, seule la technologie LTE a développé de façon industrielle cette capacité.

Pour la sécurité intérieure : un réseau pouvant transporter des flux critiques est un réseau qui assure une permanence des communications sur des cas de pannes des réseaux énergies, des infrastructures de transport ou des centres de commandement et dont les nœuds principaux sont sécurisés physiquement à l'accès et accessibles aux intervenants techniques de l'administration en toute circonstance (cas se rapportant uniquement à PC STORM).

De facto, et à ce jour, seuls les réseaux opérés LTE disposent à la fois de la technologie et des infrastructures permettant d'assurer l'établissement d'un réseau de transport proche de la satisfaction des besoins des communications critiques multimédias des unités du ministère de l'Intérieur.

À ce jour, les réseaux mobiles opérés disposent d'un peu moins de 20 000 sites chacun dont 7 à 8000 en LTE. Leurs engagements auprès de l'ARCEP de couverture en LTE les portent au-delà de 98 % de la population et de l'ordre de 95 % du territoire métropolitain pour un service piéton extérieur à l'horizon du début de la prochaine décennie.

Essentiellement, ses fonctions visent à retrouver la permanence des communications en mode isolé, permettant ainsi à l'ensemble des agents sous couverture d'un site de pouvoir toujours communiquer entre eux.

Le niveau de service des réseaux TETRAPOL (ACROPOL, ANTARES, RUBIS) correspond à l'assurance d'une communication voix de groupe en tout lieu, au moins à l'extérieur des bâtiments.

La garantie de permanence des communications assurée par les réseaux TETRAPOL est donc actuellement à ce niveau de service (voix).

Si la demande des utilisateurs est bien de bénéficier de niveau de service d'au moins celui des réseaux opérateurs en débit et en couverture en mode nominal, la contrainte de permanence

des communications est, à court terme, d'atteindre sur le niveau actuel de couverture des services voix des réseaux TETRAPOL.

A noter également que ces usages multimédias ne sont pas considérés comme critiques à la mission, (c'est à dire comme un requis à la mobilisation des agents). Seules les communications voix, les signalisations de détresse, de péril imminent et la géolocalisation le sont.

L'évolution de l'offre de service multimédia, si elle est satisfaisante, entraînera à coup sûr une augmentation de la demande en termes de débit, de bande passante, de communication « temps réel », etc.

Et en parallèle, tant que leurs services sont nominaux, d'assurer les communications multimédias par les réseaux opérés offrant les qualités de services nécessaires.

6.2.5 Réseaux partenaires

Ici, les réseaux partenaires sont des réseaux aptes aux communications critiques, émettant en 700 MHz PPDR assujettis à des obligations d'accueil des intervenants de l'administration concourant à la sécurité civile. Du point de vue de l'utilisateur, les réseaux partenaires, doivent offrir les mêmes services que les solutions en propres de l'administration.

En approche d'un réseau partenaire, l'utilisateur doit pouvoir basculer sans coupure et sans interruption (même momentanée de service) vers le réseau partenaire dès que celui-ci est plus apte à porter ses services et vice-versa. C'est le principe du *roaming* ou de l'itinérance en français.

Les réseaux partenaires se doivent de répondre également à cet objectif et mettre en œuvre les moyens nécessaires afin d'interfacer les éléments de réseau de l'administration ou de ces délégués.

Les deux modes de passages de réseaux envisagés avec les réseaux partenaires sont les :

- Roaming Home routed avec S10 ;
- RAN sharing MOCN.

Le choix de l'usage d'un mode ou de l'autre doit résulter d'une décision commune maximisant l'expérience utilisateur et diminuant les efforts d'exploitation.

Dans le cas où des réseaux partenaires sont en parallèle avec un réseau opéré délégué par l'administration, il appartiendra au gestionnaire du réseau opéré de mettre en place, avec le réseau partenaire les décisions de mobilité permettant de s'assurer du transport des communications au mieux des ressources disponibles et des priorités.

6.3 Services offerts

6.3.1 Communication de groupes multimédias

L'ensemble des intervenants doit pouvoir communiquer en multimédia entre eux suivant leur organisation. Le même terminal doit être unique quelque soit le réseau utilisé (multi-opérateur ou bulles tactiques). Chaque utilisateur doit pouvoir maîtriser son périphérique de façon intuitive. Pour cela, la « couche technique » doit être le plus possible à charge des intervenants spécialisés tels que les administrateurs. La mise en place d'une supervision des terminaux incluant une gestion à distance de ceux-ci est un sujet qu'il convient de maîtriser si l'on recherche l'adhésion des utilisateurs à ce nouvel outil.

PCSTORM prévoit en conséquence une application de communications de groupe multimédia, un jeu d'applications clientes sur un terminal unique.

La communication de groupe multimédia se doit également de pouvoir prendre en compte le manque de ressources indiqué par les réseaux afin d'assurer la communication des utilisateurs et des informations considérées comme les plus critiques.

La communication de groupe multimédia est conçue pour prendre en compte les créations, les modifications ou les suppressions de groupes en fonction de la situation tactique, les hiérarchies et les différentes priorités de communications au sein d'un même groupe. Cette gestion fine est assurée en temps réel et permet d'adapter l'ordre complémentaire des transmissions (OCT) à la situation tactique et cela sans délai.

Les communications de groupe multimédia sont protégées en authentification et en cryptage. Le ST(SI)² et l'ANSSI ont collaboré pour créer un OS spécifique à PCSTORM. Ce logiciel est dérivé d'ANDROID et se nomme SECDROID.

6.3.2 Applications métiers

Les unités sur le terrain doivent disposer de nombreuses applications métiers construites sur des serveurs web, email, etc.

Chaque service devra concevoir des applications propres à son métier et peu de logiciel seront mutualisables, hors les logiciels critique Par exemple, les besoins, très spécifiques, de la police scientifique ne seront probablement pas identiques à ceux des démineurs de la sécurité civile.

Dans le domaine applicatif, les logiciels devront être spécialisés et évolutifs, donc techniquement suivis par les concepteurs.

Ces applications sont en cours d'adaptation aux ergonomies et aux outils des mobiles qui seront choisis pour équiper les flottes usagers.

Certaines de ces applications sont considérées comme plus critiques à la mission que d'autres. Par exemple, la cartographie par rapport à un compte-rendu ou la géolocalisation des personnels et la transmission des détresses.

La plupart des applications métiers n'embarquent pas de protection d'authentification et de cryptage en propre. Elles se basent généralement sur un tiers de confiance pour les accès et les droits et sur des solutions externes à l'application de protection du transport tel que des tunnels chiffrés.

PCSTORM doit prévoir les environnements d'authentifications des utilisateurs et de transport sécurisés afin de permettre l'usage des applications métiers.

L'interopérabilité entre services ne se fera qu'aux prix d'une uniformisation des mesures de protection du réseau et des données pouvant être stockées dans chaque périphérique. Dans le cas contraire, il faudra craindre une séparation des réseaux entre les services qui feront l'effort de la sécurité et ceux moins exigeant dans ce domaine.

Les communications de groupe multimédia et les applications métiers utilisent les mêmes ressources réseaux pour échanger. En cas de limitation des ressources, il s'agit donc d'assurer une prise de décision automatique et efficace afin qu'un maximum des échanges puisse s'effectuer en particulier les plus importants. Les mécanismes de QoS en place sur le réseau des opérateurs devront systématiquement favoriser les services publics opérationnels.

PCSTORM prévoit un gestionnaire des demandes interfacés avec l'ensemble des applications métiers et de communications multimédia de groupe, afin de regrouper, qualifier et hiérarchiser les demandes d'ouvertures de flux vers les réseaux LTE.

Cette hiérarchie peut être appelée à évoluer mais reste du ressort des opérateurs sur leurs réseaux respectifs.

6.3.3 Gestion des terminaux

La gestion de la configuration des terminaux nécessite un dialogue sécurisé avec un serveur de configuration et de logiciel. Cette fonction de MDM (*Mobile Device Management*) permet de gérer les terminaux à distance et de veiller à ce que ces derniers soient à jour lors de la prise de garde par exemple.

L'architecture de PCSTORM intègre une fonction de MDM administrable par chaque entité utilisatrice. A titre indicatif, le MININT a déjà déployé la solution Mobile Iron et la solution Maas360.

6.3.4 Accès aux réseaux nationaux et internationaux

L'accès au réseau ne doit pas se limiter à quelques zones délimitées à la zone de responsabilité d'une unité. PCSTORM permet de joindre l'ensemble de ses intervenants sur le territoire national et au-delà.

En premier lieu, la signalisation de « détresse » ou de « péril imminent » doit pouvoir être assurée de la façon la plus fiable possible pour les utilisateurs, même à l'intérieur d'un bâtiment, en utilisation de terminaux discrets de type « *handset* » en France et à l'étranger.

À ce jour, les réseaux radio larges bandes disponibles en France et à l'étranger sont ceux des opérateurs commerciaux « fixes » (wifi) et « mobiles » (cellulaires 2G, 3G, 4G).

PCSTORM peut exploiter le plus grand nombre de ces réseaux afin d'assurer la plus grande disponibilité géographique et temporelle des communications ainsi que les réseaux tactiques ou fixes de l'administration.

6.3.5 Terminaux

Les terminaux utilisés par PCSTORM peuvent se connecter sur les réseaux tactiques et des réseaux commerciaux. Si nécessaire la bascule, d'un réseau à l'autre, est transparente pour l'utilisateur. Les bandes de fréquence utilisées pour les bulles tactiques sont PPDR : 700 MHz PPDR.

Chaque terminal PCSTORM dispose des applications dites critiques (MCPTT par exemple) et les applications clientes (légères ou lourdes) propres à chaque service (applications métiers).

Un logiciel client MDM pour *mobile device management* est installé sur chaque périphérique.

Définition : une application de *mobile device management* (MDM) ou « gestion de terminaux mobiles », est une application permettant la gestion d'une flotte d'appareils mobiles, qu'il s'agisse de tablettes, de smartphones, voire d'ordinateurs hybrides au format tablette ou d'ordinateurs portables. Cette gestion est effectuée au niveau du service informatique de l'unité.

L'objectif du MDM est d'harmoniser et de sécuriser la flotte des périphériques en s'assurant que tous les utilisateurs aient des programmes à jour et que leurs appareils soient correctement sécurisés.

Cette gestion centralisée, en temps réel et à distance permet à l'utilisateur de disposer d'un outil constamment à jour.

Les terminaux doivent fournir aux applications les services et interfaces permettant la géolocalisation, la prise de cap, la prise de photo, de vidéo, la prise de son, l'affichage de contenu multimédia, etc.

6.3.6 Service téléphonique

Le mode primordial de communications des intervenants est la communication en groupe fermé d'utilisateurs (communication de groupe multimédia).

Cependant, certains d'entre eux sont amenés à prendre contact avec des personnes en dehors de leur groupe de communication ou en dehors des services de la sécurité intérieure. Par exemple, si un préfet ne disposant pas de périphérique équipé pour la communication de groupe désire contacter un COS sur le terrain, il est nécessaire de conserver les capacités de communication à la voix, utilisant la 2G.

Ce service de téléphonie est prévu uniquement pour joindre des intervenants en dehors de la sphère sécurisée des intervenants. La sphère de communication sécurisée des intervenants locaux ou distants est assurée par les communications de groupe multimédia.

Techniquement, en dehors de la couverture native de l'opérateur, cela revient à implémenter une solution VoIP dont le serveur est directement géré par l'opérateur de service. A lui d'assurer le maximum de continuité de ses services entre le monde « data/IP » et le monde « circuit » natif du téléphone.

Opérationnellement, la mise en œuvre peut être plus simple car le partage de responsabilités entre le bénéficiaire et l'opérateur se situe au niveau du simple transport de flux et à l'installation du client de l'application sur le terminal. L'ensemble du service est sous gestion de l'opérateur.

En termes de sécurité, la gestion se fait au niveau du transport de flux et du terminal.

Ce dernier mode peut sembler moins sécurisé car reposant plus sur le fournisseur de service.

Il reste ouvert à une solution de *mobile virtual network operator* (« MVNO ») étatique. Il s'agit d'un opérateur de téléphonie mobile qui, ne possédant pas de concession de spectre de fréquences ni d'infrastructure de réseau radio propres, contracte des accords avec les opérateurs mobiles possédant un réseau mobile (connu sous le sigle MNO, de l'anglais Mobile Network Operator) pour leur acheter un forfait d'utilisation de leur réseau radio et le revendre sous sa propre marque à ses clients.

6.3.7 Cartes SIM, authentification et identification

Les terminaux sont authentifiés grâce à la carte SIM sur l'ensemble des réseaux dont ils pourront bénéficier. C'est à dire :

- réseaux tactiques nominaux ;
- réseaux opérés métropolitains et étrangers ;
- les réseaux de repli.

La carte SIM permet donc d'authentifier le réseau et le terminal tout en accédant à un maximum des réseaux mobiles, en particulier métropolitains.

La carte SIM permet de gérer les secrets et authentification liés à l'accès à ses propres réseaux (tactiques ou fixes, de repli ou non).

6.4 Présentation des lots composants l'offre PC STORM

6.4.1 Lot 1 : fourniture de bulles tactiques et de terminaux en bande 700MHz PPDR.

Configuration tactique :

Soutien/proximité : Cette solution est proposée pour les petites unités isolées et vise à fournir une solution légère pour des petites équipes. L'installation permanente en véhicule léger et sur l'homme (routeur portable en Wifi ou en 3G/4G) permettra la communication vocale. Les principales caractéristiques sont :

- un hébergement de la sécurité (SSI et résilience) et du MCPTT ;
- une autonomie de la batterie de 2 heures.

Intervention : cette solution propose un lot à déployer en quelques minutes desservant une force d'intervention. Les matériels :

- sont rackables pour installation en véhicule pré-équipé ;
- hébergent des applications métiers, de la sécurité (SSI et résilience) et de MCPTT sur serveur standardisé et pouvant être mis à jour facilement ;
- Autonomie batterie 2 heures.

Événementiel : Ce lot offre également une solution pour les équipes assurant le soutien sanitaire lors d'un événement planifié. Ce lot permet une couverture et une capacité importante. L'hébergement des applications métiers, de la sécurité et de MCPTT sont sur un serveur standardisé et mis à jour facilement (flux vidéo et stockage important à prévoir).

Le lot 1 proposera un ensemble de terminaux :

- smartphones standards ;
- tablettes ;
- accessoires associés ;
- contrôle par le MDM de l'administration.

MDM= *mobile device management* (permet de superviser à distance les périphériques de façon dynamique et en temps réel).

6.4.2 Lot 2 : Cartes SIM

Chaque terminal doit être équipé d'une carte SIM particulière qui répond aux besoins suivants :

- capacité à créer des cartes SIM en volume restreint aux requis de l'administration ;
- intégrer les secrets et les paramètres nécessaires à l'accès aux réseaux ;
- assurer la distribution sécurisée des secrets vers le HSS centralisé ;
- mise à jour « à distance » des paramètres ;
- ergonomie de sélection des profils d'accès depuis le smartphone ;
- capacité multi-USIM (plusieurs IMSI) et ergonomie de sélection ;
- confidentialité et facilité opérationnelle de la gestion des clefs en création et en répudiation ;
- mise à jour des paramètres et identifiants des cartes SIM « over the air » ;
- possibilité de distribuer rapidement de nouvelles configurations de cartes SIM.

6.4.3 Lot 3 : services opérateurs

Ce lot a pour but de pouvoir bénéficier des services des réseaux opérés commerciaux en données, voix et SMS. Les spécifications de ce lot sont :

- Les services de données sur plusieurs réseaux opérés métropolitains majeurs. Afin d'obtenir le meilleur accès au réseau en tout lieu et en tout temps, il convient de pouvoir basculer d'un opérateur à l'autre en fonction de l'état de son réseau à un moment donné ;

- les services de téléphonie voix, SMS, MMS sur plusieurs réseaux opérés métropolitains majeurs. L'administration désire conserver en parallèle des services critiques et multimédia, les services 2G qui peuvent être utilisé en mode dégradé. Le besoin d'itinérance en 2G répond à la nécessité d'offrir ce service même dans une zone non couverte par un opérateur donné ;
- les secrets d'accès au service et paramètres sur la carte SIM fournis par le lot 2 ;
- l'itinérance des services sur les réseaux étrangers en particulier en Europe pour les unités de la sécurité civile amenés à être projeté à l'étranger ;
- la continuité des services de téléphonie voix, SMS, MMS sur la bulle tactique ;
- la QoS sur la couche transport qui permet de préserver la permanence des communications (et lutter contre les interférences, pannes, dénis de services, etc.) et assurer une qualité de service permettant la fluidité des applications.

6.4.4 Lot 4 : applications et sécurité

Le lot 4 de PCSTORM permettra la diffusion des applications métiers de serveurs centraux ou locaux vers les périphériques des utilisateurs. Ce réseau sera sécurisé.

La solution proposée est entièrement gérée et déclinable sur les réseaux opérés et tactiques. Ce lot est bien sûr compatible avec des terminaux du lot 1.

Ce lot intègre la communication de groupe multimédia et la gestion de la QoS LTE conforme aux interfaces standards 3GPP MCPTT :

- chat, photo, vidéo, localisation, etc;
- poste tactique « *Dispatcher* ».

Ce lot traitera de la sécurisation de bout en bout pour les applications métiers jugés sensibles. L'interfaçage des applications développées par le secteur privé sont prévus dans le lot 4.

Pendant la phase de transition, l'interconnexion entre les périphériques TETRAPOL et RRF sont assurés par le lot 4.

6.4.5 Lot 5 : Passerelle

Ce lot permet l'interopérabilité des Centres de Commandement respectant la norme NF 399 avec les personnels équipés MCPTT.

Chaque CODIS, équipé d'un SGO respectant la NF 399, doit pouvoir participer aux communications de groupe et disposer de la géolocalisation des personnels dotés de périphériques PCSTORM.

Le traitement d'un appel de détresse émis par le service MCPTT doit pouvoir être exploité par un SGO NF 399.

6.4.6 Lot 6 : assistance à maîtrise d'œuvre

Il s'agit d'un lot portant sur le maintien en condition opérationnelle en cours de définition.

6.4.7 Lot 7 : services de sites fixes et interopérabilité réseaux partenaires.

L'objectif de ce lot est de disposer de communications de groupe multimédia résilientes permanentes sur des zones d'intérêt pour les unités de la sécurité civile que sont :

- l'emprise privée armée-par des agents de sécurité et d'incendie ;
- les établissements répertoriés.

Ce lot intègre l'étude d'ingénierie radio des zones sensibles d'intérêt pour le ministère. Les négociations, la mise en place et l'exploitation, la maintenance de points radio (nœud PPDR) en 700 MHz PPDR résilients entre dans le domaine de compétence de ce lot.

Ce lot vise également à résoudre les difficultés de communication dans un milieu « indoor ».

La mise en place et l'exploitation de la continuité de service entre les réseaux 700 MHz PPDR de l'administration et les réseaux opérés est prise en compte par le lot 7.

7 Perspectives : impacts du Réseau Radio du Futur

7.1 D'un point de vue opérationnel

Les sapeurs-pompiers ont conçu leurs schémas de communication en fonction d'une ressource radio rare (nombre de canaux relativement limités) et figée (reconfiguration du réseau en temps réel limitée). Le Réseau Radio du Futur, par ses capacités techniques, permet de s'affranchir de ces deux contraintes :

- la possibilité de créer des « salons de discussion » de manière dynamique permet d'envisager la création de groupes spécifiques sur des interventions de moyenne et grande envergure ;
- les capacités de transmission en « 4G » et « 5G » permettent de passer des informations non disponibles aujourd'hui :
 - vidéos ;
 - logiciels embarqués ;
 - informations issues de capteurs divers ;
 - etc.
- la possibilité de multiplier, presque, à l'infini le nombre de « salons de discussions ».

Cette liberté est bénéfique pour les secours. Toutefois, il conviendra de l'encadrer afin d'éviter que toutes ces communications et informations s'enchevêtrent et rendent incompréhensibles les messages.

Ainsi, il semble opportun qu'un travail portant sur les ordres complémentaires des transmissions (OCT) soit mené. En effet, même si l'OCT statique sera conservé pour 90% des interventions (communications entre un engin isolé tel qu'un VSAV et le CODIS), les communications « horizontales » sur le terrain (tant à l'intérieur d'un service d'incendie et de secours qu'en inter-services) pourraient être développées par l'intermédiaire des salons de discussion remettant ainsi en question la « verticalité » des communications. Cette étude devrait être menée à la fois par les COMSIC et par les services en charge des opérations au sein des services d'incendie et de secours car elle impacte directement la manière de commander (« *on ne parle qu'à son supérieur hiérarchique* »).

Preco_01	Réfléchir à l'évolution des OCT pour les opérations de moyenne et grande envergure	1
----------	--	---

Preco_02	Définir les modalités d'usage des « salons de discussion » afin de pouvoir mettre en œuvre aisément des communications inter-services	1
----------	---	---

L'augmentation du nombre de salons de discussion permettrait de créer autant de salons de discussions privés n'incluant que la station directrice et les engins concernés par une intervention. Il serait ainsi possible d'améliorer la confidentialité des messages alors qu'il suffit aujourd'hui de se mettre sur une communication de portée départementale pour entendre l'ensemble de l'activité (même si le terminal n'est pas engagé sur une opération). Ce cloisonnement permettrait également de communiquer des informations confidentielles étant donné que le salon est privé sans avoir à réaliser d'opérations particulières (telles que l'appel privé ou l'usage du téléphone portable). La figure ci-dessous représente un exemple garantissant l'étanchéité totale.

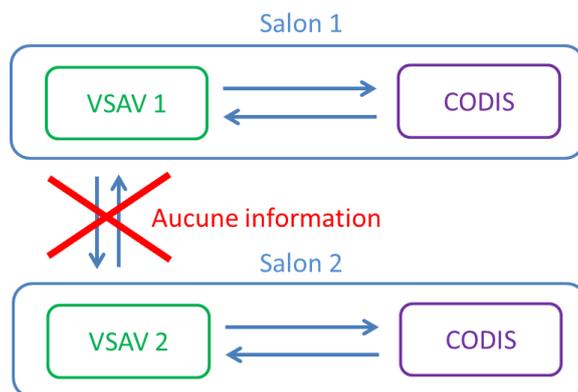


Figure 29 : exemple de cloisonnements entre « salons de discussion »

Afin de garantir une bonne communication avec la station directrice, et étant donné qu'un engin n'entend pas les autres communications, il est envisageable de mettre en place un indicateur sur le terminal montrant la disponibilité de la station directrice. En outre, il est également envisageable de créer une fonctionnalité permettant de s'inscrire dans la file d'attente de communication avec la station directrice. Un degré d'urgence spécifié par l'utilisateur pourrait être associé à cette inscription.

Preco_03	Étudier l'intérêt de cloisonner les communications opérationnelles et définir les modalités de mise en œuvre de ces cloisonnements	1
----------	--	---

D'autre part, il conviendra de définir des fonctions spéciales et des droits spéciaux afin de diriger les communications :

- possibilité de « couper la parole » à un utilisateur trop volubile ;
- possibilité de préemption de la parole à l'intérieur d'un salon de discussion (ex : COS s'adressant à l'ensemble de ces chefs de secteur) ;
- capacité d'un interlocuteur à parler à une personne de son choix présente dans un autre salon de discussion sans entendre les autres.

Enfin, il conviendra également de définir les conditions d'utilisation de toutes les applications opérationnelles autres que celles connues actuellement (usage de la vidéo, reconnaissance à distance via la vidéo, applications prioritaires, etc.).

Preco_04	Définir les conditions d'emploi des applications opérationnelles	1
----------	--	---

7.2 D'un point de vue organisationnel

Comme indiqué précédemment, un des enjeux est de pouvoir créer des « salons de conférence » dynamiquement tant en interne qu'en externe. Par conséquent, il convient de définir le personnel chargé de cette mission. Nous avons identifié deux catégories de personnel à qui confier la mission :

1. les « OFFSIC » ;
2. les chefs de salle CODIS.

Dans le premier cas, l'OFFSIC (et sous réserve qu'il soit intégré dans la garde) pourra répondre rapidement aux sollicitations du COS. Il sera parfaitement capable de maîtriser ce nouveau rôle étant donné sa technicité. D'autre part, sa connaissance du monde opérationnel lui permet de rapidement comprendre les attentes du COS, voire de les anticiper.

A contrario, certains départements n'ayant pas d'OFFSIC dans la garde, il pourrait être intéressant de confier cette mission au chef de salle « CODIS ».

Preco_05	Définir à qui confier le rôle d'administration des « salons de discussion »	1
----------	---	---

En parallèle, il convient de préciser les modalités de déploiement des bulles tactiques. Idéalement, la bulle tactique est intégrée aux véhicules d'intervention et l'intervention du chef d'agrès est basique (uniquement allumer la bulle tactique par une simple pression manuelle). Toutefois, du personnel devrait être disponible pour régler les petits problèmes soit à distance, soit sur place. Deux choix sont à nouveau possibles :

1. confier la mission aux « OFFSIC » ;
2. confier la mission à des techniciens.

Preco_06	Définir à qui confier le support technique des bulles tactiques	1
----------	---	---

7.3 D'un point de vue du développement d'applications

Jusqu'à présent, les services d'incendie et de secours disposaient de terminaux ayant un logiciel embarqué propriétaire. D'autre part, les terminaux actuels possèdent une capacité de calcul limitée. Avec l'arrivée du RRF et l'usage de terminaux grands publics (tablettes et/ou smartphone), basé sur un système d'exploitation ouvert, il sera possible de donner libre à cours à l'imagination. Toutefois, les ressources humaines et matérielles seront limitées. Par conséquent, il semble nécessaire de coordonner les développements applicatifs afin d'éviter un foisonnement d'applications onéreuses et non compatibles entre elles.

Preco_07	Coordonner le développement d'applications	1

Cette préconisation de coordination devrait être initiée le plus rapidement possible afin d'être prêts au moment des premiers déploiements.

D'autre part, il semble intéressant de favoriser l'émergence de standards d'échanges de données notamment pour tous les équipements (pompiers connectés, caméras thermiques, instruments de diagnostics connectés, etc.).

Preco_08	Favoriser/Renforcer l'émergence d'un standard pour les objets connectés pouvant être utilisés par la sécurité civile.	1

7.4 D'un point de vue de la formation

Ce changement de technologie va nécessiter de nombreuses actions:

- la mise à jour du REAC SIC en tenant compte notamment des missions confiées aux différents niveaux (COMSIC, OFFSIC et Chefs de salle) ;
- la formation des COMSIC ;
- la formation des OFFSIC ;
- la formation des COS ;
- la formation des chefs d'agrès ;
- la formation des autres sapeurs-pompiers ;
- la formation des personnels techniques au sein des SDIS.

La formation des personnels techniques est un point important notamment en termes d'acquisition. Contrairement à la situation actuelle, les services techniques vont pouvoir procéder à l'achat de marques différentes.

Par conséquent, le personnel qui procédera aux achats devra être formé bien avant afin de pouvoir établir un dossier de consultation des entreprises conformes aux besoins du SDIS alors que, dans la situation actuelle, les efforts se portaient principalement sur les conditions tarifaires et le maintien en condition opérationnelle. En absence de formation indépendante, il

se pourrait que ce soient les fabricants eux-mêmes qui forment le personnel avec toutes les limites que ce type de formation implique.

Preco_09	Mettre en place une formation destinée aux supports techniques des SDIS afin qu'ils puissent acquérir du matériel satisfaisant les besoins des sapeurs-pompiers.	1
----------	--	---

Preco_10	Anticiper une évolution du REAC SIC	1
----------	-------------------------------------	---

7.5 D'un point de vue de l'acquisition et de la maintenance

Comme indiqué à la section 7.4, l'acquisition de matériel et le maintien en condition opérationnelle va être plus complexe grâce à la liberté offerte par le RRF. Par conséquent, le rôle des acheteurs (services techniques et services marchés) va être renforcé.

Par conséquent, il semble intéressant d'explorer la création de cahiers de charges types pour les terminaux et les bulles tactiques qui seraient modifiés par chacun des entités adjudicatrices à l'image du cahier des charges type consacré au « Système de Gestion Opérationnelle » dont l'écriture a été dirigée par la DGSCGC. Ces cahiers types contiendraient l'ensemble des points essentiels (depuis la spécification des besoins jusqu'au maintien en condition opérationnelle en passant par la conduite du changement) ; les services d'incendie et de secours pouvant adapter ces points clefs à leurs propres spécificités. Cette manière de procéder permettrait de réduire le temps nécessaire pour basculer de l'INPT au RRF tout en garantissant que les points clefs soient bien pris en compte.

Preco_11	Coordonner au niveau national la création d'un cahier des charges « type » portant sur les terminaux et les bulles tactiques à destination des services d'incendie et de secours.	1
----------	---	---

Dans cette optique, la mutualisation des achats par les services d'incendie et de secours semble constituer également une piste à évaluer afin de réduire les coûts (tant pour la procédure d'achat que pour les achats de matériel que de prestations). Cette mutualisation pourrait être inter-services. Il serait ainsi intéressant d'évaluer les mutualisations possibles avec les autres services concourant aux missions de sécurité civile afin de procéder à des marchés communs lorsque les besoins sont similaires (ex : création de bulles tactiques).

7.6 D'un point de vue de la structure porteuse

Les usages et les technologies évoluent extrêmement rapidement à l'image de la société qui subit des transformations profondes. Des pans entiers de l'économie sont menacés de disparition ou de transformation sous l'émergence de différentes tendances :

- l'*ubérisation* de certains secteurs (chacun devenant producteur d'un service ou de fournitures au détriment de structure figée),
- le fonctionnement transversal de la société et la remise en cause des organisations verticales,
- la numérisation de certains métiers et le remplacement par l'intelligence artificielle (ex : la disparation du métier de « caissier » et de « conseiller téléphonique »).

Grâce aux choix d'une technologie grand public, il existe une opportunité pour offrir aux sapeurs-pompiers des outils évoluant avec les usages et les technologies. L'évolution des outils RRF devra se faire au même rythme que l'évolution des outils grands publics pour éviter que les utilisateurs préfèrent d'autres outils et se détournent ainsi des outils RRF.

Il nous apparaît ainsi important que la structure porteuse soit à même de fédérer l'ensemble des acteurs (start-up, universités, services d'incendies et de secours, hackatons, etc.) pouvant innover et proposer des services à valeurs ajoutées. Elle pourrait ainsi animer un réseau de compétences (avec par exemple des appels à projets, des labellisations) au bénéfice de tous les utilisateurs. Les acteurs de ce réseau pourraient se voir confier en cogestion ou en délégation certains projets.

Cette possibilité permettrait également de faire émerger de nouveaux acteurs économiques qui pourraient proposer de nouveaux services, créer des entreprises et exporter leur savoir-faire et produits.

Enfin, il nous intéresse de développer des méthodes « agiles » à l'image de certains projets nationaux utilisant cette méthode projet. Les temps de développement et de mise en œuvre devront être courts. Les étapes normatives trop longues qui créent un décalage entre la société civile et la sécurité civile devront être réduites au strict minimum.

8 Conclusion

Les choix à la base du Réseau Radio du Futur permettent d'envisager une adoption rapide de ce nouvel outil tout en répondant aux besoins du terrain. Le champ du possible s'élargit énormément ; la seule limite étant l'imagination. L'enjeu sera d'exploiter au mieux les capacités techniques entre-aperçues alors que la sécurité civile a longtemps vécu avec un système prioritaire et fermé. Face à ce changement de paradigme, il conviendra de faire preuve d'adaptation et de créativité. La société civile et l'ensemble des parties prenantes de la sécurité civile devront se concerter pour faire émerger ces outils innovants.

D'autre part, le Réseau Radio du Futur devra être souple et s'adapter avec les évolutions technologiques et d'usages afin de rester en phase avec son temps. L'arrivée de nouvelles générations de sapeurs-pompiers, pratiquement nées avec un *smartphone*, constitue une force sur laquelle s'appuyer pour imaginer le futur.

Ce travail de mémoire a permis d'esquisser les besoins. Un travail rigoureux et approfondi complémentaire devrait être mené pour préciser plus finement les besoins fonctionnels et la manière de les implanter. Ainsi, au-delà des aspects techniques (en passant de la couverture réseau à la fiabilité et la résilience), l'ergonomie est la principale attente. D'autre part, les fonctionnalités permettant d'améliorer la sécurité des intervenants ainsi que la compréhension de l'événement ont été jugés comme prioritaires.

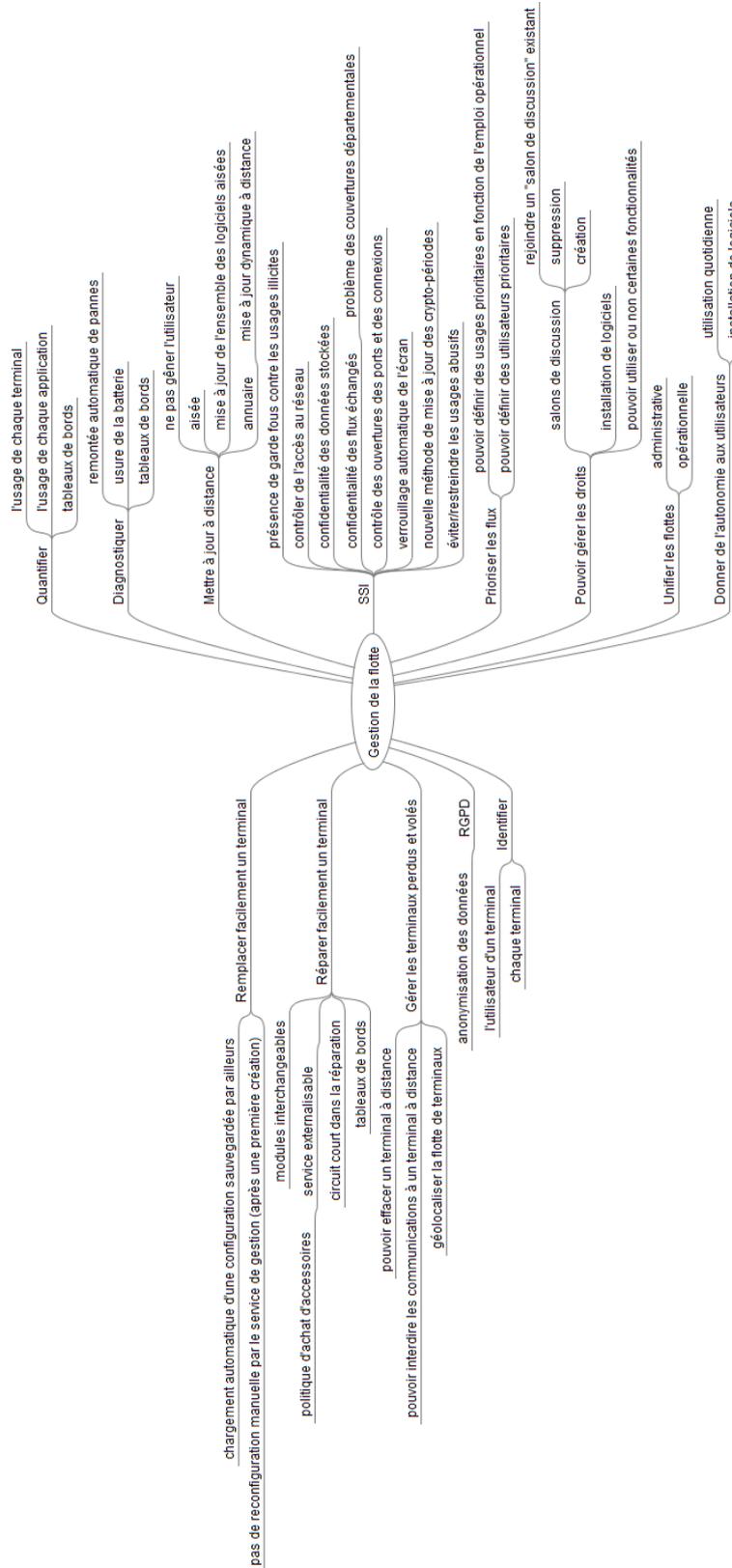
Alors que les entretiens avec les personnels portaient sur les outils de communication, ces utilisateurs ont insisté sur la nécessité d'adapter la technique aux Hommes (et non l'inverse). L'être humain doit rester le centre de décision et les outils doivent être pensés comme une aide facilitant les missions du commandant des opérations de secours. Ainsi, il devra être fait attention à ne pas submerger le sapeur-pompier d'informations.

Le métier de sapeur-pompier est un métier humain au service de la population et de l'environnement.

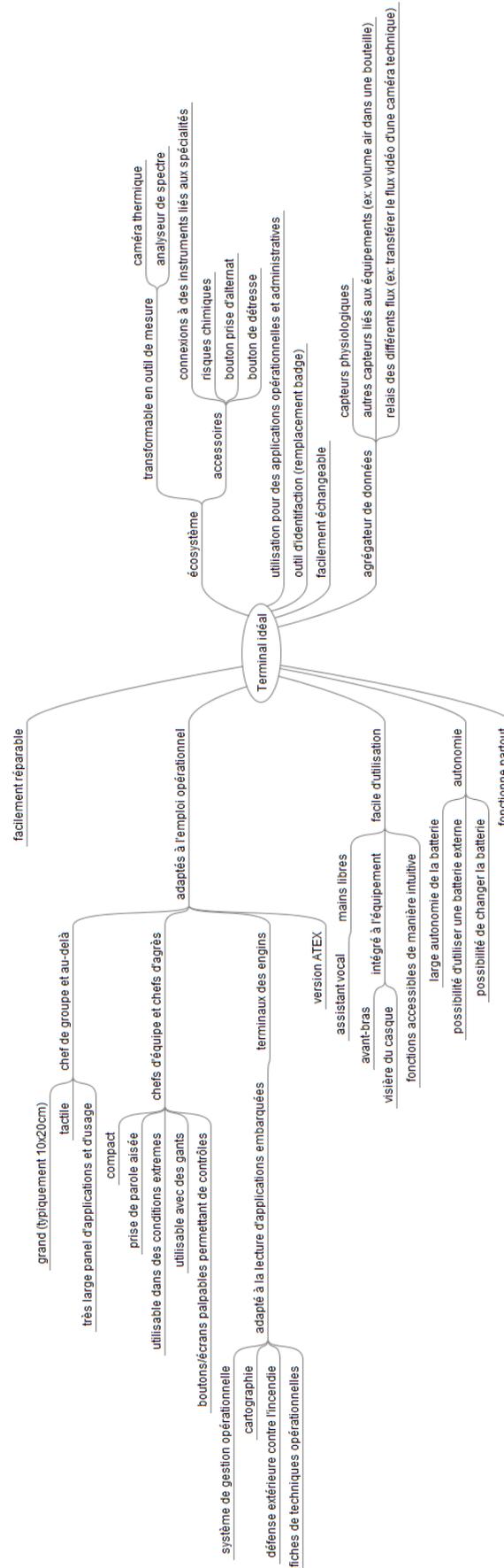
9 Annexes

9.1 Cartes mentales

9.1.1 Besoins de l'administrateur fonctionnel



9.1.2 Terminal idéal



9.2 Cartes de couverture par les opérateurs commerciaux en Guyane

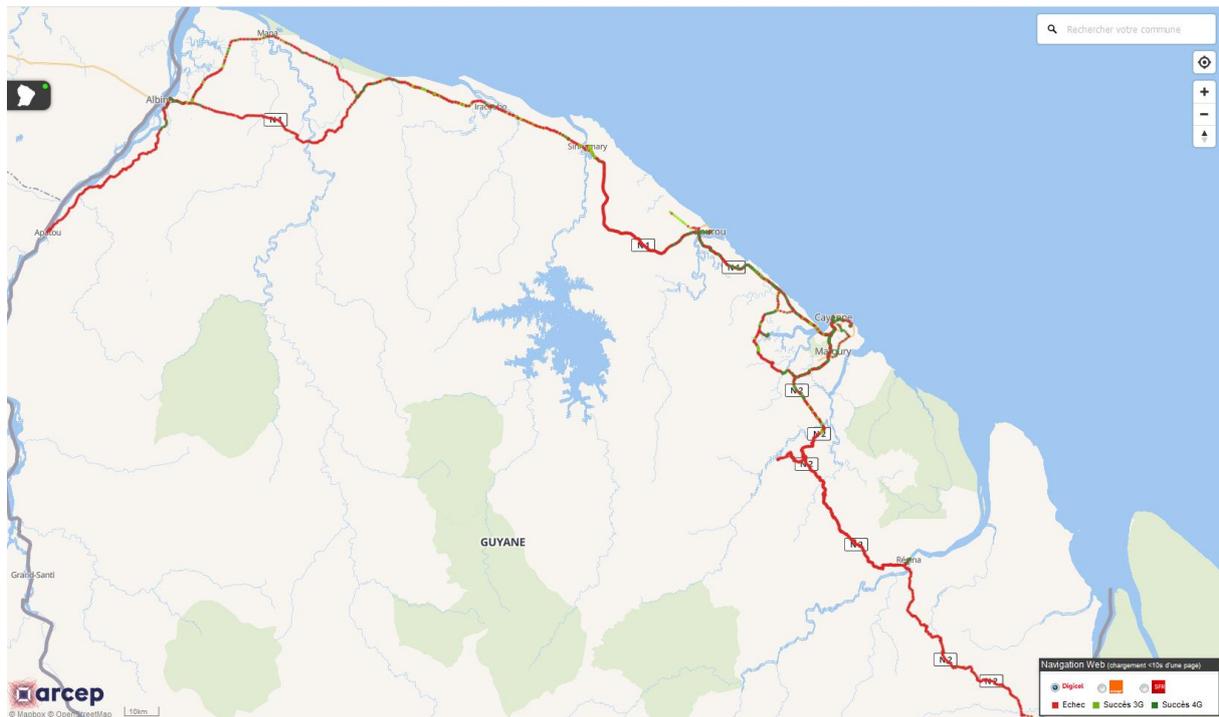


Figure 30 : Digicel

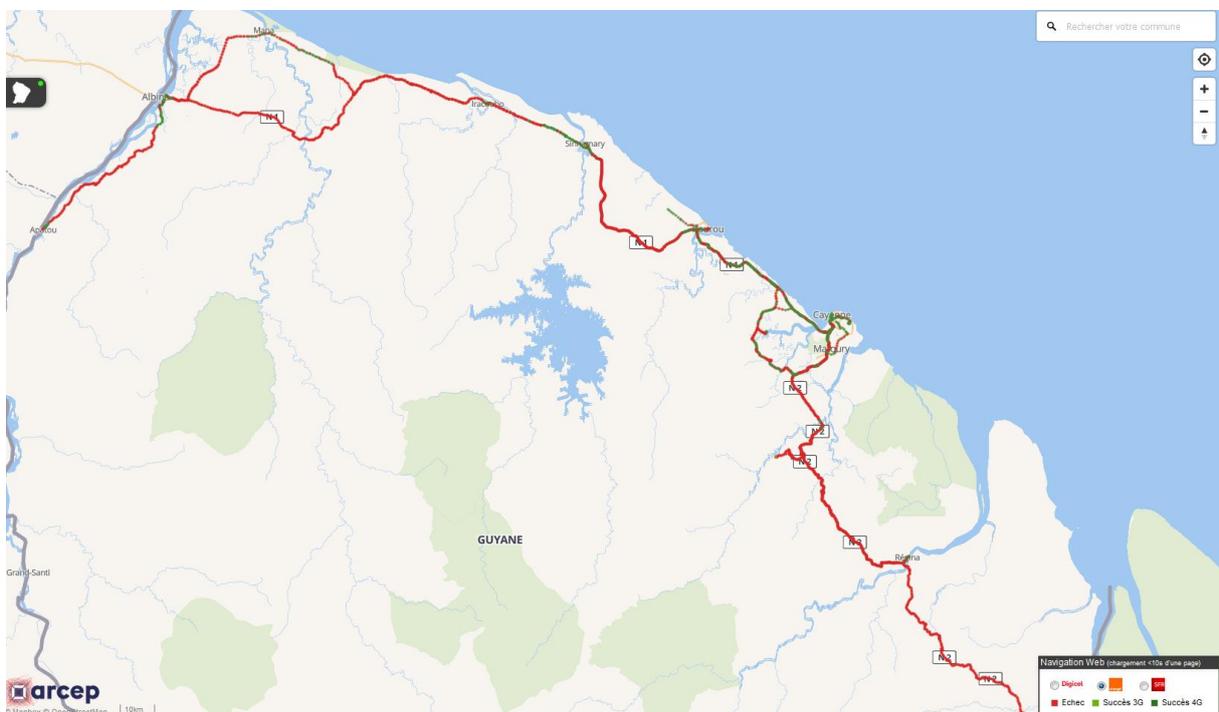


Figure 31 : Orange



Figure 32 : SFR

10 Bibliographie

Airbus. (2011). *Système PMR - Présentation Générale*. Airbus.

Finley, & Al. (2017). *Benefits of mobile end user network switching and multihoming*. Computer Communications.

Herreman, T., & al. (2009). *ANTARES: document de vulgarisation à destination des COMSIC*. ENSOSP.

Juppé, A. (1997). *Décret n°97-464 du 9 mai 1997 relatif la création et à l'organisation des services à compétence nationale*.

Karimi, & Al. (2017). *Evaluating 5G Multihoming services in the mobility first future Internet architecture*. IEEE 85th Vehicular Technology Conference (VTC Spring).

Kodiak. (2017). *What is MCPTT ?* Kodiak.

MI. (2018). *Le réseau radio du futur*. Ministère de l'Intérieur - Réunion des COMSIC;.

Pujolle. (2011). *Les réseaux - édition 2011*. Eyrolles.

Pujolle. (2018). *Les réseaux - l'ère des réseaux cloud et de la 5G*. Eyrolles.

Villebrun, E. (2018). *Le Réseau Radio du Futur*. Sécurité et Défense Magazine.

RÉSUMÉ

Le Réseau Radio du Futur, basé sur le standard *Long Term Evolutioni (LTE)*, est amené à prendre la relève de l'Infrastructure Nationale Partagée des Transmissions au cours de la prochaine décennie. Ce mémoire présente tout d'abord les technologies sous-jacentes à ce nouveau réseau avant d'aborder les besoins des sapeurs-pompiers. Ces besoins ont été étudiés sous trois angles : le besoin fonctionnel du sapeur-pompier sur le terrain, la description du terminal idéal et enfin les besoin de l'administrateur fonctionnel d'un service d'incendie et de secours. Les contraintes de réalisation ont été identifiées pour trois cas particuliers : une zone urbaine très dense, une zone frontalière et la Guyane. La première brique de ce nouveau réseau, appelée *PC STORM*, est ensuite présentée. Quelques impacts de ces nouvelles technologies et de ces nouveaux usages autorisés ont enfin été répertoriés. Des propositions de réflexions et d'anticipation sont proposées.

ABSTRACT

French firefighters use a network which will be changed in the next few years. This new network is called "Réseau Radio du Futur" (i.e. Future Radio Network in English) and will be based on Long Term Evolution (LTE) standards. This dissertation first introduces key technologies used by this new network. Firefighter needs are then analyzed. Three points of views are considered: tactical needs, description of the ideal mobile terminal and administrator needs. Environment constraints for three regions are then summarized: high density area, border regions and Guyane. First products used in this next generation network, called *PC STORM*, are introduced. As this technology opens up a large panel of use and applications, consequences and some recommendation are listed.