Radio logicielle : analyse d'architectures matérielles et outils informatiques

Michaël Nicolas

le cnam

CONSERVATOIRE NATIONAL DES ARTS ET MÉTIERS

CENTRE RÉGIONAL ASSOCIÉ DE VERSAILLES

MÉMOIRE

présenté en vue d'obtenir

le DIPLOME D'INGÉNIEUR CNAM

SPÉCIALITÉ : ÉLECTRONIQUE

par

Michaël NICOLAS

Radio logicielle : analyse d'architectures matérielles et outils informatiques

Soutenu le

JURY

PRESIDENT :

MEMBRES :

Remerciements

Je tiens en premier lieu à remercier très sincèrement Emmanuel Duponchelle pour m'avoir accueilli au sein de son laboratoire et proposé un sujet de stage aussi passionnant que celui-ci. Je tiens aussi à remercier chaleureusement Chaouki Kasmi pour avoir accepté d'endosser la responsabilité de co-encadrant (avec Emmanuel) après seulement une année d'exercice à l'ANSSI (chapeau !). Mes deux tuteurs ont su me donner les bons conseils aux bons moments afin de me guider dans les recherches et expérimentations, tout en me laissant une large autonomie et une grande liberté dans le choix des axes d'étude.

Je remercie vivement toute l'équipe du laboratoire Sans Fil pour sa disponibilité, sa volonté de rendre service, sa générosité, sa bonne humeur et les connaissances qu'elle m'a fait partager. Je tiens notamment à exprimer toute ma gratitude à Pierre-Michel Ricordel pour m'avoir permis de réaliser ce mémoire dans des conditions optimales, ainsi que pour ses conseils pertinents. Je souhaite également remercier tout particulièrement Jean-Louis Ferracci ainsi que son équipe, Hervé Cagnon, Christine Blé et Isabelle Lenormand pour leur soutien et leur disponibilité. Mes remerciements s'adressent aussi à Philippe Mège (mon tuteur CNAM), Olivier Levillain, Christian Lixi, Dominique Chandesris, Loïc Duflot et à toutes les personnes qui m'ont aidé pendant ce stage.

Enfin, j'ai une pensée toute particulière pour mon épouse Isabelle et mes filles Angélina et Annaëlle, que je remercie pour leur soutien et leur patience infinie tout au long de cette aventure.

Liste des abréviations

3GPP *3rd Generation Partnership Project* (projet de partenariat de 3ième génération). 3GPP est une coopération internationale entre organismes de standardisation en télécommunication (exemple : l'ETSI pour la zone Europe), visant à produire des spécifications techniques pour les réseaux mobiles de troisième génération (3G) ainsi que la maintenance et le développement de spécifications techniques pour les normes mobiles GSM (GPRS, EDGE...).

AGC *Automatic Gain Control* (contrôle automatique de gain).

ANSSI Agence nationale de la sécurité des systèmes d'information.

AM *Amplitude modulation* (modulation d'amplitude). L'AM consiste à faire varier l'amplitude d'un signal de fréquence élevée en fonction d'un signal utile basse fréquence.

API *Application Programming Interface* (interface de programmation). Une API est un ensemble de fonctions, procédures ou classes mises à disposition par une bibliothèque logicielle, un système d'exploitation ou un service. Son rôle est de permettre l'interaction des programmes les uns avec les autres.

ARC *Access Rights Class* (classe de droits d'accès), indique le type d'accès à un réseau DECT (public, privé ou résidentiel). Cf. annexe C §C.4.

ARCEP Autorité de Régulation des Communications Électroniques et des Postes

ARI (DECT) *Access Rights Identity* (identité de droits d'accès), identité globalement unique indiquant les droits d'accès à un fournisseur de service. Il y a trois catégories d'ARI : PARI, SARI et TARI. Cf. §IV.3.1.2 et annexe C §C.4.

ASIC *Application-Specific Integrated Circuit* (circuit intégré à application spécifique). Cf. annexe B §B.9.1.

BPSK *Binary Phase Shift Keying* (modulation par déplacement de phase à deux états). La BPSK est une modulation par changement de phase à deux états (0 et π).

BTS (GSM) *Base Transceiver Station* (station de base), ou antenne relais. Cf. §III.4.2.

BSS (Wi-Fi) *Basic Service Set* (ensemble de services de base). Cf. §III.3.1.
(GSM) *Base Station Sub-system* (sous-système radio). Cf. §III.4.2.

CAN Convertisseur analogique/numérique. Cf. annexe B §B.4.

CDMA *Code Division Multiple Access* (Accès multiple par répartition en code - AMRC). CDMA est un système de codage des transmissions basé sur la technique d'étalement de spectre et permettant à plusieurs liaisons numériques d'utiliser simultanément la même fréquence porteuse.

CEA Commissariat à l'énergie atomique et aux énergies alternatives.

CIC *Cascaded Integrator-Comb* (filtre d'intégrateurs en cascade). Un filtre CIC est un filtre numérique de décimation ou d'interpolation de facteur entier.

CLB (FPGA) *Configurable Logic Block* (bloc logique configurable). Cf. annexe B §B.9.3.

CORBA *Common Object Request Broker Architecture*. CORBA est une norme industrielle décrivant les interfaces entre composants logiciels. Elle utilise un langage de définition d'interface, IDL, indépendant du langage de programmation. Le code IDL peut ensuite être compilé pour un langage de programmation spécifique, et génère automatiquement le code d'interface interprocessus nécessaire, comme par exemple des commandes pour la mémoire partagée ou les appels de procédure distante ou RPC (*Remote Procedure Call*). Cela permet une interopérabilité entre les composants de différents utilisateurs, même en cas d'utilisation de langages de programmation différents.

CPRI *Common Public Radio Interface* (interface radio publique commune). Cf. [cpri].

CSMA/CA *Carrier Sense Multiple Access with Collision Avoidance* (accès multiple avec détection de porteuse et évitement de collision). Le CSMA/CA est un protocole utilisant un mécanisme d'esquive de collision basé sur un principe d'accusé de réception réciproque entre l'émetteur et le récepteur.

CW *Continuous Wave* (onde continue). En terminologie radioamateur, ce terme est synonyme de code Morse.

dB Décibel. Le dB correspond au dixième de bel, unité de mesure logarithmique du rapport entre deux puissances.

dBc *Decibels relative to the carrier*. Le dBc représente le rapport de puissance entre un signal et une porteuse.

dBi *Decibels relative to an isotropic antenna*. Le dBi représente le gain d'une antenne en prenant pour référence une antenne isotrope (antenne fictive rayonnant uniformément dans toutes les directions).

DBPSK *Differential Binary Phase Shift Keying* (modulation par déplacement de phase différentielle à deux états). Technique de modulation consistant à matérialiser le signal binaire par un changement de phase d'une porteuse, un déphasage de π étant interprété comme un '1' binaire et l'absence de déphasage comme un '0'.

DCS *(GSM) Digital Communication System*. Cf. §III.4.3.1.

DDC *Digital Down-Converter* (convertisseur/abaisseur numérique). Cf. annexe B §B.7.

DECT *Digital Enhanced Cordless Telephone* (téléphone sans-fil numérique amélioré). Cf. §IV.3.1 et annexe C.

DQPSK *Differential Quadrature Phase Shift Keying* (modulation différentielle par déplacement de phase en quadrature). DQPSK est basé sur le même principe que DBPSK mais avec quatre états (symboles sur 2 bits, déphasages de $\pi/2$).

DSP *Digital Signal Processor* (processeur de signal numérique). Un DSP est un microprocesseur optimisé pour le traitement numérique du signal. Cf. annexe B §B.9.4.

DSSS *Direct Sequence Spread Spectrum* (étalement de spectre à séquence directe). Le DSSS est une technique d'étalement de spectre combinant les signaux utiles à un signal pseudo aléatoire de fréquence beaucoup plus élevée afin de permettre à plusieurs liaisons de partager la même fréquence porteuse (accès multiple par répartition par code), au prix d'une occupation spectrale plus large.

DUC *Digital Up-Converter* (convertisseur/éleveur numérique). Cf. annexe B §B.6.

éch/s Contraction de “échantillons par seconde”, unité de mesure de taux d'échantillonnage.

ECM *Electronic Counter Measures* (contre-mesures électroniques - CME).

EDGE *Enhanced Data rates for GSM Evolution*. Cf. §III.4.1.

ETSI *European Telecommunications Standard Institute* (institut européen des normes de télécommunication).

EVDO *EVolution-Data Optimized*. Standard de télécommunication pour la téléphonie 3G utilisant des techniques de multiplexage dont CDMA et TDMA.

FDD *Frequency Division Duplexing* (duplexage fréquentiel). Le FDD est une méthode de duplexage de transmissions sans fil, où la fréquence de la porteuse du signal est différente suivant que le sens de la liaison est montant ou descendant.

FEC *Forward Error Correction* (correction d'erreur directe). FEC est un système de protection contre les erreurs de transmission, basé sur de la redondance de données afin de permettre au destinataire de détecter et de corriger une partie des erreurs.

FFT *Fast Fourier Transform* (transformée de Fourier rapide). La FFT est un algorithme amélioré de calcul de la transformée de Fourier discrète. Elle est couramment utilisée en traitement numérique du signal pour transformer des données discrètes du domaine temporel dans le domaine fréquentiel.

FHSS *Frequency Hopping Spread Spectrum* (étalement de spectre par saut de fréquence). Le FHSS est une méthode de transmission de signaux utilisant un étalement de spectre par saut (ou évasion) de fréquence. Il utilise plusieurs canaux répartis sur une large bande de fréquences selon une séquence pseudo aléatoire connue de l'émetteur et du récepteur.

FI Fréquence intermédiaire. C'est une fréquence interne à l'émetteur et au récepteur radio, servant de support à la modulation. Le signal modulé FI subit généralement une transposition en fréquence RF pour pouvoir être transmis.

FIR *Finite Impulse Response filter* (filtre à réponse impulsionnelle finie). Un filtre FIR est un filtre numérique dont la réponse est uniquement basée sur les valeurs du signal d'entrée (ce filtre est non récursif).

FIFO *First In, First Out* ("premier entré, premier sorti"), méthode de traitement des éléments d'une file.

FM *Frequency Modulation* (modulation de fréquence). La FM est un mode de modulation consistant à transmettre un signal par la modulation de la fréquence d'une porteuse. Les radios de la « bande FM » émettent en FM dans la bande [87,5 MHz - 108 MHz].

FP *Fixed Part* (station de base DECT), groupement d'équipements d'un réseau DECT situés entre le réseau local et l'interface air DECT.

FPGA *Field-Programmable Gate Array* (réseau de portes programmables *in situ*). Cf. annexe B §B.9.3.

GMSK *Gaussian Minimum Shift Keying* (modulation à déplacement minimum gaussien). La modulation GSMK est une modulation MSK associée à un filtre gaussien.

GPP *General Purpose Processor* (processeur à usage général). Cf. annexe B §B.9.5.

GPRS *General Packet Radio Service* (service général de radiocommunication en mode paquet).

GPU *Graphics Processing Unit* (processeur graphique). Cf. annexe B §B.9.6.

GRC *GNU Radio Companion*. Cf. §I.4.4.4.

GSM *Global System for Mobile Communications* (système global de communication mobile). Cf. §III.4.

HBF *Half-Band Filter* (filtre demi bande).

HDL *Hardware Description Language* (langage de description de matériel). HDL est un langage informatique permettant la description d'un circuit électronique.

HDLC *High-Level Data Link Control* (protocole de haut niveau de contrôle de la couche de liaison de données).

HDMI *High Definition Multimedia Interface* (interface multimédia haute définition). HDMI est une norme et interface audio/vidéo entièrement numérique pour le transfert de flux vidéo chiffrés non compressés.

HF Haute fréquence. La HF désigne les ondes radio dont la fréquence est comprise entre 3 MHz et 30 MHz.

HiperLAN *HIgh PERformance radio LAN*. L'HiperLAN est un standard européen de réseau local sans fil, et une solution alternative au 802.11 mais qui n'a pas connu le même succès.

I2C *Inter Integrated Circuit*. I2C est un bus série et synchrone.

ICNIA *Integrated Communications, Navigation, Identification, Avionics.*

IDL (CORBA) *Interface Description (or Definition) Language*. Cf. "CORBA".

IMEI (GSM) *International Mobile Equipment Identity* (identité internationale d'équipement mobile). Cf. §III.4.2.

IMSI (GSM) *International Mobile Subscriber Identity* (identité internationale d'abonné mobile). Cf. §III.4.2.

IP (VHDL). *Intellectual Property* (propriété intellectuelle). Cf. annexe B page XXVI.
(Réseau). *Internet Protocol.*

IPUI (DECT) *International Portable Users Identity* (identité internationale d'un PP). Cf. annexe C §C.4.

ISM Industriel, Scientifique, et Médical. Les bandes ISM [ism] sont des bandes de fréquences pouvant être utilisées librement pour des applications industrielles, scientifiques et médicales. Les seules obligations à observer sont la puissance d'émission (en intérieur ou en extérieur) et la non-perturbation de fréquences voisines. La situation des bandes ISM n'est pas la même selon les pays. Seule la bande des 2,4 GHz est libérée dans le monde entier. Exemples d'utilisations : Bluetooth, WLAN, liaisons domestiques et télécommandes. Les émetteurs en bande ISM doivent être estampillés "CE" pour pouvoir être utilisés en Europe. En France, la bande ISM principalement utilisée est la bande S (de 2,4 GHz à 2,4835 GHz), dans laquelle on trouve notamment des réseaux WLAN et le Bluetooth. Il y a aussi la bande "433 MHz" pour les liaisons domestiques bas débit (télécommandes de voiture ou de portails, thermomètres d'extérieurs, etc.), et la bande [5,150 GHz - 5,725 GHz].

JTRS *Joint Tactical Radio System*. Cf. §I.2.5.1.

LAN *Local Area Network* (réseau local).

LNA *Low Noise Amplifier* (amplificateur faible bruit). Cf. annexe B §B.3.2.

LSB *Least Significant Bit* (bit de poids faible). En représentation binaire conventionnelle, le LSB est le bit le plus à droite d'un nombre binaire. Lors d'une opération de numérisation, le LSB correspond au pas de discrétisation (plus petite variation de tension que peut rendre le signal discrétisé).

LTE *Long Term Evolution*. LTE est un projet de réseau mobile de 3,9G du 3GPP.

LUT (FPGA) *Look-Up Table* (table de correspondance). Cf. §II.3.1.6 et annexe B §B.9.3.

MAC *Media Access Control* (contrôle d'accès au support). La couche MAC est la sous-couche inférieure de la couche de liaison de données du modèle OSI. Elle se situe juste au dessus de la couche physique (PHY).

MAQ Modulation d'amplitude sur deux porteuses en quadrature. Une MAQ peut être à M états, M étant en général une puissance de deux.

MBITR *Multiband Inter/Intra Team Radio.*

MIMO *Multiple Input Multiple Output* (entrées multiples, sorties multiples). Cf. note de bas de page "4" (page 12).

MMIC *Monolithic Microwave Integrated Circuit* (circuit intégré monolithique hyperfréquence).

MS (GSM) *Mobile Station* (station mobile).

MSB *Most Significant Bit* (bit de poids fort). En représentation binaire conventionnelle, le LSB est le bit le plus à gauche d'un nombre binaire.

MSK *Minimum-Shift Keying* (modulation à déplacement de fréquence minimum). MSK est un type de modulation numérique par déplacement de fréquence à phase continue.

OBSAI *Open Base Station Architecture Initiative*. Cf. §I.2.5.3.

OFDM *Orthogonal Frequency Division Multiplexing* (multiplexage par répartition en fréquences sur des porteuses orthogonales). L'OFDM est un procédé de codage de signaux numériques par répartition de multiples sous-porteuses orthogonales entre elles.

OFDMA *Orthogonal Frequency-Division Multiple Access*. L'OFDMA est une version multiutilisateur de l'OFDM où chaque sous-porteuse est exclusivement assignée à un seul utilisateur.

OL Oscillateur Local.

OMAP *Open Multimedia Application Platform*. OMAP est un processeur ARM embarqué à très faible consommation fabriqué par Texas Instruments.

OMG *Object Management Group*. Association américaine dont l'objectif est de standardiser et promouvoir le modèle objet.

OSSIE *Open Source SCA Implementation – Embedded*. [ossie]

OSI *Open Systems Interconnection* (interconnexion de systèmes ouverts). OSI est un modèle de communications entre ordinateurs de l'Organisation internationale de normalisation (ISO).

PARI (DECT) *Primary Access Rights Identity* (identité de droits d'accès primaire), information d'identité transmise par *broadcast* sur le canal N_T. Cf. annexe C §C.3.4.

PARK (DECT) *Portable Access Rights Keys*. Cf. §IV.3.1.2 et annexe C §C.4.

PGA *Programmable Gain Amplifier* (amplificateur à gain programmable).

PHY Couche physique (niveau 1 du modèle OSI). Parfois notée PHL (*PHysical Layer*).

PLL *Phase-Locked Loop* (boucle à verrouillage de phase). La PLL est un circuit électronique effectuant un asservissement de la phase instantanée du signal de sortie sur la phase instantanée du signal d'entrée, ou bien de la fréquence de sortie sur un multiple de la fréquence d'entrée.

PP *Portable Part* (portable DECT), matériel mobile situé entre l'utilisateur et l'interface air DECT. Cf. note de bas de page "44" (page 94).

QPSK *Quadrature Phase Shift Keying* (modulation par déplacement de phase en quadrature). QPSK est basé sur le même principe que BPSK mais avec quatre états (symboles sur deux bits, phases multiples de $\pi/2$).

RF Radio Fréquence. Désigne le spectre radiofréquence des ondes radioélectriques.

RFP *Radio Fixed Part* (station de base radio DECT), sous-ensemble d'un FP composé d'équipements de terminaison radio et d'un seul aérien, et conversant avec un ou plusieurs PP via l'interface air. Cf. note de bas de page "44" (page 94).

RFPI (DECT) *Radio Fixed Part Identity* (identifiant du RFP). Cf. annexe C §C.3.4.

RFI *Request For Information* (demande d'informations). Un RFI a pour objectif d'évaluer la faisabilité de projets sur un plan technique et financier.

RMS *Root Mean Square* (moyenne quadratique), valeur efficace d'un signal périodique ou d'un signal aléatoire ergodique.

RNIS Réseau Numérique à Intégration de Services.

RTCP Réseau Téléphonique Commuté Public

RTS/CTS (Wi-Fi) *Request to Send / Clear to Send* (demande d'envoi / prêt à envoyer).

SARI (DECT) *Secondary Access Rights Identity* (identité de droits d'accès secondaire). Cf. annexe C §C.4.

SCA *Software Communications Architecture* (architecture logicielle de communications). Cf. §I.4.2.2.

SD *Secure Digital*. Une carte SD est une carte mémoire amovible de stockage de données numériques.

SDR *Software-Defined Radio* (radio logicielle restreinte). La SDR est souvent confondue avec la SR (Software Radio, radio logicielle) dans la littérature, même spécialisée.

SFDR (CAN) *Spurious Free Dynamic Range* (dynamique de codage). La SFDR représente la différence (en dB) entre la composante fondamentale et la composante harmonique de plus forte puissance d'un signal, ce qui au niveau d'un CAN correspond à la différence (en dB) entre la valeur efficace de la raie fondamentale et l'amplitude de la plus forte raie parasite (harmoniques comprises).

SFH *Slow Frequency Hopping* (saut de fréquence lent). Cf. §III.4.3.4.

SIM (GSM) *Subscriber Identity Module* (module d'identification d'abonné). Cf. §III.4.2.

SIMD *Single Instruction Multiple Data* (instruction unique à données multiples). Le SIMD est un mode de fonctionnement des ordinateurs où une même instruction est appliquée en parallèle à plusieurs données.

SIP *Session Initiation Protocol* (protocole d'initialisation de session). SIP est un protocole standard ouvert utilisé dans les télécommunications multimédia.

SNR *Signal-to-Noise Ratio* (rapport signal à bruit).

SPI *Serial Peripheral Interface* (interface série pour périphériques). SPI est un bus de donnée série synchrone opérant en full duplex.

SSB *Single-SideBand modulation* (modulation à bande latérale unique - BLU). La SSB est une modulation d'amplitude dans laquelle on a supprimé la porteuse et l'une des bandes latérales. On utilise donc soit la Bande Latérale Unique Supérieure (B.L.U.S., ou en anglais USB – *Upper SideBand*), soit la Bande Latérale Unique Inférieure (B.L.U.I., ou en anglais LSB – *Lower SideBand*).

SUPELEC École supérieure d'électricité.

TARI (DECT) *Tertiary Access Rights Identity* (identité de droits d'accès tertiaire). Cf. annexe C §C.4.

TDD *Time-Division Duplex* (duplex par séparation temporelle). Le TDD est une technique permettant à un canal de télécommunication utilisant une même ressource de transmission de séparer dans le temps l'émission et la réception.

TDMA *Time Division Multiple Access* (accès multiple à répartition dans le temps). Le TDMA est un mode de multiplexage temporel permettant de transmettre plusieurs signaux sur un même canal physique.

UHF Ultra haute fréquence. L'UHF désigne les ondes radio dont la fréquence est comprise entre 300 MHz et 3 GHz.

UML *Unified Modeling Language* (langage de modélisation unifié). UML est un langage de modélisation graphique à base de pictogrammes.

UMTS *Universal Mobile Telecommunications System* (système de télécommunication mobile universel). L'UMTS constitue l'implémentation européenne des spécifications IMT-2000 de l'UIT pour les systèmes radio cellulaires de troisième génération (3G).

USRP *Universal Software Radio Peripheral* (Périphérique universel de radio logicielle). Cette dénomination correspond à la fois à une famille d'équipements et à la première version commercialisée (USRP1). Cf. §II.3.

VCO *Voltage-Controlled Oscillator* (oscillateur contrôlé en tension).

VCXO *Voltage-Controlled Crystal Oscillator* (oscillateur à quartz contrôlé en tension).

VHDL *VHSIC Hardware Description Language* (langage de description matérielle de VHSIC). Cf. annexe B §B.9.2.

VHF *Very High Frequency*, ou Très haute fréquence. La VHF désigne les ondes radio dont la fréquence est comprise entre 30 MHz et 300 MHz.

VHSIC *Very High Speed Integrated Circuit* (circuit intégré très rapide).

W-CDMA *Wideband Code Division Multiple Access* (multiplexage par code large bande). Le W-CDMA est une évolution de la technique CDMA. Elle est utilisée pour la téléphonie mobile de troisième génération, dont notamment l'UMTS.

WHDI *Wireless Home Digital Interface*, norme de transmission sans fil de la vidéo Full HD.

WiMAX *Worldwide Interoperability for Microwave Access* (interopérabilité mondiale pour l'accès par micro-ondes). WiMAX désigne un mode de transmission et d'accès à Internet en haut débit, portant sur une zone géographique étendue, et comprend la famille de normes IEEE 802.16.

WLAN *Wireless LAN* (réseau local sans fil). WLAN désigne un réseau informatique ou numérisé qui connecte différents postes ou systèmes entre eux par ondes radio. La norme la plus utilisée actuellement pour les réseaux sans fil est la norme IEEE 802.11, mieux connue sous le nom de Wi-Fi.

WMAN *Wireless Metropolitan Area Network* (réseau métropolitain sans fil). Plus connu sous le nom de boucle locale radio, un WMAN est un réseau métropolitain sans fil basé sur le standard 802.16, le plus répandu étant le WiMAX.

WPAN *Wireless Personal Area Network* (réseau personnel sans fil). Le WPAN est un réseau sans fil de faible portée (quelques mètres). Les exemples les plus connus sont le Bluetooth et ZigBee.

XML *eXtensible Markup Language* (langage de balisage extensible). XML est un langage informatique de balisage générique.

Glossaire

802.11 Cf. §III.3.

802.15.4 Protocole de communication IEEE destiné aux réseaux LR WPAN (*Low Rate Wireless Personal Area Network*). Cf. §III.2.1.

802.16 Norme de transmission sans fil et groupe de travail de l'IEEE responsable du développement du standard WiMAX.

Barker (Code ou séquence de). Séquence de N valeurs de +1 et de -1 possédant des propriétés particulières d'autocorrélation et utilisée dans les techniques d'étalement de spectre.

Bitstream Le terme *bitstream* est fréquemment utilisé pour décrire les données de configuration à charger dans un FPGA.

Chip En communications numériques, un chip est une impulsion (généralement rectangulaire) d'un code DSSS, tel qu'un code pseudo aléatoire utilisé dans les techniques d'accès de canal CDMA à séquence directe.

Chirp Signal pseudopériodique modulé en fréquence et également modulé en amplitude par une enveloppe dont les variations sont lentes par rapport aux oscillations de la phase.

Circulateur Dispositif à trois ports permettant au signal RF de ne circuler que dans un seul sens : un signal entrant dans le port 1 est envoyé au port 2 et isolé du port 3, tandis qu'un signal injecté au port 2 est transmis au port 3 et isolé du port 1, etc.

Codec Procédé de compression et/ou de décompression d'un signal numérique.

Constellation (Diagramme de). Représentation bidimensionnelle (plan complexe I/Q) d'un signal modulé par une modulation numérique.

Cospas-Sarsat Système à composante satellitaire fournissant des données de localisation et alertes de détresse au profit des autorités de recherche et sauvetage (SAR).

Cygwin Collection de logiciels « libres » permettant à différentes versions de Windows de Microsoft d'émuler un système Unix.

dB Décibel. Le dB correspond au dixième de bel, unité de mesure logarithmique du rapport entre deux puissances.

dBc *Decibels relative to the carrier*. Le dBc représente le rapport de puissance entre un signal et une porteuse.

dBi *Decibels relative to an isotropic antenna*. Le dBi représente le gain d'une antenne en prenant pour référence une antenne isotrope (antenne fictive rayonnant uniformément dans toutes les directions).

Décimation En traitement du signal, la décimation est synonyme de sous-échantillonnage : on ne garde qu'un certain nombre d'échantillons par rapport au signal original. Cf. annexe B §B.7.

Dynamique d'entrée (CAN). La dynamique d'entrée d'un CAN est la différence entre le niveau de puissance maximal pour lequel un CAN ne saturera pas (niveau dit de « pleine échelle ») et le niveau de bruit de quantification. Il s'agit donc d'un rapport signal à bruit qui dans le cas d'un CAN parfait a pour valeur `6,02.n + 1,76`; où n est la résolution du CAN (nombre de bits effectifs).

Duplexeur Dispositif électronique permettant l'utilisation d'une même antenne pour l'émission et la réception du signal.

éch/s Contraction de "échantillons par seconde", unité de mesure de taux d'échantillonnage.

Facteur de bruit Différence entre les rapports signal sur bruit (exprimés dB) en sortie et en entrée d'un composant électronique.

Firmware Micrologiciel intégré dans un composant matériel.

Fond de panier (*Backplane* en anglais). Ensemble souvent placé au fond d'un équipement électronique et constitué de connecteurs reliés par un câblage interne dans lesquels on peut enficher des cartes électroniques. [wiki3]

Forme d'onde Dans une radio logicielle, une forme d'onde est l'ensemble des transformations algorithmiques appliquées à l'information pour la convertir en signal radio. Une forme d'onde est entièrement logicielle et définit les caractéristiques du signal RF, dont la fréquence, la modulation et le format.

Glue logique Ensemble personnalisé d'éléments logiques utilisés pour interfacer un certain nombre de circuits intégrés prêts à l'emploi.

Handover Ensemble des opérations permettant à une station mobile de changer de cellule sans interruption de service.

Idle Mode d'activité restreinte (économie d'énergie, repos,…).

Interpolation En radio logicielle, l'interpolation consiste à effectuer un suréchantillonnage pour rajouter de nouveaux échantillons entre deux points de mesure existant. Il existe diverses méthodes d'interpolation : linéaire, polynomiale, etc. Cf. annexe B §B.6.

Nyquist (critère de). Le critère de Nyquist s'énonce comme suit : « Tout signal peut être représenté sous la forme d'échantillons discrets si la fréquence d'échantillonnage est d'au moins deux fois la bande passante du signal. ». Ce qui signifie que pour une fréquence d'échantillonnage donnée, il n'existe aucune ambiguïté sur le signal d'entrée dans une bande de fréquences égale à la moitié de la fréquence d'échantillonnage.

Peak hold Valeur maximale mesurée.

PCI Express (Abrégé PCI-E ou PCIe). Standard spécifiant un bus local série et un connecteur de cartes d'extension sur la carte mère d'un ordinateur, destiné à remplacer tous les connecteurs PCI, PCI-X et AGP. Cf. §II.5.2.

Prédistorsion Méthode de linéarisation d'un amplificateur basée sur l'ajout de systèmes accomplissant une compensation en gain et/ou en phase.

Reed-Solomon (Code de). Code correcteur basé sur les corps de Galois et le suréchantillonnage.

Repliement spectral (*aliasing*) Si l'on ne respecte pas le critère de Nyquist, les fréquences supérieures à la moitié de la fréquence d'échantillonnage introduisent un recouvrement spectral également appelé crénelage ou repliement. On pourrait croire que si l'on respecte la règle du double de la fréquence maximale du signal il n'y a pas de risque de repliement. C'est sans compter sur la présence éventuelle d'un bruit haute fréquence sur le signal à échantillonner, qui lors de l'échantillonnage, va se superposer au signal utile. Une solution palliative repose sur l'utilisation d'un filtre antirepliement (fréquence de coupure égale à la moitié de la fréquence d'échantillonnage) dont le rôle est d'éliminer, avant échantillonnage, les fréquences supérieures à la fréquence maximum utile.

Slew rate (ou vitesse de balayage). Le *slew rate* représente la vitesse de variation maximale que peut reproduire un amplificateur.

Socket Modèle permettant la communication interprocessus afin de permettre à divers processus de communiquer aussi bien sur une même machine qu'à travers un réseau.

Softcore (Processeur). Implémentation de CPU disponible sous la forme de description de haut niveau en HDL.

Symbole État physique élémentaire définissant une information quantifiable sur un ou plusieurs bits.

Tap Cf. note de bas de page "25" (page 46).

Turbo Code Code correcteur basé sur l'association de deux codeurs introduisant de la redondance dans un message afin de le rendre moins sensible aux bruits et perturbations subies lors d'une transmission.

Viterbi	(Algorithme de). Algorithme permettant de corriger, dans une certaine mesure, les erreurs survenues lors d'une transmission à travers un canal bruité. Il s'appuie sur la distance de Hamming afin de faire ressortir la plus faible métrique entre les différentes valeurs probables d'une séquence d'états.
Wi-Fi (802.11)	Ensemble de protocoles de communication sans fil défini par les normes du groupe IEEE 802.11. Cf. §III.3.
Wireshark	Logiciel « libre » multiplateforme d'analyse de protocole.
ZigBee	Cf. §III.2.2.

Table des matières

Introduction

Jusque dans les années 80 les équipements de transmission radiofréquence concentraient l'essentiel de leur technologie dans l'association de composants analogiques peu flexibles et généralement dédiés à la mise en œuvre et l'exploitation d'une forme d'onde spécifique dans une bande de fréquences prédéterminée. Modifier le comportement d'un matériel se révélait impossible à moins de devoir remplacer certains composants. Ce paradigme qui a prévalu pendant près d'un siècle n'était plus viable face à l'explosion du nombre de normes de radiocommunication. Les progrès réalisés en informatique et en électronique numérique ont permis de remplacer une partie de la technologie analogique des systèmes de transmission radiofréquence par une composante numérique et logicielle, et donc une capacité à la configuration et la synthèse de différentes formes d'onde. C'est dans ce contexte qu'est apparu le concept de radio logicielle.

La radio logicielle exploite la puissance de traitement des technologies informatiques modernes pour émuler le comportement d'un circuit radio. Une radio logicielle est un système de radiocommunication configurable utilisant des techniques de traitement logiciel sur des signaux radio. Une radio logicielle multistandard doit pouvoir traiter plusieurs normes de communications radio ayant des spécifications différentes, à savoir des canaux de communications à bande étroite ou large, opérant à des fréquences pouvant atteindre plusieurs gigahertz et à des niveaux d'émission et de réception variés. Le traitement numérique doit être adapté à la norme sélectionnée et répondre aux exigences en termes de modulation et de technique d'accès.

L'émergence des radios logicielles au sein des équipements de radiocommunication apporte de la souplesse de fonctionnement, une grande évolutivité et permet de réaliser des économies d'échelle. Mais la migration logicielle des fonctions de traitement du signal radio a aussi des inconvénients. En effet, de nombreuses normes de radiocommunication sont soumises à licence et/ou restrictions d'emploi. Les équipements conventionnels sont sensés respecter ces contraintes de fonctionnement. Depuis quelques années des radios

logicielles « libres » apparaissent et sont commercialisés en dehors de tout cadre réglementaire. Ces équipements offrent la possibilité au plus grand nombre d'étudier le spectre radio, et notamment les protocoles de transmission radiofréquence. Divers projets universitaires emploient ces radios logicielles à des fins d'étude et de recherche dans des bandes de fréquences autorisées (exemple : bandes ISM). Mais rien n'empêche l'utilisation de ces équipements sur d'autres parties du spectre, pour par exemple étudier des réseaux sans fil (GSM, GPS, DECT, etc.).

Ce mémoire consiste dans un premier temps à procéder à une étude générale de la technologie radio logicielle (constituants, fonctions réalisées, différentes techniques), puis à dresser un panorama des radios logicielles « libres » plus ou moins disponibles (aspects matériels et logiciels), en se concentrant principalement sur les architectures matérielles USRP (versions 1 et 2), associées au projet logiciel GNU Radio, disponibles pour l'étude. Ensuite quelques protocoles de radiocommunication sont étudiés dans le cadre d’une mise en œuvre radio logicielle. Enfin sont présentées quelques réalisations pratiques.

Chapitre I

La radio logicielle

I.1 Liminaire

I.1.1 Rôle d'un équipement radio

Un récepteur radio se compose de plusieurs parties : une antenne qui reçoit le signal radiofréquence, un sous-système radiofréquence/fréquence intermédiaire (RF/FI) qui convertit et filtre le signal dans la bande spectrale désirée, et un démodulateur/décodeur qui convertit ce signal sous un format exploitable. Le résultat obtenu est transmis à une application et enfin à l'utilisateur. Un émetteur radio effectue le processus inverse, en prenant les données des utilisateurs, les codant, les modulant, les convertissant en FI puis en RF, amplifiant le signal RF et le transmettant à une antenne.

I.1.2 Un besoin issu de la diversité des normes de transmission sans fil

Au cours du siècle dernier les progrès réalisés sur les équipements radio se focalisaient sur l'amélioration du matériel : meilleurs composants, circuits haute densité, qualité de fabrication, etc. Chaque équipement était conçu pour un usage particulier, la bande de fréquences et la forme d'onde étant figées à travers une architecture spécifique. Modifier le comportement d'un équipement se révélait impossible à moins de remplacer certains composants. Il existe de nombreux standards et normes de transmission radiofréquence, utilisant des fréquences, largeurs de canaux et modulations différentes. Citons par exemple le GSM et le WCDMA pour les communications cellulaires, l'HiperLAN et la série des 802.11 (dont le futur standard 802.11vht) pour les réseaux sans fil, le WHDI pour la télévision haute définition, et bien d'autres encore. Le tableau I présente les caractéristiques principales de quelques formes d'onde et standards de transmission sans fil.

Jusqu'à récemment la gestion de multiples standards de radiocommunication par un terminal unique impliquait que ce dernier devait embarquer des composants dédiés à chacun de ces standards, ce qui s'avérait coûteux et grevait le poids du système complet. La radio logicielle a été créée en réponse à cette nécessité de simplification matérielle et de flexibilité des systèmes de radiocommunication multiprotocole.

Tableau I : Caractéristiques principales de quelques normes de communication sans fil

Standard	**802.11g**	**802.15.1**	**802.15.4**	**802.16e-2005**	**GSM 900**	**UMTS/FDD**
Nom	**Wifi**	**Bluetooth**	**ZigBee**	**Mobile WiMax**		
Type	WLAN	WPAN	WPAN	WMAN	WMAN	WMAN
Bande(s) de fréquence (MHz)	2400 à 2483.5	2402 à 2480	0.868 à 0,8686 0,902 à 0,928 2,4 à 2,483.5	2 à 6	895 à 915 montant 935 à 960 descendant	1920 à 1980 montant 2110 à 2170 descendant
Nb. de canaux	14	79	1 – 10 – 16	variable	2*124	2*12
Largeur canal (MHz)	22	1	0.6 à 5	5 à 10	0.2	5
Technique d'accès	OFDM	FHSS	DSSS PSSS	OFDMA	TDMA	W-CDMA
Modulation	DBPSK DQPSK MAQ-16 MAQ-64	GFSK DQPSK π/4-DQPSK 8DPSK	OQPSK BPSK ASK	QPSK MAQ16 ou 64	GMSK	QPSK-CDMA
Débit (Mbit/s)	1 à 54	1 à 24	40 (868 MHz) 20 (915 MHz) 250 (2.4 GHz)	Jusqu'à 30	0.01	0.144 à 2

I.1.3 Ce que la radio logicielle promet

Les progrès technologiques en traitement numérique du signal ont ouvert la voie à une nouvelle approche d'implémentation de plateformes de communication sans fil où la majeure partie du traitement du signal est réalisée au niveau logiciel plutôt qu'au niveau matériel. Cette approche d'équipement radio à composante logicielle et configurable est regroupée sous le vocable de radio logicielle. La radio logicielle apporte un haut niveau de souplesse dont notamment la possibilité d'implémenter différents algorithmes pour le traitement numérique du signal. Le passage d'un traitement analogique à un traitement numérique du signal apporte d'indéniables avantages mais aussi quelques inconvénients. Le tableau suivant reprend les principales caractéristiques de ces traitements.

Tableau II : Traitement numérique vs traitement analogique

	Traitement numérique	**Traitement analogique**
Largeur de bande utilisable	Limitée par l'échantillonnage	Peut travailler à très haute fréquence
Rapport signal à bruit Précision	Fixes et connus à l'avance	Dépendent de la qualité des composants
Configuration	Changement de logiciel	Principalement matérielle, calibration nécessaire
Sources de bruit	Bruit de quantification	Bruit électromagnétique, température, humidité, vieillissement

Pour pouvoir gérer la plupart des standards de transmission radiofréquence, une radio logicielle doit être capable d'opérer dans un spectre radiofréquence le plus large possible (fréquences allant de quelques centaines de kilohertz à plusieurs gigahertz). Un terminal radio logiciel multistandard doit pouvoir traiter plusieurs normes de communications radio ayant des spécifications différentes, à savoir des canaux de communications à bande étroite ou large (200 kHz pour le GSM, 20 MHz pour le Wi-Fi, ...), centrés sur des fréquences porteuses pouvant atteindre 6 GHz voire plus, et de dynamique pouvant atteindre plus de 100 dB. Le traitement numérique doit être adapté à la norme sélectionnée et répondre aux exigences en termes de modulation et de technique d'accès. Nous verrons que la réalisation d'un récepteur radio logiciel satisfaisant toutes ces contraintes n'est pas encore possible à cause de nombreuses limitations technologiques. Nous constaterons que les conceptions actuelles sont basées sur une architecture intermédiaire appelée radio logicielle restreinte ou SDR (*Software Defined Radio*).

I.1.4 Bref historique

Issue de la recherche militaire américaine à la fin des années 70 sur les radios multimodes opérant en bandes VHF et UHF (programme ICNIA de l'*US Air Force* en 1978 [wiley]), la radio logicielle aboutit au début des années 90 à la famille de projets SPEAKeasy Phase I et Phase II, première implémentation de radio logicielle émulant des radios tactiques. Elle rejoint en 1991, par l'intermédiaire du chercheur Joseph MITOLA III, la communauté scientifique dans le cadre des applications de télécommunications civiles. En 1995 un RFI (*Request For Information*) sur la radio logicielle pour la téléphonie mobile marquera le point de départ d'une activité accrue dans le domaine. En 1996 est apparu le *Modular Multifunctional Information Transfer System Forum* (MMITS Forum), renommé en 1998 en *Software Defined Radio Forum* (SDR Forum), renommé en 2009 en *Wireless Innovation Forum*, corporation animée par une centaine de contributeurs internationaux dont l'objectif est de promouvoir et de développer la technologie radio logicielle [sdrforum].

I.2 Présentation

I.2.1 Définitions

Une radio logicielle, en anglais *Software Radio*, est un système de radiocommunication configurable utilisant des techniques de traitement logiciel sur des signaux radiofréquences. Une radio logicielle utilise des circuits numériques

programmables pour effectuer du traitement de signal. Sa flexibilité lui permet de s'adapter à un large spectre de réseaux, protocoles et techniques de radiocommunication, et de répondre au besoin croissant de performance et d'interopérabilité entre systèmes hétérogènes. L'objectif ultime de la radio logicielle consiste en une dématérialisation complète de l'interface radio. Elle fait partie de la tendance globale des circuits électroniques à migrer du "tout transistor" vers le "tout logiciel". L'évolution ultime de la radio logicielle est la radio intelligente (*Cognitive Radio*, [wiki1]). Une radio intelligente est une radio logicielle dans laquelle les éléments de communication sont conscients de leur environnement (localisation, etc.) et de leur état interne, peuvent prendre des décisions en fonction de leur comportement et d'objectifs prédéfinis, et sont également capables d'apprentissage.

Une radio logicielle met en œuvre deux notions fondamentales : la plate-forme et la forme d'onde. Une plate-forme est l'ensemble des matériels radio et des systèmes de traitement qui hébergent une ou plusieurs formes d'onde. Dans une radio logicielle, une forme d'onde est l'ensemble des transformations algorithmiques appliquées à l'information pour la convertir en signal radio. Une forme d'onde est entièrement logicielle et définit les caractéristiques du signal RF, dont la fréquence, la modulation et le format. Les radios logicielles permettent l'utilisation de multiples formes d'ondes, éventuellement dans différentes bandes spectrales, pour différents usages, voire même de façon simultanée. Les forces armées américaines se sont notamment intéressées à la radio logicielle dès ses prémisses, et tentent de construire un poste de radio tactique multistandard large bande [jtrs3]. Puisque les formes d'onde sont entièrement logicielles, elles peuvent facilement être implémentées sur une plate-forme existante grâce à une mise à jour, mais à condition qu'elles soient portables sur la plate-forme considérée, d'où l'importance des recherches actuelles dans le développement de standards ouverts. Dans une radio logicielle les propriétés de la fréquence porteuse, de la bande passante du signal, de modulation et d'accès au réseau sont définies par logiciel. Les radios logicielles modernes mettent également en œuvre des fonctions cryptographiques, de correction d'erreurs et de codage de source de la voix, vidéo ou des données.

I.2.2 Les différents types de radio logicielle

Entre une radio toute simple, c'est-à-dire une radio sans composante logicielle, et une radio intelligente il existe une panoplie de classes intermédiaires. Le tableau suivant résume les propriétés des différentes classes de radio logicielle.

Tableau III : Fonctionnalités des différents types de radio logicielle[1]

Propriété	Radio logicielle « capable » (*software capable radio*)	Radio programmable par logiciel (*software programmable radio*)	Radio définie par logiciel (*software defined radio*)	Radio consciente (*aware radio*)	Radio adaptative (*adaptive radio*)	Radio intelligente (*cognitive* ou *intelligent radio*)
Saut de fréquence	X	X	X	X	X	X
Établissement automatique de lien (choix du canal)	X	X	X	X	X	X
Capacité de mise en réseau		X	X	X	X	X
Interopérabilité, formes d'ondes multiples		X	X	X	X	X
Évolutivité fonctionnelle		X	X	X	X	X
Contrôle logiciel des fonctionnalités de traitement du signal, cryptographie et de mise en réseau.			X	X	X	X
Mesure de la qualité de service et recueil d'informations sur l'état des canaux				X	X	X
Modification des paramètres radio en fonction des informations captées					X	X
Apprentissage de l'environnement						X
Expérimentation autonome de différents réglages						X

Une radio logicielle est composée de deux sous-systèmes : un sous-système matériel et un sous-système logiciel. La répartition des opérations réalisées dans les sous-systèmes matériels et logiciels est représentée dans le schéma suivant.

[1] Adapté de [fette].

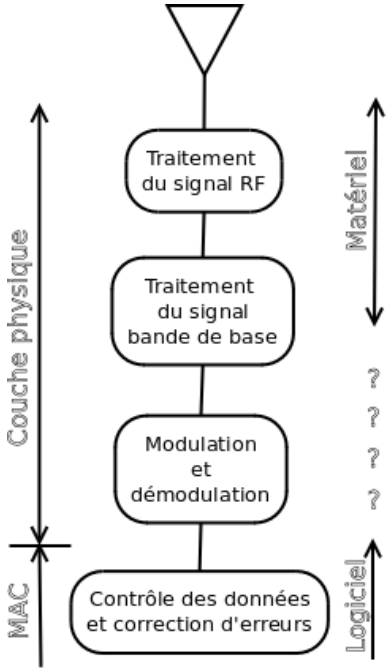

Figure 1 : Répartition matériel/logiciel dans une radio logicielle

Il est possible d'effectuer une catégorisation du type de radio en fonction de l'endroit où l'on fixe la limite entre le sous-système matériel et le sous-système logiciel, et incidemment en fonction de son degré de reconfiguration. Le tableau suivant résume ces différentes catégories.

Tableau IV : Classification des radios logicielles selon leur niveau de configuration[2,3]

Catégorie	Dénomination	Degré de reconfiguration
0	Radio matérielle	Radio qui ne peut pas être modifiée par logiciel ; reconfiguration par échange de composants.
I	Radio contrôlée par logiciel	Reconfiguration logicielle limitée à un jeu prédéfini de paramètres (niveaux de puissance, interconnexions,...).
II	Radio définie par logiciel	Contrôle logiciel et reconfiguration des formes d'ondes, fréquence, bande passante, (dé)modulation, détection du signal, paramètre de sécurité, etc.
III	Radio logicielle idéale	Conversion analogique au niveau de l'antenne, du haut-parleur et du microphone ; tout le reste est logiciel.
IV	Radio logicielle ultime	Comprend tout type de trafic et d'informations de contrôle, et supporte la plupart des applications et circuits d'antenne.

[2] Adapté de [seskar].

[3] Selon [massiani] dans une architecture radio logicielle, le terme "configuration" recouvre plusieurs aspects. Du point de vue système il concerne les processeurs de traitement du signal. La gestion d'architectures hétérogènes (communications interprocesseur, exécution de tâches en parallèle) relève de la configuration fonctionnelle. Les fonctionnalités et interconnexions des unités de traitement arithmétique sont de niveau « opérateur logique ». La configuration des éléments logiques d'un composant et de leur interconnexion constitue le dernier aspect.

I.2.3 Objectifs de réalisation d'une radio logicielle

On assiste actuellement à une profusion de standards de communications sans fil (Wi-Fi, GSM, UMTS, WiMAX, etc.) dont les composantes radio sont incompatibles. L'un des objectifs de réalisation d'une radio logicielle est de remplacer des contraintes matérielles en contraintes logicielles, plus faciles à résoudre et moins onéreuses. Il faut donc implémenter en logiciel tout ce qui peut l'être, et gagner en souplesse de configuration et de contrôle sur la partie matérielle restante. La conversion analogique/numérique est ainsi positionnée au plus proche de l'antenne, tant à l'émission qu'à la réception, pour effectuer un maximum d'opérations dans le domaine numérique. En synthèse, une radio logicielle idéale est un émetteur/récepteur multibande et multimode modifiable par logiciel, de la tête RF jusqu'aux protocoles de communication.

I.2.4 Avantages de la radio logicielle

La radio logicielle est une évolution logique des systèmes de radiocommunication car elle apporte de nombreux avantages pour l'ensemble des acteurs du domaine. En effet, comparée à une architecture "tout matériel", la radio logicielle promet des équipements multistandards et multiservices.

La radio logicielle constitue tout d'abord un avantage pour les fabricants et équipementiers, grâce à la disparition de certains composants analogiques coûteux et encombrants (filtres, oscillateurs, etc.), ainsi que la possibilité d'implémenter une famille de produits " radio " sur une unique plateforme matérielle et d'utiliser un même code logiciel dans différents équipements. La mise à jour logicielle et la maintenance du *firmware* de l'équipement (dont d'éventuels modules de sécurité) peuvent également s'en trouver facilitées. Ensuite, c'est une aubaine pour les fournisseurs de services radio, grâce à l'ajout facilité de nouvelles fonctionnalités ou amélioration des performances d'une infrastructure opérationnelle, une adaptation dynamique aux caractéristiques du canal de propagation, une mobilité totale grâce à un fonctionnement multistandard, une portabilité des formes d'onde, et le téléchargement et mise à jour logicielle à distance. Et enfin, la radio logicielle offre au plus grand nombre la capacité (légitime ou non) d'étudier divers protocoles et communications sans fil à l'aide d'équipements abordables techniquement et financièrement.

I.2.5 La radio logicielle et ses différents usages

I.2.5.1 Les radios logicielles tactiques

Les militaires ont des besoins évidents de radios logicielles. Une radio logicielle peut changer son codage, sa modulation et/ou son chiffrement en fonction du besoin, ce qui lui donne un avantage important sur le champ de bataille. Les radios logicielles sont considérées comme un élément clé de la communication radio dans le domaine tactique de la « guerre réseau centrée » (NCW - *Network Centric Warfare*). Le concept de radio logicielle offre une interopérabilité lors d'opérations interarmées et interalliées où les unités combattantes peuvent utiliser différents types de systèmes de communication sans fil implémentant ou non de nouvelles technologies de transmission dans les bandes HF à UHF. Par ailleurs, les radios logicielles permettent des transmissions haut débit à l'aide de formes d'onde spécifiques (WNW – *Wideband Networking Waveform*) [north].

La radio logicielle est un élément fondamental de la numérisation de l'espace de bataille. En France, le plan d'étude amont NCT (Nœud de Communication Tactique) s'inscrit dans le cadre d'études préparatoires à de futurs programmes de développement de radios logicielles tactiques au profit des armées (intégration de nouvelles formes d'onde à haut débit dans les équipements de radiocommunications militaires). Au niveau européen le projet européen ESSOR (*European Secure Software Radio Programme*) a pour objectif d'améliorer l'interopérabilité entre les forces européennes en établissant un référentiel normatif de radios logicielles sécurisées. ESSOR se base sur le modèle d'architecture logicielle SCA (cf. §I.4.2.2) et a défini une forme d'onde à haut débit sécurisée appelée ESSOR HDR.

Aux États-Unis le principal programme de radio logicielle militaire est actuellement le JTRS (*Joint Tactical Radio System*) [jpeojtrs]. Le programme JTRS a été lancé en 1997 à la suite des succès du précédent programme *Speakeasy* (début des années 1990) qui utilisait la technologie radio logicielle pour supporter les communications entre les services de l'armée américaine. Le but du JTRS, qui s'appuie également sur le standard SCA, est de développer une famille de radios tactiques capables d'interagir avec d'autres radios dans la bande de fréquences [2 MHz - 2,5 GHz], établir un pont de communication entre ces formes d'onde et leur propre forme d'onde, et créer des réseaux mobiles *ad hoc* ou MANET (*Mobile Ad-hoc NETworks*), réseaux sans fil capables de s'organiser sans infrastructure définie au préalable. JTRS est prévu pour fonctionner sur quatre bandes radio : 2 MHz à 30 MHz, 30 MHz à 512 MHz, 512 MHz à 1215 MHz et 1215 MHz à

2500 MHz. Au fil des ans, le programme JTRS est devenu cher. De nombreux retards dus aux objectifs ambitieux de fournir un maximum de fonctionnalités dès la version bêta ont imposé la restructuration du programme en 2005 pour se concentrer sur les besoins les plus urgents, notamment la Radio Mobile Terrestre (GMR – *Ground Mobile Radio*) en cours de certification [jtrs]. La GMR est destinée aux installations véhiculées, dont le HMMWV (*High Mobility Multi-purpose Wheeled Vehicle*) et les principaux chars de combat [jtrs2]. D'autres radios JTRS ciblant des implémentations plus petites que le GMR sont en développement : le JTRS *Airborne, Maritime Fixed Station* (AMF) pour la Marine et l'armée de l'Air, et le JTRS *Handled, Man-pack, Small Form Fit* (HMS) pour l'armée de Terre. Citons en outre le programme JTRS *Enhanced* MBITR, adaptation d'une radio logicielle existante, la MBITR, à l'architecture logicielle SCA [jtrs3].

Le système HOOK2, également américain, est un réseau sans fil fournissant des informations GPS, de messagerie bidirectionnelle et d'identification sur un lien sécurisé au profit des unités combattantes. La radio logicielle durcie AN/PRC-112G HOOK2 CSAR (*Combat Search-and-Rescue*), fabriquée par General Dynamics [csar] fonctionne dans trois bandes : 121,5 MHz à 123,1 MHz, 225 MHz à 320 MHz et 406 MHz Cospas-Sarsat. Elle prend en charge les modulations AM, MSK et BPSK et a une autonomie de quatre jours. Le récepteur GPS prend en charge douze canaux en parallèle pour réduire les effets des brouilleurs, et peut même identifier la direction des interférences. L'AN/PRC-112G peut notamment être modifiée à la demande pour supporter la modulation FM, le GPRS, des communications par satellite supplémentaires, et les formes d'onde LPE (*Low Probability of Exploitation*).

I.2.5.2 Guerre électronique et radar

D'autres applications, telles que les moyens passifs de guerre électronique (ESM – *Electronics Support Measures*) et le radar peuvent profiter de la technologie radio logicielle, en particulier des normes telles que SCA. Un dispositif d'attaque électronique (ECM *Jammer*), par exemple, utilise un récepteur pour identifier les types d'émission radio présents dans l'environnement, et un émetteur pour générer un signal d'interférence. Des radios logicielles peuvent être utilisées pour permettre au système ECM (*Electronic CounterMeasure*) de s'adapter rapidement à des types d'émission imprévus, ou tout simplement d'augmenter les capacités d'un équipement donné. La technologie des antennes intelligentes peut être utilisée pour localiser une émission hostile (principe de radiogoniométrie), diriger convenablement des interférences, ou annuler les interférences

d'autres brouilleurs. Les radars peuvent utiliser la technologie radio logicielle pour gérer leurs formes d'onde et ressources matérielles.

I.2.5.3 Radio mobile grand public

Dans le domaine de la radio mobile grand public, la technologie radio logicielle est un choix pertinent pour gérer les mises à jour, permettre la mise en œuvre d'une grande variété de fonctionnalités, et supporter de nouvelles technologies telles que le MIMO[4], tout en maintenant la compatibilité avec les normes existantes. On constate également l'intégration de radios logicielles dans les stations de base des réseaux de téléphonie cellulaire. Des normes telles que l'OBSAI (*Open Base Station Initiative Architecture*) et CPRI (*Common Public Radio Interface*) définissent pour les stations de base WiMAX ou 3GPP des interfaces entre les équipements radio et leurs systèmes de contrôle (équipement de contrôle de la radio, en anglais RCE – *Radio Controlling Equipment*), l'ensemble implémentant des fonctionnalités radios logicielles. Ces interfaces s'appuient sur des liaisons numériques à haute vitesse, généralement optiques [cpri]. Ce type d'architecture trouve notamment un écho favorable au sein des entreprises. En effet l'équipement radio doit généralement être situé au dernier étage ou sur le toit des bâtiments car c'est là que l'antenne est installée, mais le RCE peut très bien être situé à un étage inférieur, voire même au sous-sol.

I.2.5.4 Radio intelligente (*cognitive radio*)

J. Mitola définit la radio intelligente comme l'intégration du raisonnement à base de modèles avec les technologies de radio logicielle [mitola2]. La radio intelligente s'appuie sur le fondement de la radio logicielle, à savoir la représentation algorithmique et le traitement des signaux radio, pour obtenir des informations sur l'environnement proche afin d'améliorer ses performances radio. Pour ce faire, elle utilise des disciplines complémentaires, telles que les systèmes experts et les méthodes d'apprentissage.

La radio intelligente apporte de nouvelles capacités aux radios logicielles : gestion fine des ressources, des protocoles réseau, prestations de services et certification des téléchargements. Pour être intelligente, une radio doit d'abord être consciente de son état, à l'aide d'informations qui lui sont remontées par des capteurs. La possibilité de reconfigurer

[4] Les systèmes SISO (*Single Input Single Output*) exploitaient la diversité temporelle et/ou fréquentielle. Les systèmes MIMO *(Multiple Input Multiple Output*) exploitent en plus la diversité spatiale. La combinaison des différents trajets empruntés par les répliques d'un même signal améliore ainsi le système de transmission sans fil. On distingue les systèmes MISO *(Multiple Input Single Output*), SIMO (*Single Input Multiple Output*), selon qu'un réseau d'antennes est utilisé en émission ou en réception, et MIMO si l'on combine les deux.

un réseau de communication en fonction de son environnement est la clé de voûte de la radio intelligente. Les radios logicielles apportent de la flexibilité au niveau des blocs de communication utilisés alors que les radios intelligentes évaluent l'environnement d'exploitation afin de maximiser leurs performances par rapport à un (ou plusieurs) objectif(s) de communication.

I.2.5.5 NASA

Le système radio de télécommunications spatiales de la NASA (STRS - NASA's *Space Telecommunications Radio System*) est une radio logicielle destinée à remplacer d'anciens équipements radios propriétaires. Le groupe de travail STRS a collaboré avec l'OMG et le SWG (*Space Working Group*) du *Wireless Innovation Forum* pour élaborer un PIM (*Platform-Independent Model*) à base d'API (*Application Programming Interface*) pour supporter les équipements spatiaux spécifiques de la NASA ainsi que les fonctions temps réel POSIX 1003.13 [nasa].

I.2.5.6 Radioamateurisme

Des radioamateurs ont mis au point leur propre technologie radio logicielle au cours de ces dernières années. Une configuration typique utilise un récepteur à conversion directe basé sur la détection et l'échantillonnage de signaux en quadrature. Les performances du récepteur sont directement liées à la dynamique des convertisseurs analogique/numérique (CAN) utilisés. Les signaux radiofréquence sont transposés dans la bande de fréquences audio, puis échantillonnés par des CAN à hautes performances. Une première génération d'équipements utilisait une carte son de PC pour fournir des fonctionnalités de CAN. La dernière génération utilise des CAN embarqués plus performants, offrant une meilleure dynamique d'entrée et une plus grande résistance au bruit et aux interférences RF. Un PC performant effectue ensuite les opérations de traitement numérique du signal à l'aide d'un logiciel spécifique capable d'effectuer tout type de modulation/démodulation, filtrage, amélioration du signal, etc., ouvrant la voie à de multiples expérimentations.

I.2.5.7 Outils d'instrumentation

Afin de pouvoir suivre le rythme effréné de mise sur le marché de nouveaux systèmes de communication sans fil, certains fabricants de matériels de test ont intégré de la radio logicielle dans leurs matériels pour obtenir des instruments RF modulaires et polyvalents [ni2] [ni3]. Rohde & Schwarz propose notamment deux gammes

d'oscilloscopes numériques tactiles à base de radio logicielle [rohde]: la série RTM (à partir de 5 K€) à 500 MHz de bande passante, 5 Géch/s de vitesse d'échantillonnage et 8 millions d'échantillons mémorisables sur deux ou quatre voies ; et la série RTO (à partir de 12 K€) à 1 GHz ou 2 GHz de bande passante, 10 Géch/s et 20 Millions d'échantillons mémorisables (par voie) sur deux ou quatre voies.

I.3 Architectures d'une radio logicielle

I.3.1 Radio logicielle idéale

Une radio logicielle idéale se compose d'une ou plusieurs antennes pour capter le signal radioélectrique, d'un filtrage RF composé d'un filtre large bande – soit un amplificateur faible bruit (LNA – *Low Noise Amplifier*) en réception – soit un amplificateur de puissance en émission, d'un filtre bande utile, d'un CAN large bande pour le circuit de réception – ou d'un convertisseur numérique/analogique (CNA) pour le circuit d'émission, et d'un processeur de traitement numérique du signal (PTS, ou DSP en anglais – *Digital Signal Processor*) pour extraire les informations utiles (sélection du canal, démodulation, décodage...) ou pour les mettre en forme (modulation, codage,...). Le synoptique suivant présente l'architecture type d'une radio logicielle idéale.

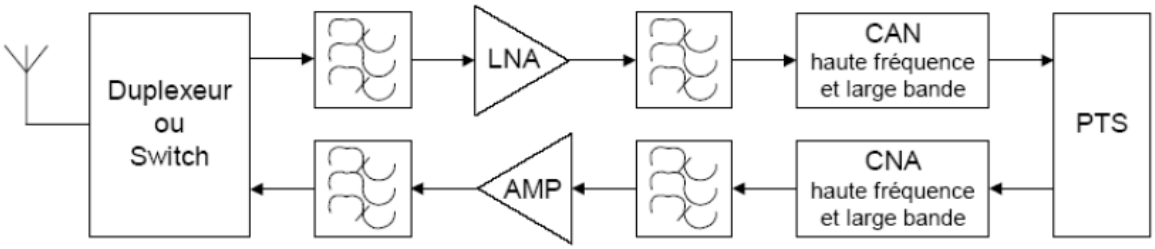

Figure 2 : Architecture simplifiée d'une radio logicielle idéale[5]

Une radio logicielle idéale présente les composants suivants :

- Antenne large bande : Une gamme de fréquence d'au moins cinq octaves[6] est nécessaire, avec un gain de 0 dBi. Actuellement aucune antenne n'est capable de telles performances ;

- Circulateur ou duplexeur : Un circulateur idéal est utilisé pour séparer le chemin des signaux en émission et en réception. On suppose que ce circulateur est très large bande, assure une isolation parfaite entre les signaux émis et reçus et est parfaitement adapté aux impédances de l'antenne et à l'amplificateur de puissance, ce qui est irréalisable

[5] Adapté de [kenington]
[6] Soit un rapport de près de 32 entre la fréquence basse et la fréquence haute.

actuellement. Dans une architecture multibande et multistandard, ces exigences sont impossibles à atteindre avec un duplexeur conventionnel (à base de filtres), car ce dernier n'est pas adapté aux fréquences élevées de commutation, aussi cherche-t-on à le remplacer progressivement par des circulateurs à ferrite. [zahwe] ;

- Amplificateur de puissance RF : L'amplificateur de puissance doit garantir une transformation idéale de la modulation RF du CAN en un signal de forte puissance approprié pour la transmission, avec de faibles émissions (idéalement aucunes) dans les canaux adjacents au canal utile. La linéarisation des amplificateurs de puissance a fait l'objet d'importantes recherches ces dernières années, aussi existe-t-il bon nombre de techniques candidates. Beaucoup de systèmes à bande étroite ont employé la technique à boucle cartésienne, offrant des taux d'intermodulation de l'ordre de -70 dBc. Pour des systèmes à bande passante plus large, la prédistorsion RF, la prédistorsion numérique et les techniques de correction aval (*feed-forward*) sont également utilisées. À l'heure actuelle, la prédistorsion numérique est une solution réalisable et convient bien à l'architecture d'une radio logicielle (elle est souvent employée dans les stations de base de téléphonie mobile).

- Convertisseur analogique/numérique : Le CAN doit disposer d'une forte résolution (de l'ordre de 20 bits), échantillonner à haute fréquence[7] (plus d'une dizaine de milliards d'échantillons par seconde) et comporter (ou être associé à) un filtre antirepliement[8]. L'emploi d'un tel CAN n'est pas pour le moment envisageable car il impliquerait une consommation électrique prohibitive. Il est toutefois possible de faire chuter la fréquence d'échantillonnage à l'aide de la technique du sous-échantillonnage, mais cela suppose que le filtrage RF et l'entrée analogique du CAN soient d'excellente qualité ;

- Convertisseur numérique/analogique : Les contraintes imposées au CNA sont du même ordre que celles du CAN. Mais compte tenu d'une complexité de réalisation moindre, la conception de CNA pour radio logicielle idéale est envisageable, mais toujours au prix d'une consommation énergétique élevée ;

- Traitement numérique du signal : Le sous-système logiciel doit être suffisamment performant (idéalement un processeur infiniment rapide !) pour supporter des opérations de traitement numérique (transformée de Fourier, modulation, démodulation, sélection de

[7] D'après le critère de Nyquist, la fréquence d'échantillonnage doit être au moins double de la bande passante du signal à exploiter.

[8] Le filtre antirepliement est un filtre fréquentiel passe-bas placé avant l'opération d'échantillonnage proprement dite, dont la fréquence de coupure est théoriquement égale à la moitié de la fréquence d'échantillonnage.

canaux, établissement de protocoles, égalisation, etc.) sur un ou plusieurs signaux potentiellement issus de standards différents [godard]. La technologie des DSP (processeurs de traitement numérique du signal et technologies équivalentes) progresse rapidement, et la principale question qui se pose à l'heure actuelle pour un équipement mobile est celle de sa consommation énergétique. Des combinaisons de matériels configurables (par exemple FPGA) et de processeurs entièrement programmables sont susceptibles de fournir les meilleurs rendements énergétiques.

Compte tenu de contraintes techniques pesant sur ses composants, la radio logicielle dite idéale s'avère irréalisable dans un proche avenir. En attendant, une déclinaison sous-optimale mais réalisable est mise en œuvre, il s'agit de la radio logicielle restreinte.

I.3.2 Radio logicielle restreinte (SDR)

Une radio logicielle Restreinte (RLR, ou en anglais SDR – *Software Defined Radio*) est un système de transmission radio où certaines fonctions sont réalisées par du matériel dédié, paramétrable et contrôlable par logiciel, et où d'autres fonctions telles que le traitement numérique du signal sont programmables par logiciel. Le terme de radio logicielle restreinte est apparu pour la première fois en 1992 dans l'article scientifique « *Software Radios : Survey, Critical Evaluation and Future Directions* » [mitola3]. Le schéma suivant présente le schéma bloc des différents étages de traitement d'une SDR. Il est composé de :

- une tête RF analogique configurable, composée de filtres, coupleurs, mélangeurs, oscillateurs locaux à fréquence intermédiaire, amplificateurs de puissance à large bande et à faible bruit,

- un étage de conversion analogique/numérique (CAN) et numérique/analogique (CNA),

- une section numérique programmable assurant la mise en forme du spectre, l'adaptation et le traitement numérique en bande de base,

- une section logicielle assurant le contrôle, la commande et la configuration logicielle des différents étages.

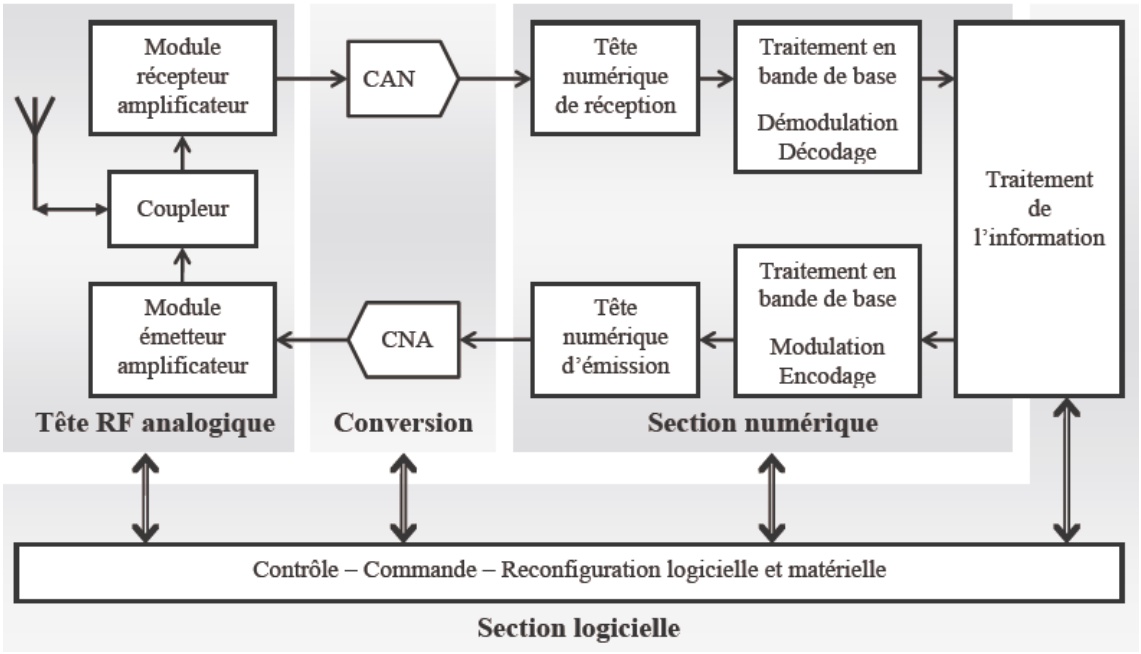

Figure 3 : Architecture de radio logicielle restreinte[9]

Des frontaux RF configurables et modulaires permettent de communiquer dans différentes bandes de fréquences. Pour adapter le taux de transfert des données entres les CAN/CNA et les fonctions de traitement numérique du signal généralement exécutées sur un ordinateur hôte, une section numérique est insérée, principalement pour réaliser des opérations de conversion de taux d'échantillonnage et de traitement en bande de base, voire également de modulation, de démodulation, d'encodage et de décodage. Les opérations de traitement numérique du signal sont généralement assurées par différents types de processeurs (on peut les associer) tels qu'un DSP (*Digital Signal Processor*), un circuit spécialisé (ASIC - *Application-Specific Integrated Circuit*, ASIP - *Application-Specific Instruction-set Processor*), un circuit intégré programmable (FPGA - *Field Programmable Gate Array*), un processeur à usage général (GPP – *General Purpose Processor*, dont le PC traditionnel fait partie), voire même depuis peu un processeur graphique (GPU - *Graphics Processing Unit*), chacun de ces processeurs étant plus ou moins adapté à certaines fonctions ou calculs.

L'usage d'équipements type FPGA et de DSP, en plus d'un ordinateur traditionnel, permet de partager voire de prendre en compte une grand partie de la charge de calcul, en contrepartie d'une moindre flexibilité. Une attention particulière doit être portée sur le choix du protocole de transfert de données entre ces différents éléments lorsqu'ils

[9] Source : [barrandon].

constituent des équipements distincts[10]. Pour obtenir de bonnes performances en gestion multistandard, des liaisons haut débit de dernière génération (exemples : Gigabit Ethernet, PCI Express, InfiniBand et USB 3.0) sont à privilégier. Une étude détaillée des éléments constitutifs d'une SDR est consultable en **annexe B**.

La radio logicielle est une forme émergente d'architecture radio, englobant un large éventail de techniques de conception afin de réaliser un système d'émission/réception véritablement flexible et adaptatif. Son domaine technologique est très large car il englobe la conception des matériels analogiques RF, FI et bande de base, la conception de matériels numériques et le génie logiciel. La radio logicielle apporte certes une plus grande adaptabilité vis à vis de différents standards radio grâce à une simple mise à jour logicielle, mais cette migration vers le "tout logiciel" amène d'autres contraintes telles que la sûreté et la sécurité de fonctionnement, et la difficulté à certifier des systèmes à comportement électromagnétique facilement modifiable.

I.3.3 Architectures des récepteurs de radio logicielle

Le circuit de réception est le point le plus délicat lors du design d'une radio logicielle car il concentre l'essentiel des contraintes technologiques de conception. En réception, la sélection d'un canal utile est réalisée en une ou plusieurs étapes par filtrage analogique et/ou numérique. La première étape est la sélection de la bande de réception à l'aide de filtres ayant des facteurs de qualité très élevés. Ces filtres, généralement à onde de surface (SAW – *Surface Acoustic Wave*), ne peuvent pas faire l'objet d'une miniaturisation. Le passage des fréquences RF aux fréquences basses s'effectue également en une ou plusieurs étapes, généralement à l'aide de mélangeurs et d'un CAN pour la numérisation. Enfin, un processeur numérique restitue les informations attendues. Les diverses architectures possibles d'un récepteur de radio logicielle peuvent être différenciées à l'aide de quatre paramètres [as37] :

- Transmission monocanal ou multicanal : la tendance monocanal tend à disparaître avec la montée en puissance des terminaux multicanaux et l'apparition de bandes de fréquences non soumises à licence. Le choix de l'un de ces deux modes de transmission a une conséquence directe sur la démodulation et la largeur des filtres RF/FI ;

Remarque : le concept d'architecture de réception multicanal est une extension de l'architecture de réception monocanal où l'on remplace le mot « canal » par « bande

[10] 1 MHz de bande spectrale nécessite un débit d'environ 40 Mbit/s par sens de transmission [farrell].

passante comprenant plusieurs canaux ». En comparaison d'une approche multirécepteur, l'approche multicanal a pour principal avantage de permettre de surveiller simultanément un grand nombre de canaux, mais s'ajoutent les contraintes suivantes : augmentation de la résolution d'échantillonnage et augmentation des contraintes de linéarité sur les circuits d'amplification.

- Transposition de fréquence : l'utilisation d'une fréquence intermédiaire (FI) est représentative d'une SDR car c'est un palliatif à la radio logicielle idéale tant que ne seront pas réglés les difficultés de numérisation directe du signal RF et de limitation de la consommation énergétique des composants haute fréquence.

- Sous-échantillonnage : Le sous-échantillonnage est une technique qui permet d'éviter l'utilisation du CAN aux fréquences élevées du signal RF.

- Démodulation numérique ou analogique : cela correspond au passage du signal à fréquence porteuse (RF ou FI) aux symboles complexes en bande de base. La démodulation analogique s'effectue avec un déphasage de $\pi/2$ pour obtenir les deux voies I et Q, et n'est utilisée que pour la réception monocanal. La démodulation numérique est obtenue par suréchantillonnage de la fréquence symbole.

Les récepteurs de radio logicielle peuvent également être classés en fonction de la position du CAN dans la chaîne de réception (en RF, en FI ou en bande de base) et par rapport au nombre et au type de transposition de fréquence utilisés. Le schéma suivant reprend l'esprit de cette classification.

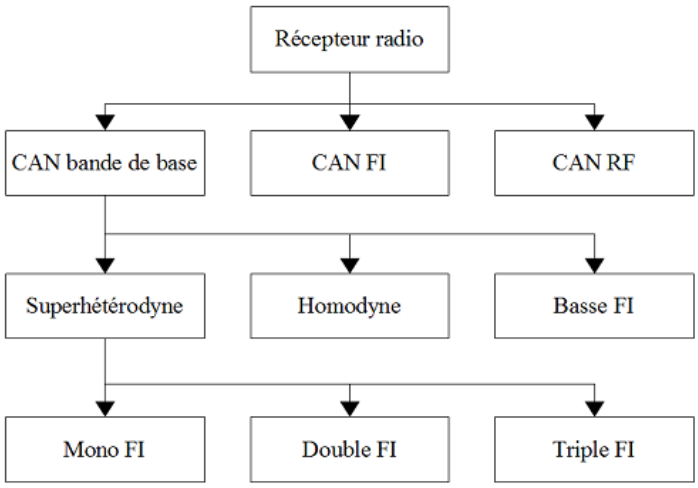

Figure 4 : Classification des récepteurs de radio logicielle

Une étude détaillée des principales architectures de récepteur de radio logicielle est consultable en **annexe A**. Le tableau V synthétise les résultats de cette étude.

Tableau V : Comparaison entre les principales architectures de récepteur de radio logicielle

Type de récepteur	Avantages	Inconvénients
Superhétérodyne	Numérisation en bande de base : importante sélectivité, grande sensibilité. Maîtrise de fabrication. Faible fuite de l'oscillateur local sur l'antenne. Utilisation de capacités de découplage pour éliminer l'offset de tension continue. Numérisation en FI : idem plus une quadrature quasi-parfaite et exempte de tout offset, et élimination de l'erreur de phase.	Nécessite des filtres de haute qualité, un nombre élevé de composants et une adaptation d'impédance entre chaque bloc. Consommation élevée. Intégration MMIC impossible. Pas du tout adapté à un fonctionnement multibande et multistandard.
Conversion directe	Simplicité de conception RF. Un seul étage de transposition. Consommation réduite. Plus de fréquence image et d'adaptation 50 ohms après le LNA. Forte intégration.	Problème de saturation par offset de tension continue. Sensibilité et dynamique élevées de la partie bande de base. Intermodulation d'ordre 2. Bruit en 1/f. Contraintes sur le traitement en bande de base. Sensibilité au désappariement et difficulté d'équilibrage des voies I et Q.
Faible fréquence intermédiaire	Consommation réduite. Forte intégration MMIC. Pas d'offset de tension continue, de problème de bruit en 1/f, d'adaptation, de filtres image et de filtres FI.	Filtrage passe-bas large bande. Sensibilité au désappariement et difficulté d'équilibrage des voies I et Q. Sensibilité et dynamique élevées de la partie bande de base. Intermodulation d'ordre 2.
Numérisation en RF	Mêmes avantages que la conversion directe. Minimisation extrême de la composante matérielle.	Rapport signal à bruit dégradé. Nécessite de filtres très sélectifs. Contraintes très fortes sur la conversion analogique-numérique.

I.3.4 Architectures des émetteurs de radio logicielle

Comme pour les circuits de réception de SDR, plusieurs types de circuit d'émission existent. Ces différentes architectures utilisent des techniques similaires à celles des récepteurs : superhétérodyne, *Low-IF* et conversion directe, avec des avantages et inconvénients mentionnés précédemment. Les contraintes de conception des émetteurs de SDR sont moindres que celles des récepteurs et ne seront pas abordées.

I.4 Composantes logicielles

I.4.1 Philosophies de conception logicielle et modèles

Il existe plusieurs techniques de programmation logicielle pouvant être appliquées aux radios logicielles : programmations linéaire, orientée objet, à base de composants, orientée aspect, ainsi que les patrons de conception. Ces techniques sont définies en **annexe E**.

I.4.1.1 Techniques de programmation dominantes en radio logicielle

Les techniques de programmation dominantes en SDR sont la programmation à base de composants, parce qu'elle imite le mieux la structure d'un système radio, à savoir l'utilisation de composants distincts pour différents blocs fonctionnels d'un système radio, et la programmation orientée objet, parce qu'elle facilite la réutilisation de code (héritage), le masquage des détails d'implémentation des algorithmes (encapsulation) et le traitement des évènements. J. Mitola souligne que s'il est possible de concevoir des logiciels pour SDR à l'aide d'une méthode d'analyse descendante, il n'est pas sage de l'utiliser dans tous les cas. [mitola] En effet, certains composants logiciels d'une SDR peuvent être réutilisés à partir de ceux d'autres projets de SDR. La possibilité et les conditions d'utilisation de ces modules logiciels préexistants doivent être étudiées suffisamment tôt dans le cycle de conception de sorte qu'ils puissent être correctement interfacés avec les autres composants. Le processus de réutilisation de ces composants logiciels, en les adaptant au besoin, s'intègre dans une analyse ascendante couplée avec le flot de conception du logiciel.

L'objectif de l'architecture logicielle dans une SDR est de permettre le développement de formes d'ondes indépendamment de la connaissance du matériel sous-jacent. Ceci est possible grâce à l'emploi d'API standardisées et de bibliothèques de formes d'onde. Certains groupes de l'industrie ont ainsi standardisé des API entières de radio logicielle, en fondant leur travail sur les techniques de programmation orientée objet.

I.4.2 Architectures et normes logicielles pour SDR

I.4.2.1 Ham Radio Control Libraries

Le *Ham Radio Control Libraries*, ou Hamlib en abrégé, est un effort de développement « libre » consistant à fournir une interface cohérente aux programmeurs désirant intégrer du contrôle d'équipement radio dans leurs programmes [hamlib]. Hamlib n'est pas une application utilisateur complète mais une couche logicielle destinée à prendre le contrôle de divers équipements radioamateurs. La plupart des émetteurs/récepteurs radios récents autorise un contrôle externe de leurs fonctions via une interface série, mais chacun avec ses spécificités. Hamlib fournit une API permettant de commander un certain nombre d'équipements radio et de rotors d'antennes [hamlibsr] mais l'éventail des actions possibles (accord en fréquence, niveau) est très limité et est fonction de l'équipement radio utilisé.

I.4.2.2 SCA

Une architecture particulièrement utilisée dans l'industrie de défense est le standard SCA (*Software Communications Architecture* - Architecture logicielle de communication), architecture logicielle standardisée parrainée par le Bureau du Programme Interarmées (*Joint Program Office* - JPO) du ministère de la défense des États-Unis dans le cadre du programme de système radio tactique interarmées JTRS (cf. §I.2.5.1). SCA est maintenant adoptée par de nombreux opérateurs de défense du monde entier. Elle comporte une spécification principale (JTRS-5000SCA) et deux suppléments couvrant les API (JTRS-5000API) et les questions de sécurité (JTRS-5000SEC). SCA est une architecture de gestion de composants fonctionnant sur système d'exploitation compatible POSIX tel que Linux ou VxWorks[11]. Elle fournit un ensemble sécurisé d'applications de traitement du signal et une infrastructure logicielle pour créer, installer, gérer, et désinstaller des formes d'onde. SCA est capable de contrôler et de gérer le matériel, d'interagir avec des services externes au travers d'un ensemble d'interfaces, et de fonctionner sur des matériels distribués et hétérogènes.

Le standard SCA a été initialement publié en Février 2000, et a connu plusieurs révisions depuis. Les versions postérieures à la 2.2.1, publiée en avril 2004, concernent la correction de bogues et l'ajout de fonctionnalités. Toutefois, une limitation majeure des versions 1.x et 2.x est de ne pas bien supporter l'emploi de DSP et FPGA. Dans la pratique un DSP ou un FPGA ne peut utiliser SCA en mode natif que s'il est en mesure d'exécuter un système d'exploitation compatible POSIX. Mais si le DSP ou le FPGA n'a pas cette capacité, comme c'est le cas sur les petits systèmes, il devra être géré par des objets "adaptateurs" s'exécutant sur un processeur hôte implémentant nativement SCA. La version 3.0, publiée en août 2004, a tenté sans franc succès de contourner cette contrainte, et son développement est actuellement au point mort. La version 2.2.2, ratifiée en juin 2006, est considérée comme la plus récente. Une évolution majeure de la SCA, nommée SCA *Next*, est toutefois en cours de spécification. [sca]

SCA cherche à répondre à deux objectifs fondamentaux, à savoir la portabilité et la réutilisation de code. SCA est construit autour du middleware CORBA (*Common Object Request Broker Architecture*) et sur le modèle CCM (modèle de composants CORBA). Bien que destiné initialement aux GPP, CORBA est de plus en plus présent au sein des

[11] VxWorks est un système d'exploitation temps réel multitâche type Unix de la société Wind River. Il est généralement utilisé dans les systèmes embarqués.

DSP et FPGA embarquant un système d'exploitation compatible POSIX. CCM permet aux applications de déclarer, à l'aide de descriptions XML, les ressources CORBA dont elles ont besoin. SCA souffre de quelques limitations telles que le support du temps réel (gestion de la latence, des processus et des *threads*). De plus, il ne spécifie pas la façon dont un composant doit être mis en œuvre, quel matériel supporte tel type de fonctionnalité ni même la stratégie de développement à suivre. SCA fournit un ensemble de règles de base pour la gestion de logiciels sur un système, en laissant de nombreuses décisions de conception au développeur. Le synoptique suivant présente l'emploi de CORBA et d'IDL dans SCA.

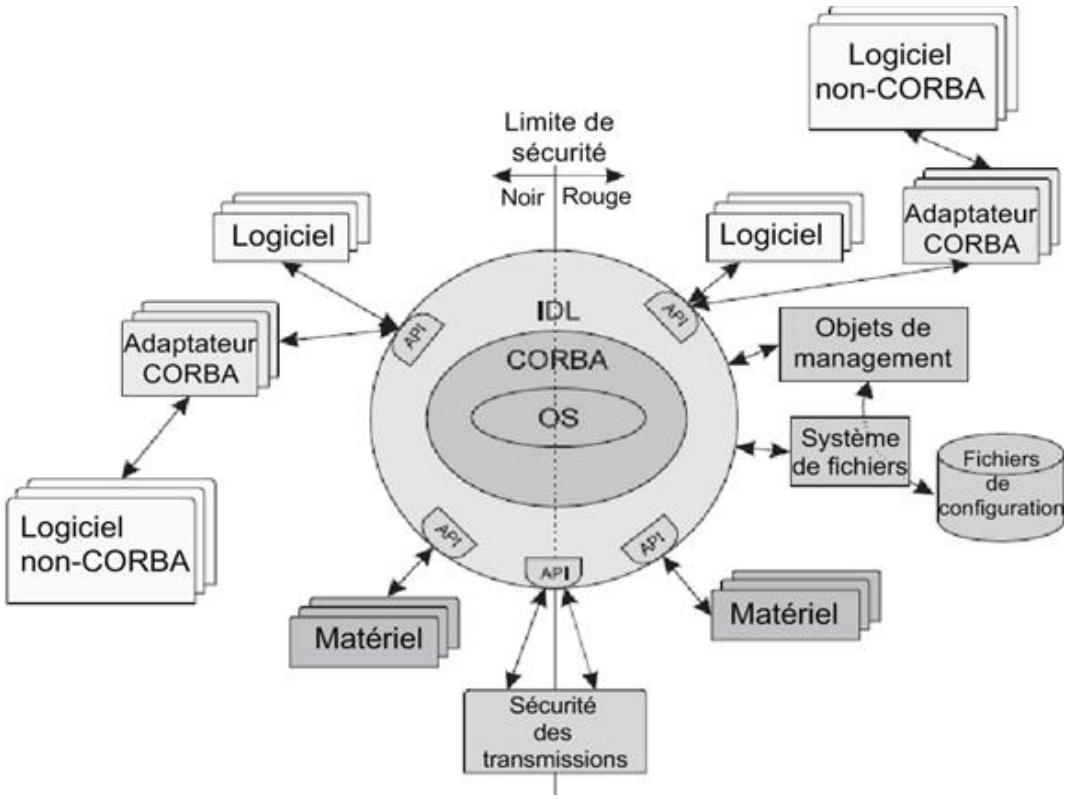

Figure 5 : Le modèle SCA/CORBA[12]

Dans l'architecture logicielle SCA, la SDR est vue comme un empilement de fonctions matérielles et logicielles, avec des interfaces au standard ouvert (cf. figure suivante). La base de la pile représente le matériel et les bus de données interprocesseurs. Au-dessus on a le chargeur de démarrage, les pilotes d'entrée/sortie et une couche d'abstraction matérielle permettant au GPP de communiquer avec des processeurs spécifiques type DSP ou FPGA. SCA a trois composantes principales : le déploiement de formes d'ondes, le *Core Framework* (CF), et le profil de domaine. Le déploiement des

[12] Adapté de [fette].

formes d'ondes contient les instanciations des éléments qui composent l'algorithme de la forme d'onde et les applications qui fournissent l'interface de haut niveau pour l'utilisateur. Le *Core Framework* est l'ensemble des logiciels qui gèrent l'équipement radio et ses ressources. Le profil de domaine est un ensemble de fichiers XML qui décrivent le matériel radio, la forme d'onde applicative, les connexions des composants, et les dépendances.

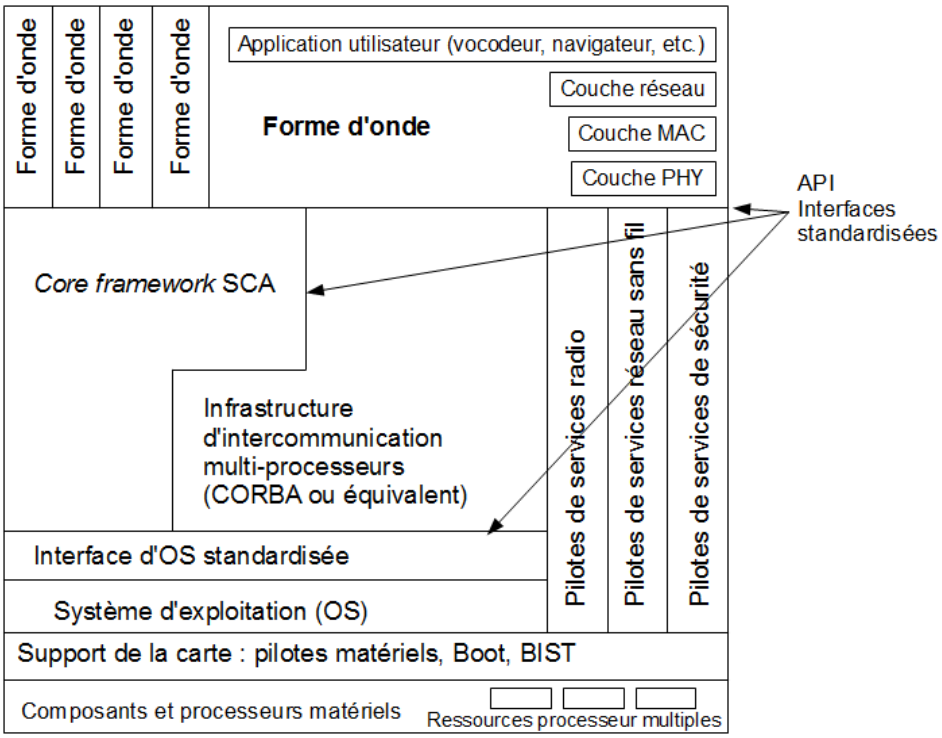

Figure 6 : Architecture logicielle SCA[13]

Le principe de SCA est axé sur les processus de déploiement et d'interfaçage de composants logiciels d'une SDR. Cela permet à ces composants d'être remplacés au besoin sans avoir à réécrire le code de l'interface, mais ne rend toutefois pas les formes d'ondes indépendantes de la plateforme. Une fois qu'un processus SCA a déployé une forme d'onde sur un système, et que le système fonctionne, il se place en arrière-plan jusqu'à ce qu'une nouvelle configuration soit requise. Par conséquent SCA n'a que peu d'impact sur les performances d'un processeur une fois la forme d'onde opérationnelle.

SCA prend en charge la sécurité des communications en définissant deux zones : une zone «rouge» et une zone «noire». La zone noire, sécurisée par des moyens de chiffrement, contient la plupart des composants de la SDR dont l'interface RF, les étages

[13] Adapté de [fette].

FI, la conversion analogique/numérique et une partie du traitement numérique. La partie rouge contient en clair le traitement et les applications " utilisateur ". L'ajout de complexité apporté par une scission du système en deux parties de sensibilité différente constitue actuellement un frein à un emploi plus généralisé de SCA. Pour exemple les entreprises PrismTech (ligne de produits Spectra [spectra]) et Zeligsoft (produit CE [zeligsoft]) fournissent des outils de développement, de middleware, et des bibliothèques destinées au développement de SDR basées sur SCA.

Plusieurs solutions de développement SCA sont aujourd'hui disponibles publiquement, comme OSSIE (*Open Source SCA Implementation – Embedded*) de Virginia Tech [ossie] ou SCARI-Open (*SCA Reference Implementation*) développé en Java par le Centre canadien de recherche en communications [scari]. Des tests comparatifs de rapidité ont été réalisés par [abgrall] sur les architectures logicielles OSSIE et GNU Radio (avantage au dernier, à cause de lenteurs de traitement dues à l'usage de CORBA).

I.4.2.3 OMG MDA

L'*Object Management Group* (OMG) définit une norme connue sous le nom MDA (*Model-Driven Architecture*) adaptable à la radio logicielle [omg]. MDA a pour objectif de définir des interfaces entre composants logiciels. Pour ce faire, une spécification basée sur MDA va définir des PIM *(Platform Independent Models*), modèles indépendants d'une technologie, architecture ou plateforme particulière. Une fois cette opération terminée, les PIM sont mappés sur une plate-forme spécifique, généralement en utilisant CORBA et/ou XML, produisant des modèles spécifiques à une plateforme (PSM – *Platform-Specific Model*). Enfin, des modèles de mise en correspondance (*mapping*) peuvent être définis pour décrire la façon de passer de manière cohérente d'un modèle à un autre.

I.4.2.4 Le standard OMG SWRadio

La spécification SWRadio est initialement une volonté de l'OMG de migrer le standard SCA vers l'industrie. Elle a évolué en 2007 pour devenir une norme indépendante. Comme SCA, la spécification SWRadio se concentre sur les interfaces entre les composants de la SDR, mais à la différence près que SWRadio utilise UML pour modéliser ces composants, et ajoute un PIM et un PSM pour la description des interfaces des composants en CORBA IDL. SWRadio prend en charge la même répartition de sécurité rouge/noir que SCA, mais apporte plus de souplesse en ne l'imposant pas. La spécification SWRadio est construite sur le modèle OSI. Elle définit une couche matérielle qui définit les ressources disponibles, une couche « environnement d'exploitation » qui

fournit le système d'exploitation et les services de middleware, une couche d'installation qui fournit des services supplémentaires à la demande, et une couche applicative.

I.4.2.5 Autres normes logicielles

L'IEEE *Standards Coordinating Committee* 41 (SCC41) travaille depuis 2005 à élaborer des normes pour les radios intelligentes, en se concentrant sur la gestion des interférences, la coexistence de réseaux sans fil hétérogènes partageant le spectre électromagnétique, l'optimisation du spectre et l'accès dynamique au spectre. À ce jour en sont sorties les normes IEEE P1900.1, standardisant les définitions et concepts de la radio intelligente, et P1900.2, couvrant le sujet des interférences et de la coexistence de systèmes. Mais la norme la plus intéressante pour les concepteurs de SDR est l'IEEE P1900.3 recommandant une procédure d'évaluation de la conformité des modules logiciels de SDR. [scc41]

I.4.3 GNU Radio

I.4.3.1 Présentation

Parmi les actuels projets « libres » de radio logicielle, un est en passe d'occuper une position dominante : GNU Radio. GNU Radio est une boite à outils logicielle sous licence GNU GPL (*General Public License*) version 3, donc « libre » et gratuite, fournissant une bibliothèque de fonctions que l'on assemble pour constituer des chaînes de création et d'analyse de formes d'onde [gnuradio1]. L'objectif de GNU Radio est de donner au plus grand nombre la possibilité d'étudier et de comprendre le spectre électromagnétique, et de réfléchir à des façons intelligentes de l'utiliser. Initiée par Eric Blossom au début des années 2000 et repris depuis septembre 2010 par Thomas W. Rondeau [gnuradio5], le projet GNU Radio est devenu une architecture « libre » presque mature de développement de radios logicielles en C++ et Python[14].

Dédiée à la plateforme matérielle USRP (*Universal Software Radio Peripheral*) mais néanmoins indépendante du matériel associé, GNU Radio est conçue pour

[14] Python est un langage orienté objet interprété et interactif. Python n'est pas conçu pour les environnements mobiles, mais peut jouer un rôle important dans les applications sans fil, comme en témoigne son utilisation par GNU Radio. Sa force réside dans sa combinaison des avantages de la conception orientée objet avec l'aisance d'un langage interprété. Avec un langage interprété, il est relativement facile de créer des programmes simples soutenant certaines fonctionnalités de base. Python va au-delà de la plupart des langages interprétés en ajoutant la capacité d'interagir avec les bibliothèques d'autres systèmes. Par exemple, en utilisant Python, on peut facilement écrire une application fenêtrée utilisant des wxWidgets, ou interagir avec des modules écrits en C/C++. Python fournit également des structures de gestion de la mémoire, simplifiant le développement d'applications. De plus, étant donné que Python est interprété, il est indépendant du système d'exploitation utilisé.

fonctionner sur divers microprocesseurs (x86 32 bits et 64 bits, PowerPC, Cell, ARM et OMAP), et sous différents systèmes d'exploitation (Linux, FreeBSD, NetBSD, Mac OS X, ainsi que Windows XP et Windows 2000 à l'aide du portage Cygwin). Pour installer GNU Radio sous Linux, un mode opératoire est disponible sur Internet [gnuradio4]. À noter toutefois que sous Windows, les pleines fonctionnalités de GNU Radio ne sont pas garanties.

GNU Radio dispose de bibliothèques de blocs de traitement du signal ou SPM[15] (*Signal Processing Module*) relatifs à la réalisation de tâches propres à une radio logicielle : modulations (GMSK, PSK, QAM), fonctions d'étalement de spectre type OFDM, codes correcteurs d'erreur (Reed-Solomon, Viterbi, Turbo Codes), fonctions de traitement du signal (filtres, FFT, égaliseurs), récupération d'horloge, opérations d'entrées-sorties telles que l'accès aux fichiers, etc., et bien sûr des interfaces de communication ou pilotes permettant d'interagir avec le matériel (USRP, cartes RF, etc.).

Le développement sous GNU Radio consiste à construire un système de communication en créant un graphe de traitement du signal (ou graphe de flux) où les nœuds sont les blocs de traitements du signal et les branches représentent le flux de données entre les blocs [gnuradio2]. Les blocs dits de bas niveau sont implémentés en C++ [gnuradio3] tandis que les blocs dits de haut niveau ainsi que la création des graphes GNU Radio sont réalisés en Python [python]. Le fonctionnement de l'ensemble est orchestré par un Ordonnanceur Python.

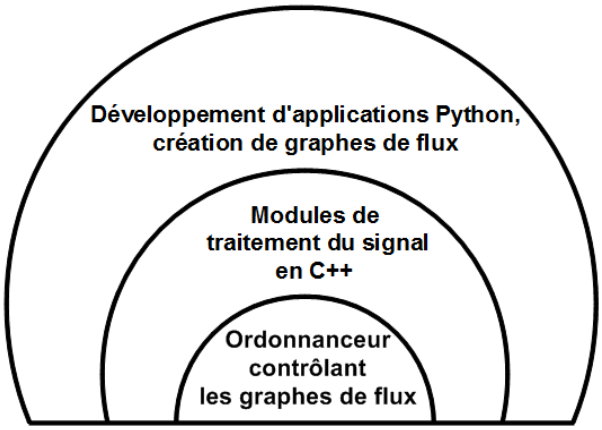

Figure 7 : Modèle de développement GNU Radio

SWIG (*Simplified Wrapper and Interface Generator*), outil de développement logiciel assurant l'interface entre des programmes écrits en C ou C++ et une variété de

[15] Une liste complète de ces blocs est accessible à [doxygen].

langage de programmation de haut niveau, est utilisé dans la GNU Radio pour relier ensemble les codes C++ et Python. [swig]

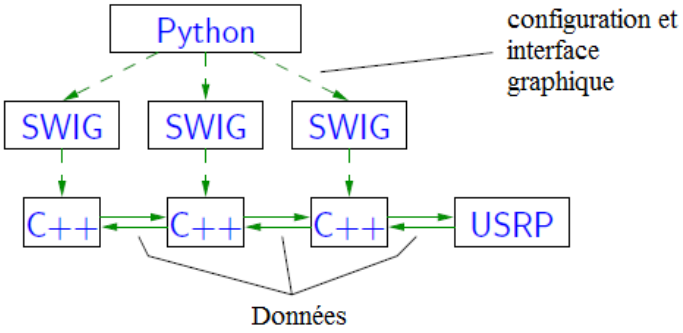

Figure 8 : GNU Radio – couches logicielles

I.4.3.2 Blocs de traitements et graphe de flux

La plupart des blocs opèrent sur un ou plusieurs flux continus de données : ils consomment les données arrivant sur leur(s) entrée(s) et génèrent des données sur leur(s) sortie(s) à l'issue d'un traitement particulier (filtrage, FFT, modulation, etc.). Des blocs spéciaux, appelés sources (respectivement *sinks*) produisent (respectivement consomment) les données. Par exemple, les blocs lisant des générateurs de tonalité, des *sockets*, descripteurs de fichier ou ports R_X d'USRP via les pilotes associés, sont des sources. Les blocs écrivant dans des *sockets*, descripteurs de fichiers, afficheurs graphiques (exemple : oscilloscope), pilotes de carte son ou de ports T_X d'USRP, sont des *sinks*. Chaque bloc présente une signature d'entrées-sorties définissant les nombres minimaux et maximaux d'entrées et de sorties qu'ils peuvent avoir, ainsi que la taille et le type des flux d'entrée et de sortie. Chaque bloc définit une fonction opérant sur les flux d'entrée pour produire les flux de sortie et indique à l'Ordonnanceur le rythme de consommation et de production des données. Pour ce faire les flux d'entrée et de sortie d'un bloc sont associés à des mémoires tampon (*buffers*) de type FIFO. L'association de blocs de traitement constitue un graphe de flux. Un graphe de flux est principalement définit à l'aide de la fonction `connect`. La fonction `connect` spécifie comment les flux de sortie d'un bloc sont reliés à un ou plusieurs flux d'entrée des blocs suivants.

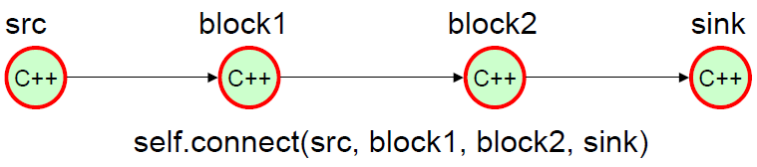

Figure 9 : Exemple d'usage de la fonction `connect`

I.4.3.3 Ordonnanceur

L'Ordonnanceur de GNU Radio exécute en continu le graphe de flux. Deux Ordonnanceurs sont disponibles : le premier est un Ordonnanceur *mono-thread* : c'est un *thread* qui boucle sur tous les blocs du graphe et exécute chaque bloc de façon séquentielle jusqu'à ce que toutes les données aient été consommées. Si suffisamment de données sont disponibles dans les *buffers* d'entrée, l'Ordonnanceur appelle la fonction de traitement du bloc. Si un bloc n'a pas assez de données en entrée, l'Ordonnanceur se déplace sur le bloc suivant dans le graphe. Les blocs " sautés " sont exécutés plus tard, dès qu'ils ont suffisamment de données en entrée. Le second est un Ordonnanceur *multi-thread* qui génère un *thread* par bloc de traitement, ce qui permet en théorie à GNU Radio de tirer profit des architectures multiprocesseurs.

I.4.3.4 Emploi et limitations

GNU Radio est en général un bon point de départ pour réaliser une SDR d'entrée de gamme, aussi rencontre-t-elle un franc succès sur le marché radioamateur et chez les universitaires. Elle souffre toutefois de quelques limitations. La limitation la plus significative réside dans les pilotes USRP. Ceux-ci sont écrits en Python, aussi la portion des blocs du diagramme de flux de la GNU Radio écrite en C++ n'a pas accès aux paramètres configurables de l'USRP. Ensuite GNU Radio ne fonctionne que sur GPP, ce qui limite *de facto* ses capacités en traitement du signal. Néanmoins le projet GNU Radio fait l'objet d'une communauté relativement active. C'est ainsi que les dernières versions de GNU Radio implémentent des fonctionnalités de couche MAC n'ayant pas besoin d'envoyer des données en continu (*message blocks* ou « *m-blocks* »), ainsi que le support des processeurs multicœurs. Pour terminer, l'utilisation de la GNU Radio impose que le développeur de radios logicielles dispose de connaissances solides dans de multiples domaines techniques, à savoir en informatique (programmation), en systèmes de télécommunication, et plus particulièrement en systèmes de radiocommunication, en traitement numérique du signal et en électronique (analogique et numérique).

I.4.4 Environnements de simulation et de développement

I.4.4.1 MATLAB

Commercialisé par MathWorks, MATLAB est un environnement de développement intégrant son propre langage de programmation, complété par de multiples boîtes à outils. L'un des modules les plus intéressants pour la radio logicielle est Simulink, plate-forme de modélisation de systèmes dynamiques, fournissant un environnement

graphique et un ensemble de bibliothèques pour le design, la simulation, l'implémentation et le contrôle de systèmes de communications et de traitement du signal. *The Mathworks*, éditeur de MATLAB, fournit un web-séminaire [mathworks] principalement axé sur le produit Simulink et le développement SCA. Lorsque MATLAB et Simulink sont utilisés en conjonction avec les modules "*Real-Time Workshop*" et "*Real-Time Workshop Embedded Coder*", ces outils peuvent générer du code exécutable sur des GPP ou des DSP. Les deux principaux fournisseurs de logique programmable, Xilinx (*System Generator for* DSP [xilinx2]) et Altera (DSP *Builder* [altera]), disposent d'interfaces Simulink permettant la génération de code FPGA sur leurs plateformes.

I.4.4.2 LabVIEW

LabVIEW (*Laboratory Virtual Instrument Engineering Workbench*) est un logiciel de développement d'applications de test automatisé (acquisition de données, contrôle/commande, contrôle d'instruments de mesure, de dispositifs expérimentaux, de bancs de test) de la société américaine National Instruments, basé sur un langage de programmation graphique (langage G) spécialisé dans le parallélisme et l'exécution par flux de données [labview]. Un programme LabVIEW permet d'automatiser un montage associant plusieurs appareils programmables, et regroupe sur une interface utilisateur unique l'accès aux fonctionnalités de ce montage. National instruments propose également des boîtes à outils (*toolkits*) permettant de mesurer et de générer des signaux spécifiques à une norme radiofréquence (*toolkits Modulation et Spectral Measurement, toolkit* GPS pour LabVIEW). [ni1]

I.4.4.3 SystemVue

SystemVue est une suite de logiciels payants spécialisée dans la conception et le développement de systèmes RF, ASIC, DSP et FPGA, vendue par la société américaine Agilent Technologies, et fonctionnant sous Windows [systemvue1]. Avantage : fonctionnellement complète [systemvue2].

I.4.4.4 GRC

GRC (GNU *Radio Companion*) est une application distribuée avec GNU Radio et avec laquelle peuvent être réalisées des radios logicielles à l'aide de graphes de flux utilisant un certain nombre de blocs fonctionnels prédéfinis (signaux source, sorties ou *sinks*, fonctions de modulation ou de démodulation, etc.) [grc]. GRC est une interface graphique " *drag and drop* " dédiée à la conception de chaînes de transmission GNU Radio

[grc2]. Les blocs de traitement du signal sont représentés graphiquement avec leurs paramètres. GRC génère automatiquement le code python équivalent au diagramme réalisé. GRC fonctionne principalement sous Linux mais aussi MacOS, Windows et NetBSD. Il sera utilisé sous Linux dans le cadre de la dernière partie de ce mémoire. Le schéma suivant décrit les traitements générés lors de l'utilisation d'un bloc dans GRC.

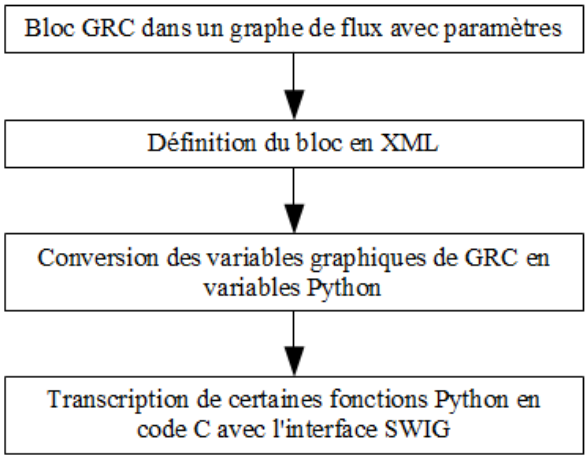

Figure 10 : Traitements associés à un bloc GRC

I.4.4.5 ISE WebPack

ISE *(Integrated Software Environment)* WebPack est un logiciel gratuit de conception de circuits logiques programmables Xilinx fonctionnant sous Windows et Linux [webpack]. ISE WebPack fait de la synthèse et de la simulation HDL (*Hardware Description Language*), et de la programmation JTAG (*Joint Test Action Group*, norme de test de cartes électroniques numériques). La fonctionnalité de configuration dynamique de FPGA est intégrée dans l'environnement ISE Design Suite version 12.2 et suivantes [xilinx3].

I.4.5 Logiciels de visualisation graphique de signaux radio

I.4.5.1 Baudline

Baudline est un analyseur de signaux disposant de son propre générateur de fonctions et d'une multitude de filtres et d'effets. Baudline combine un traitement numérique du signal, un affichage haute vitesse polyvalent, et des outils de capture en continu pour traquer et étudier les caractéristiques de signaux brefs. Baudline fonctionne sur de multiples processeurs (x86, x86_64, PPC, S/390, SPARC) et OS (Linux, FreeBSD, Mac OS X et Solaris). Voici quelques-unes de ses caractéristiques : bande passante 192 kHz en temps réel, 96 dB de dynamique, entrée réelle ou en quadrature, support de

plusieurs cartes son, canaux d'entrée configurables pouvant effectuer diverses opérations de traitement numérique du signal, diverses transformations (Fourier, réponse impulsionnelle, fonction de transfert), égalisation de canal, analyse statistique de distribution (fréquence, temps et amplitude), génération de signaux de test, gestion de multiples formats d'enregistrement, nombreuses mesures (distorsions, rapport signal/bruit, etc.). [baudline]

I.4.5.2 GNU Radio WXGUI Signal Analysis Tools

L'outil GNU Radio WXGUI *Signal Analysis Tools* améliore l'interface graphique de GNU Radio en apportant des fonctionnalités d'analyse de signaux. Il comporte un analyseur de spectre, un spectrographe 2D (*waterfall*), un oscilloscope, un histogramme et un diagramme de constellation. [wxgui]

I.4.5.3 Et aussi…

Les logiciels de visualisation de signaux radio sont nombreux mais généralement dédiés aux radioamateurs. Parmi ceux-ci, citons :

- **Ham Radio Deluxe** (HRD) est une suite logicielle gratuite pour Windows permettant un contrôle par ordinateur des émetteurs-récepteurs radioamateurs les plus courants [hrd]. HRD intègre également le repérage sur carte, la poursuite satellite et le logiciel de contrôle Digital Master 780 [dm780]. HRD fonctionne sous Windows 2000, XP, Vista et Seven. Internet Explorer 6.0 (ou version ultérieure) est également requis. La version 4 de HRD est opérationnelle et la version 5 est en version Bêta. [hrdv5] ;

- **Linrad** : logiciel fonctionnant sous Linux, Windows et Free BSD et avec n'importe quelle carte son à partir du moment où le PC dispose des drivers adéquats. [linrad] ;

- **Perseus Control Software** : logiciel associé à la plateforme matérielle du même nom, Perseus Control Software fonctionne sous Microsoft Windows 2000, XP et Vista. Il supporte jusqu'à 2 Méch/s et une réjection des images supérieur à 110 dB dans une largeur de bande de 1600 kHz. [perseusoft] ;

- **PowerSDR** : logiciel « libre » sous Windows XP, Vista et Seven, fonctionnant avec les équipements FlexRadio ainsi qu'avec d'autres plateformes matérielles (SDR-1000, SoftRock [softrock] et HPSDR). [powersdr] ;

- **Quisk** : logiciel « libre » qui permet la visualisation des signaux CW, SSB et AM. Quisk est écrit en Python et C et fonctionne sous Linux. [quisk]. En tant que récepteur,

Quisk peut utiliser l'équipement RFSpace SDR-IQ (cf. §II.2.3.1) comme source d'échantillonnage. Il existe plusieurs taux de décimation[16] disponibles. Le récepteur Quisk lit les données échantillonnées, fait l'accord en fréquence, filtre, démodule et envoie le tout à la carte son. La carte son peut également être utilisée comme source d'échantillonnage. En tant qu'émetteur, Quisk peut contrôler un excitateur SSB/CW et un émetteur-récepteur par liaison Ethernet ;

- **Rocky** : Windows uniquement. Supporte les SDR SoftRock [rocky] ;

- **SDRMAX** : logiciel « libre » associé au matériel radio Quicksilver QS1R et fonctionnant sous Windows XP, Vista, et Seven en version SDRMAXII [sdrmax] et sous Linux en version SDRMAXIII. [sdrmax3] ;

- **SDR-Shell** : logiciel « libre » de visualisation sous Linux développé avec la bibliothèque Qt[17]. Ne fonctionne actuellement qu'en mode réception (mode émission en cours de développement) [sdrshell] ;

- **SpectraVue** : Pour Windows uniquement, associé au récepteur SDR-IQ. [spectravue] ;

- **Spectrum Lab** : analyseur de spectre audio [spectrum] [spectrum2] ;

- **Winrad** : Windows uniquement. Supporte les SDR radioamateurs SDR-14, SDR-IQ, Perseus et Elektor WA6KBL. [winrad]

Actuellement, hormis GNU Radio, la majorité des logiciels « libres » de SDR sont à vocation radioamateur et se concentrent sur l'aspect "visualisation spectrale du signal". Quelques solutions payantes sont spécialisées dans la réalisation de certaines fonctions de développement logiciel de SDR (simulation, programmation de FPGA, etc.). Le marché de l'industrie de défense est quant à lui dominé par l'architecture logicielle SCA.

[16] Cf. le glossaire et l'annexe B §B.7 pour une explication de la notion de décimation.
[17] Qt est une bibliothèque multi plateforme de création d'interfaces graphiques utilisateurs, écrite en C++ mais pouvant être utilisée dans d'autres langages comme Java, Python et C#.

Chapitre II

Revue (non exhaustive) des plateformes existantes

Les plates-formes et bancs d'essai de radios logicielles « libres » offrent aux chercheurs et développeurs la possibilité de concevoir leurs propres applications radios logicielles, du moins sous la forme de prototype. Une plateforme de prototypage permet de tester et de valider les performances d'une architecture proche d'un système en production. Au vu de la complexité croissante des systèmes à concevoir, une plateforme de prototypage est choisie en fonction de critères multiples : flexibilité, rapidité de calcul, communications entre composants et avec les interfaces externes. Bien que la radio logicielle restreinte offre de multiples avantages aux concepteurs de systèmes radio, il reste de nombreuses questions ouvertes sur la façon de mettre en œuvre et de gérer la flexibilité dans un système de transmission sans fil.

La technologie radio logicielle a connu des améliorations substantielles ces dernières années. La réalisation de plates-formes à faible coût est maintenant possible et nombreuses sont les réalisations de SDR radioamateur. Des SDR sont également vendues par différentes entreprises spécialisées dans la conception d'équipements d'instrumentation, de test ou autre. Et dans le cadre de projets de recherche, plusieurs plateformes radios logicielles expérimentales ont pu voir le jour. La liste des radios logicielles à l'état de prototype, en développement, réalisées ou généralement pas finies, est assez impressionnante (cf. [f4dan] pour en avoir un aperçu). On distingue deux catégories de dispositifs à base de SDR :

- Les dispositifs spécifiques, conçus et développés pour répondre à un besoin particulier, relativement peu flexibles, souvent coûteux mais précis dans la tâche qu'ils accomplissent. On retrouve notamment dans cette catégorie les équipements de test et de métrologie (SDR d'industriels) et les plateformes de recherche à gros budget, mais également certaines fabrications artisanales visant une norme de radiocommunication ou un protocole particulier ;

- Les dispositifs flexibles, généralement plus accessibles financièrement, mais avec une précision moyenne et des performances contenues. On retrouve notamment dans cette catégorie des montages « libres », et certaines plateformes de recherche.

Les SDR présentées ci-après ont le mérite de faire l'objet d'un suivi plus ou moins actif. On se rendra compte que la plupart des SDR ont une vocation radioamateur et que finalement peu d'entre-elles sont large bande.

II.1 SDR professionnelles

II.1.1 Lyrtech

La société Lyrtech propose une plateforme de développement SDR modulaire pouvant fonctionner dans les bandes [200 MHz – 1 GHz], [1.6 GHz – 2.3 GHz], et WiMAX (SISO ou MIMO 2*2) 2.5 GHz ou 3.5 GHz [lyrtech]. La bande passante varie de 5 MHz à 22 MHz, selon le module RF utilisé. Le design de la SDR est réalisé à l'aide de l'environnement de développement Simulink et l'architecture logicielle SCA. Différentes configurations sont proposées pour des prix variant de 2 900 $ (module de DSP uniquement) à plus de plus de 10 000 $.

II.1.2 National Instruments

Les solutions National Instruments intègrent des technologies telles que les processeurs multicœurs, les FPGA, le PCI Express ainsi que les architectures logicielles parallèles permettant l'automatisation des tests sur les standards de communication sans fil Wi-Fi, WiMAX, GPS, RFID, ZigBee, GSM/EDGE, Bluetooth et WCDMA[ni4]. Le module récepteur PXIe-5663 analyse des signaux dans la bande [10 MHz - 6,6 GHz] avec jusqu'à 50 MHz de bande passante instantanée. Le module émetteur PXIe-5673 génère des signaux dans la bande [85 MHz - 6,6 GHz] avec jusqu'à 100 MHz de bande passante instantanée. L'ensemble fonctionne avec le logiciel NI LabVIEW présenté au paragraphe I.4.4.2. En terme de prix ces solutions sont particulièrement onéreuses (pour exemple le générateur et le récepteur cités précédemment coûtent chacun plus de 20 000 € en moyenne, et une solution SDR basée sur le NI PXIe-5641R coûte environ 41 000 €). [pxi5641r]

National Instruments vend également un pack SDR basé sur l'émetteur PXIe-5641R et couvrant les fréquences de 250 kHz à 2,7 GHz avec une bande passante instantanée de 20 MHz [nisdr]. Il comporte un CAN 14 bits 100 Méch/s à DDC intégré, et un CNA 14 bits 200 Méch/s à DUC intégré. Les données I/Q sont transmises à un FPGA Xilinx Virtex-5 SX95T pour effectuer des tâches d'analyse, de démodulation et de traitement des signaux en utilisant le logiciel NI LabVIEW FPGA. Prix toutes options : environ 46 000 €. [ni5]

II.1.3 Pentek

Pentek est une société américaine à renommée mondiale, spécialisée dans la conception et la fabrication de cartes destinées à l'acquisition et au traitement du signal. Constructeur de solutions intégrées FPGA et DSP, Pentek fournit également des processeurs *softcore* et propose à la vente des émetteurs et récepteurs numériques bandes larges ou étroites. La liste particulièrement longue des produits proposés est consultable à [pentek2].

II.2 SDR grand public

II.2.1 SDR avec numérisation par carte son d'une FI I/Q

Ce type de SDR nécessite quelques prérequis au niveau du PC hôte, à savoir de disposer d'une bonne carte son (CAN 24 bits, échantillonnage entre 96 kHz et 192 kHz, SNR 100 dB, entrée stéréo pour signaux I/Q), un CPU minimum 1 GHz double cœur, une mémoire vive de 2 Go ou plus, et des ports USB 2.0, FireWire (IEEE-1394) ou norme plus rapide.

II.2.1.1 FlexRadio

FlexRadio *Systems* vend trois émetteur/récepteurs de radio logicielle propriétaire s'adressant principalement au marché radioamateur : les FLEX 1500, 3000, 5000A et 5000C. Ces équipements intègrent tout le matériel radio dans un seul châssis se connectant à un ordinateur hôte via une connexion FireWire IEEE-1394a. Ils fonctionnent dans le spectre [10 kHz – 60 MHz] et utilisent des convertisseurs 24 bits 48 kHz (un comparatif est consultable à [flexradio]). Leur prix s'échelonne de 650 $ à 2 700 $.

II.2.1.2 PM-SDR

PM-SDR est un récepteur SDR dans la plage [0,1 MHz – 55 MHz], doté d'un port USB 2.0 et délivrant des signaux I/Q audio à une carte son [pmsdr]. Prix : environ 200 €.

II.2.2 SDR avec numérisation par CAN d'une FI I/Q

II.2.2.1 µWSDR

Le projet µWave SDR (µWSDR), actuellement en développement, a pour objectif de créer une SDR fonctionnant dans la bande HF. La plateforme matérielle, de taille particulièrement réduite (10 cm * 16 cm) est composée d'un frontal de traitement numérique et d'un frontal RF spécifique à chaque bande (c'est le principe d'architecture matérielle le plus employé actuellement pour concevoir une SDR). Elle comporte

notamment une interface Ethernet 100 Mbit/s, un CPU Atmel type ARM7 [atmel], un CAN AKM AK5394A 24 bits 192 kHz max utilisé à 48 kHz [akm], un CNA PCM1740E 24 bits 96 kHz max [pcm], et un peu de glue logique. Au niveau RF, l'objectif est de réaliser un frontal fonctionnant dans la bande [50 MHz – 1.4 GHz], et un autre (nom de code GeMMA) couvrant la bande [1.3 GHz – 5.6 GHz]. L'interface graphique de la µWSDR fonctionne sous Windows, Linux et Mac OS X. [µwsdr]

II.2.3 SDR avec numérisation par CAN RF et DDC à base d'ASIC

II.2.3.1 Récepteur VLF-HF RFSpace SDR-IQ

SDR-IQ est un récepteur SDR opérant dans la bande [100 Hz – 30 MHz] [sdriq]. Il se compose notamment d'un CAN 14 bits cadencé à 66,6 MHz, d'un DDC ASIC AD6620 et d'une interface USB 2.0. SDR IQ est livré avec le logiciel Moetronix SpectraVue et supporte différents schémas de modulation radioamateur (CW, SSB, etc.). Son prix est d'environ 500 $. Il existe une version plus musclée appelée SDR-IP (CAN 16 bits, FPGA Xilinx) [sdrip] mais aussi plus chère (plus de 3 000 $).

II.2.4 SDR avec numérisation par CAN RF et DDC à base de FPGA

Ce type de radio logicielle est en train de s'imposer car il concilie performances, souplesse d'emploi et prix abordable. On retrouve notamment dans cette catégorie la famille des USRP.

II.2.4.1 Heron RTG003

La société Hunt Engineering propose une SDR pouvant fonctionner en autonome ou se raccorder à un PC via une connexion USB 2.0. Cette SDR est composée d'un FPGA Xilinx XC2V1000-4, de deux CAN 12 bits 125 Méch/s, de deux CNA 14 bits 125 Méch/s et d'un DSP à 300 MHz, 32 Mo de SDRAM et 2 Mo de Flash ROM. Son prix est d'environ 3 700 £. [heron]

II.2.4.2 Perseus VLF-HF Receiver

Perseus est un récepteur SDR VLF-LF-MF-HF composé d'un CAN 14 bits 80 Méch/s, un DDC à base de FPGA et une interface USB 2.0 [perseus]. Il fonctionne dans la bande [10 kHz - 40 MHz] avec une dynamique de 100 dB et une bande passante instantanée de 10 kHz.

II.2.4.3 Quicksilver QS1R VERB

Le récepteur SDR QS1R VERB (*Versatile Receiver Board*) est composé d'un CAN Linear Technologies LTC2208 16 bits 130 Méch/s, un FPGA Altera EP3C25 Cyclone III une interface USB 2.0 [qs1r]. QS1R couvre nativement la bande de 10 kHz à 62,5 MHz et peut être utilisé jusqu'à 500 MHz avec un sous-échantillonnage. Le *firmware*, les logiciels et l'HDL du FPGA sont tous « libres ». Le QS1R coûte environ 1 000 €. Il est associé au logiciel « libre » SDRMAXII mais fonctionne aussi avec le logiciel Winrad.

II.3 USRP

L'USRP (*Universal Software Radio Peripheral*, périphérique de radio logicielle universel), conçu par Ettus Research LLC[18], est un sous-système matériel de radio logicielle (partie CAN/CNA + section numérique) à architecture « libre » (sont disponibles les schémas de brochage des cartes et le code source du FPGA) [ettus]. Il constitue l'interface entre le domaine analogique RF et un GPP, et peut donc être vu comme un frontal radio a usage général, capable de générer et de recevoir toute sorte de signaux. Il convertit en réception les ondes radio captées par une antenne en équivalent numérique exploitable par un ordinateur, et convertit en émission une onde synthétisée par l'ordinateur en signal RF.

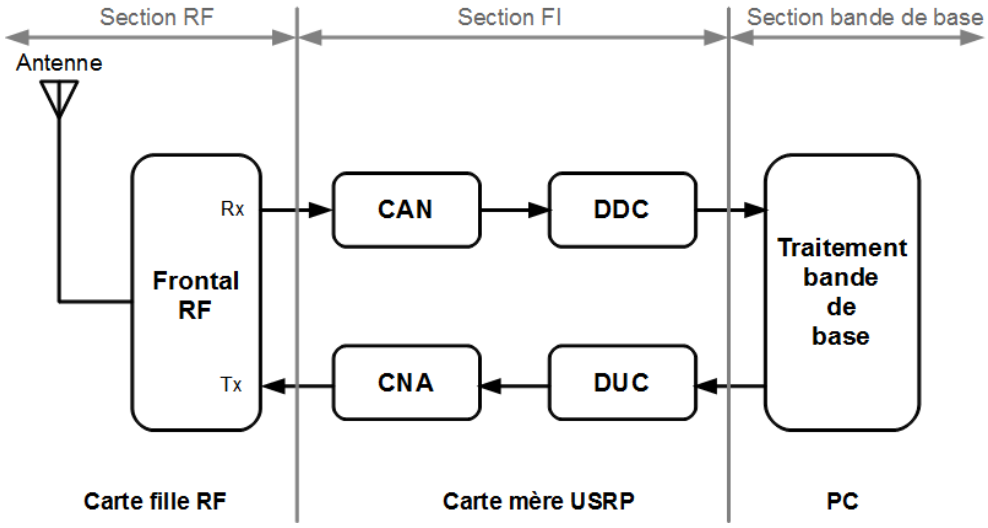

Figure 11: Architecture simplifiée d'une SDR USRP

La famille des produits USRP a été déclarée technologie de l'année 2010 par le *Wireless Innovation Forum*. Elle a été considérée comme la technologie la plus favorable au développement de la radio logicielle et de la radio intelligente sur la période

[18] National Instruments Corporation a racheté Ettus Research LLC en février 2010.

de 2005 à 2010. En produisant des frontaux radio polyvalents, bon marché et surtout « libres », Ettus Research a rendu le domaine des radios logicielles accessible à nombre de chercheurs, encouragé une nouvelle génération d'expérimentateurs radio et comblé le fossé entre la simulation et l'expérimentation. [businesswire]

Pleinement compatible avec le projet GNU Radio, l'USRP est principalement connu au travers de ses deux premières versions [ettus1] : USRP1 et USRP2. Toutes deux se présentent sous la forme d'une carte mère contenant un FPGA, un amplificateur à gain programmable, des CAN, des CNA et un port de communication pour la connecter à un ordinateur. Des cartes filles, ou frontaux RF, peuvent s'enficher sur la carte mère en fonction de la bande fréquentielle désirée, et se raccordent à une antenne adaptée. Une liste des composants des cartes mères de l'USRP1, de l'USRP2 et de quelques cartes filles Ettus est consultable en **annexe D**. Le tableau suivant résume les caractéristiques principales de l'USRP1 et de l'USRP2.

Tableau VI : Comparatif USRP1 - USRP2

	USRP1	**USRP2**
Année de sortie	2004	2008
CAN	12 bits, 64 Méch/s, SFDR 85 dB	14 bits, 100 Méch/s, SFDR 88 dB
CNA	14 bits, 128 Méch/s, SFDR 83 dB	16 bits, 400 Méch/s, SFDR 80+ dB
Bande passante RF instantanée maximale (full duplex)	8 MHz (2 CAN) 4 MHz (4 CAN)	25 MHz
FPGA	Altera Cyclone EP1C12	Xilinx Spartan 3 2000
Interface	USB 2.0 (32 Mo/s *half duplex*)	Gigabit Ethernet (125 Mo/s)
Nombre de canaux d'entrée	4 (ou 2 paires I-Q)	2 (ou une paire I-Q)
Nombre de canaux de sortie	4 (ou 2 paires I-Q)	2 (ou une paire I-Q)
Cartes filles enfichables	2 modules d'émission 2 modules de réception	1 module d'émission 1 module de réception
SRAM	Non	1 Mo
MIMO-capable	2*2	Équipement seul : non. Mais possibilité d'aller jusqu'à MIMO 8*8 en en chaînant plusieurs.
Systèmes d'exploitation supportés	Linux, Mac OS X, Windows XP, Windows 2000, FreeBSD et NetBSD	Linux, Mac OS X
Alimentation	6 V, 3A	
Coût	700 $	1400 $

II.3.1 USRP1

II.3.1.1 Présentation

Figure 12 : USRP1

Proposé par Ettus Research LLC, L'USRP1 (souvent dénommé USRP) est un sous-système matériel de radio logicielle (partie CAN/CNA + section numérique) à architecture « libre », généralement utilisé comme plateforme modulaire pour le prototypage de circuits radiofréquences. L'USRP1 constitue l'interface entre une carte RF et un PC, permettant à ce dernier de fonctionner comme une radio logicielle.

L'intérêt principal de l'USRP1 est la flexibilité de presque tous ses composants : chaque élément de la chaîne de transmission peut être modifié dans la limite de ses caractéristiques de fonctionnement. L'USRP1 se présente sous la forme d'une carte électronique, communicant avec un ordinateur par l'intermédiaire d'une connexion USB 2.0, et sur laquelle peuvent être enfichées jusqu'à quatre cartes RF filles. L'ensemble des fonctionnalités de l'USRP1 est contrôlable par le logiciel « libre » GNU Radio à l'aide des langages Python (niveau d'abstraction le plus élevé), C++ et VHDL (accès à la couche matérielle). L'USRP1 peut gérer jusqu'à deux modules d'émission et deux modules de réception. La carte mère de l'USRP1 intègre un FPGA, quatre convertisseurs analogique/numérique (CAN), quatre convertisseurs numérique/analogique (CNA) et quelques E/S analogiques et numériques. L'USRP1 dispose d'une horloge interne à 64 MHz. Il est compatible MIMO 2x2 et coûte environ 700 $. Ses performances sont limitées et plutôt orientées vers un usage de type " expérimentation " que dédiées à l'implémentation efficiente d'un standard de communication particulier.

Les signaux analogiques issus d'une carte RF sont convertis par l'USRP1 en échantillons numériques puis transposés en bande de base grâce au FPGA intégré. L'USRP1 prend ainsi en charge les opérations de conversions (CAN, CNA, DDC, DUC, décimation, interpolation[19]) et laisse au CPU les actions de traitement numérique en bande de base. Les schémas ainsi que les pilotes de l'USRP1 sont disponibles sur Internet. Son

[19] Cf. le glossaire et l'annexe B §B.6 pour une explication de la notion d'interpolation.

orientation "logiciel et matériel libre" a permis à une communauté de développeurs et d'utilisateurs de constituer une base de données de codes et de fournir de nombreuses applications pratiques tant matérielles que logicielles.

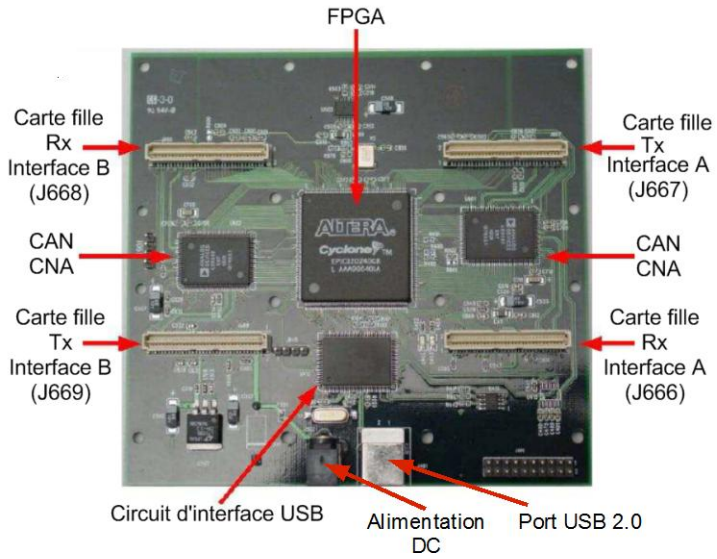

Figure 13 : Carte mère de l'USRP1[20]

La connexion USB 2.0 reliant l'USRP1 au PC limite la vitesse de transfert à 56 Mo/s [cypress], soit 2*14 Méch/s pour des échantillons sur 16 bits, permettant la gestion d'une bande spectrale d'au maximum 7 MHz par sens de transmission. D'après Ettus Research LLC, l'USRP1 est capable de traiter des signaux de largeur jusqu'à 16 MHz (dans ce cas seul un sens de transmission est possible). Ceci est obtenu grâce aux fonctionnalités de décimation/interpolation assurées par le FPGA, mais s'accompagne d'une diminution du contenu informationnel transmis. Du fait de cette limitation en bande passante, les standards tels que le 802.11b/g (canaux de largeur 20 MHz) ne sont pas exploitables avec l'USRP1.

Il est envisageable de modifier (physiquement) l'USRP1 pour lui adjoindre une connexion plus rapide que l'USB 2.0 (par exemple du Gigabit Ethernet). Il est alors possible de traiter des signaux de largeur de bande de plusieurs mégahertz si l'on utilise une carte RF Ettus (variable selon le type de carte considéré et l'emploi de signaux réels ou complexes [dboards]), voire un peu plus si on fabrique sa propre carte RF (dans ce cas la limitation est apportée par les CAN, cf. paragraphe suivant). Le schéma suivant présente sous la forme de blocs les différents constituants de l'USRP1, lesquels sont détaillés par la suite.

[20] La composition matérielle de la carte mère de l'USRP1 est fournit en annexe D.

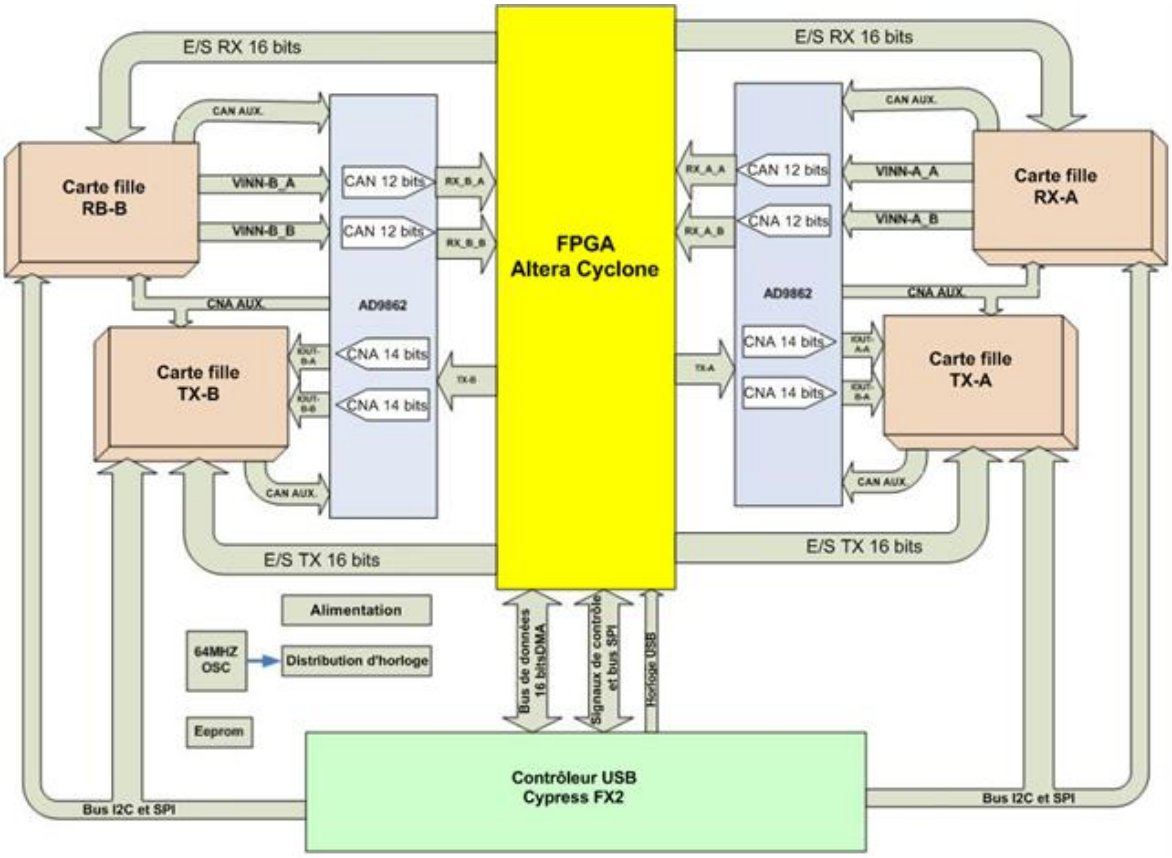

Figure 14 : Diagramme par blocs de l'USRP1[21]

II.3.1.2 Conversion analogique/numérique (CAN)

Les CAN numérisent en théorie un signal de largeur de bande de 32 MHz. Il est possible en pratique d'aller jusqu'à 200 MHz mais au prix d'un repliement spectral (*aliasing*). Et plus la fréquence d'échantillonnage est élevée, plus le rapport signal à bruit se dégrade. Il est conseillé de ne pas dépasser 100 MHz. Les CAN numérisent un signal avec une pleine échelle de 2 Vcc sous 50 Ω différentiels (soit une puissance de 40 mW, ou 16 dBm). Un PGA (*Programmable Gain Amplifier*) de gain maximum 20 dB est placé avant le CAN pour amplifier si nécessaire le signal d'entrée afin d'atteindre les 2 Vcc requis. D'autres fréquences d'échantillonnage sont disponibles : 42.66, 32, 25.6 ou 21.33 Méch/s.

II.3.1.3 Conversion numérique/analogique (CNA)

Les CNA permettent la génération de signaux analogiques de fréquence maximale 64 MHz. Chaque convertisseur peut fournir 1 Vcc sous 50 Ω différentiels (soit une puissance de 10 mW, ou 10 dBm), et est relié à un PGA de gain maximum 20 dB. Les signaux du CNA (`IOUTP_A` / `IOUTN_A` et `IOUTP_B` / `IOUTN_B`) sont en sortie de courant

[21] Adapté de [firas].

(maximum 20 mA), et peuvent être convertis en tensions différentielles à l'aide d'une résistance adaptée. Dans le cas d'un échantillonnage réel, l'USRP1 présente quatre entrées et quatre sorties de signaux RF. En échantillonnage complexe (I/Q), ceux-ci sont regroupés deux par deux. On obtient alors deux entrées complexes et deux sorties complexes.

II.3.1.4 Canaux d'entrée/sortie analogiques auxiliaires

Huit voies d'entrées analogiques auxiliaires sont connectées aux entrées de CAN 10 bits bas débit (`AUX_ADC_A1_A`, `AUX_ADC_B1_A`, `AUX_ADC_A2_A`, `AUX_ADC_B2_A`, `AUX_ADC_A1_B`, `AUX_ADC_B1_B`, `AUX_ADC_A2_B`, et `AUX_ADC_B2_B`) et consultables par logiciel. Ces CAN peuvent convertir jusqu'à 1.25 Méch/s et ont une bande passante de l'ordre de 200 kHz. Les voies d'entrées analogiques auxiliaires sont utiles pour récupérer diverses informations tels que le niveau de signal reçu (RSSI - *Received Signal Strength Indication*), la température, etc. Six canaux de sortie analogique auxiliaires son connectés à des CNA 8 bits bas débit (`AUX_DAC_A_A`, `AUX_DAC_B_A`, `AUX_DAC_C_A`, `AUX_DAC_A_B`, `AUX_DAC_B_B` et `AUX_DAC_C_B`). Ces CNA peuvent être utilisés pour fournir des tensions de contrôle (exemple : commande des amplificateurs à gain variable). En outre, il y a deux autres CNA 12 bits sigma-delta (`AUX_DAC_D_A` et `AUX_DAC_D_B`) avec filtre passe-bas externe. Les connecteurs de la carte mère de l'USRP1 (`RXA` et `TXA`) partagent quatre canaux de sortie analogique (`AUX_DAC_A_A` à `AUX_DAC_D_A`) et ont chacun deux canaux d'entrée analogiques indépendants (`AUX_ADC_A1_A` et `AUX_ADC_B1_A` pour `RXA`, `AUX_ADC_A2_A` et `AUX_ADC_B2_A` pour `TXA`). Le même principe est appliqué pour `RXB` et `TXB`. `AUX_ADC_REF` fournit quant à lui un niveau de référence pour le réglage éventuel du gain.

II.3.1.5 Ports d'entrée/sortie numériques auxiliaires

La carte mère de l'USRP1 dispose de ports de d'E/S haut débit 64 bits divisés en 32 bits pour `IO_RX` et 32 bits pour `IO_TX`. Ces E/S numériques sont reliées aux connecteurs d'interface des cartes filles (`RxA`, `TxA`, `RxB` et `TxB`). Chacun de ces connecteurs est sur 16 bits. Ces signaux peuvent être contrôlés à partir du logiciel par lecture/écriture dans des registres spéciaux du FPGA et peuvent être configurés indépendamment, soit comme entrée ou sortie numérique. Certaines de ces broches sont utilisées pour contrôler des opérations spécifiques de cartes filles installées telles que la sélection du port d'entrée RF de réception, l'alimentation des équipements d'émission/réception, etc., et peuvent également être utilisées pour le débogage des implémentations du FPGA à l'aide d'un analyseur logique.

II.3.1.6 FPGA

Les quatre canaux d'entrée/sortie numériques principaux sont reliés à un FPGA Altera Cyclone EP1C12024DC8 fonctionnant à 64 MHz. Le FPGA effectue des calculs mathématiques et adapte le taux de transfert des données au circuit d'interface USB 2.0 Cypress EZ-USB FX2 en implémentant des DDC. La description des circuits à configurer dans un FPGA s'effectue en VHDL. Le tableau suivant décrit les principales caractéristiques de l'Altera Cyclone EP1C12024DC8 et les ressources utilisées en configuration standard par l'USRP1.

Tableau VII : Ressources du FPGA de l'USRP1 utilisé en configuration standard[22]

	Capacité	Utilisés	%
Nombre d'éléments logiques (avec LUT à 4 entrées)	12060	11138	92
Nombre de LAB	1206	1182	98
Nombre de blocs RAM 128*36 bit	52	42	81
Nombre de broches d'E/S	173	173	100
Nombre de broches d'horloge	2	2	100
Nombre de boucles à verrouillage de phase (PLL)	2	0	0
Nombre de blocs CRC	1	0	0
Nombre de blocs ASMI[23]	1	0	0

Un LAB *(Logic Array Block*, bloc matriciel logique) de la famille des FPGA Altera Cyclone contient dix LE (*Logic Element*) ainsi que d'autres éléments, représentés dans la figure suivante.

[22] Adapté de [ingemarsson].
[23] ASMI (*Active Serial Memory Interface*) : bloc IP permettant de lire un flux binaire de configuration à partir d'un équipement série externe. [asmi]

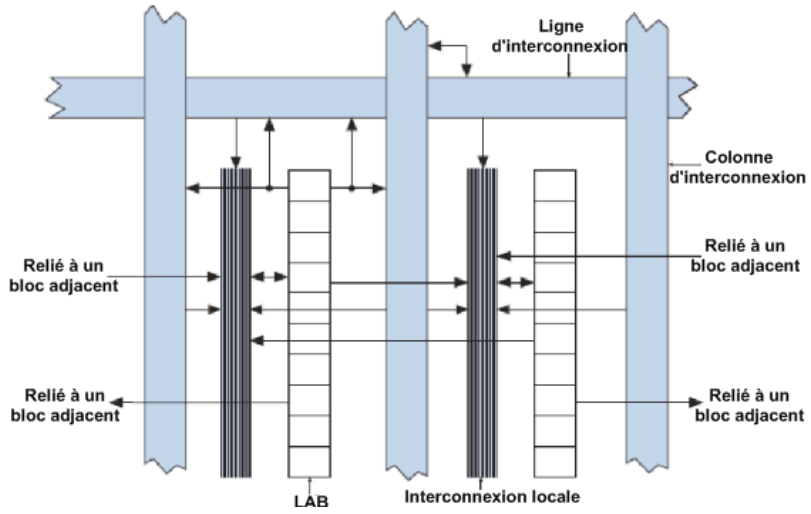

Figure 15 : Structure d'un bloc de FPGA Cyclone

Un LE comprend une table de correspondance ou LUT (*Look-up Table*) et un registre. Les blocs de RAM du FPGA sont des blocs mémoire double port 4 kilobits avec parité (4608 bits). Ces blocs fournissent de la mémoire de longueur jusqu'à 36 bits (il y a 128 mots de 36 bits) à 250 MHz.

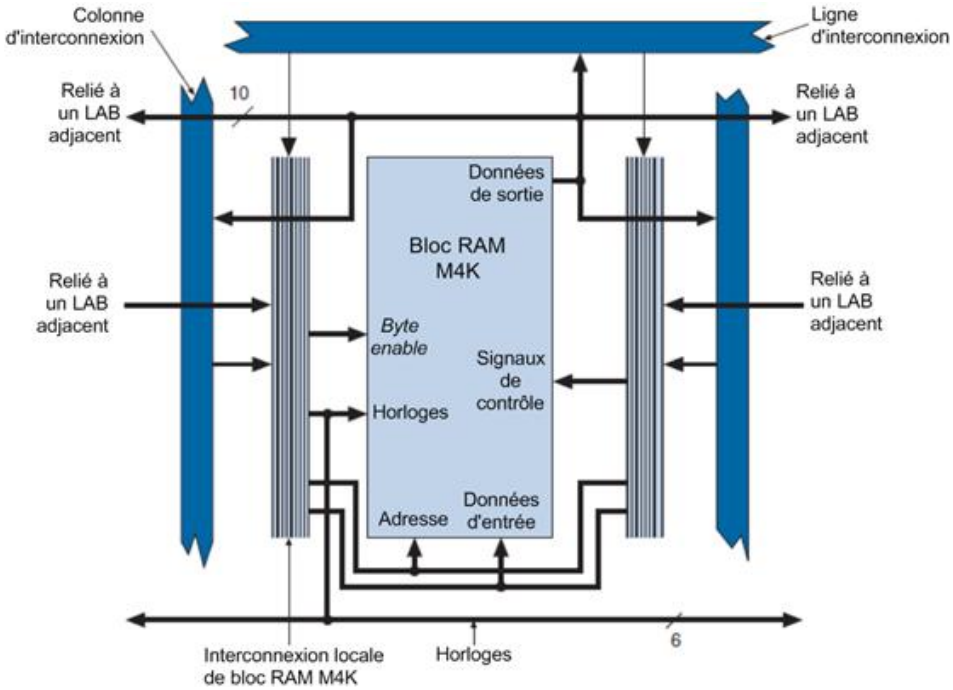

Figure 16 : Interfaçage d'un bloc mémoire dans la matrice logique du FPGA

La configuration standard du FPGA, partie réception, comprend quatre DDC réalisés à partir de filtres d'Hogenauer CIC[24] (*Cascaded Integrator and Comb*) quatre

[24] Un filtre CIC d'ordre N est composé de N intégrateurs et d'autant de blocs *comb* (correspondant à un calcul de dérivée dans le cas présent).

étages (plage de décimation [4 ; 128]), suivis d'un filtre demi bande ou HBF (*Half-Band Filter*) composé de 31 *taps*[25] (pour la mise en forme spectrale et la réjection hors-bande) et effectuant une décimation de rapport 2 (activation optionnelle). Chaque DDC transpose le signal complexe de la bande FI vers la bande de base. Cette transposition est obtenue par multiplication complexe par un OL numérique utilisant l'algorithme de Cordic. Ensuite le DDC effectue à l'aide des filtres CIC et HBF un filtrage et une décimation du signal de sorte que le débit binaire soit compatible avec la liaison USB 2.0. Chaque DDC a une entrée I (en phase) et une entrée Q (en quadrature, c'est-à-dire déphasée de 90°). La plage de décimation globale est ainsi de [4 ; 256]. Chacun des quatre CAN peut être relié à l'une des entrées I ou Q de l'un des quatre DDC grâce à l'utilisation d'un multiplexeur (MUX). Un MUX est comme un commutateur, il détermine quel CAN est connecté à quel DDC. Ce multiplexeur permet à l'USRP1 de supporter à la fois des signaux réels et complexes.

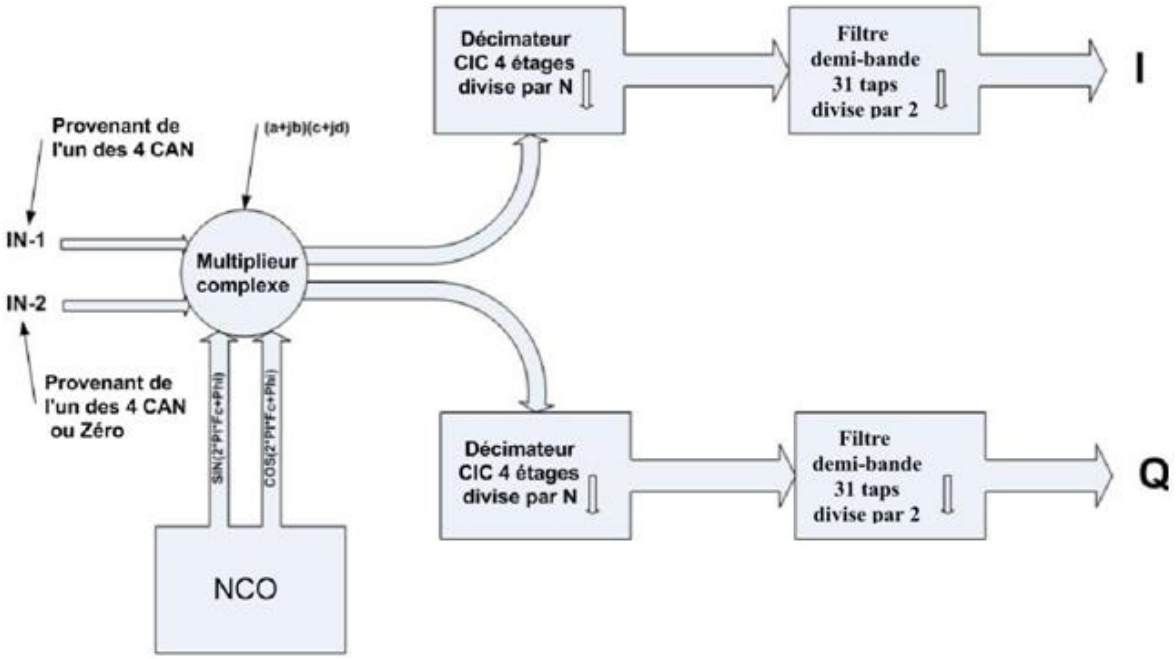

Figure 17 : Implémentation d'un DDC sur le FPGA de l'USRP1[26]

Les échantillons numériques provenant du CAN sont multipliés par une fonction sinus (respectivement cosinus) issue d'un oscillateur contrôlé numériquement ou NCO (*Numerically-Controlled Oscillator*), pour obtenir les voies I et Q. Ensuite une décimation

[25] Dans un filtre numérique à réponse impulsionnelle finie, le nombre de '*taps*' détermine la durée de la fenêtre (pas forcément rectangulaire) appliquée sur la réponse impulsionnelle du filtre numérique. Plus un filtre comporte de *'taps'*, plus sa fenêtre est grande et plus le filtre se rapproche du filtre idéal. Par contre, plus le nombre de *taps* est grand, plus le produit de convolution numérique est long à effectuer (d'où apparition d'un retard de groupe ou de phase). Un décalage temporel est ensuite nécessaire pour rendre le signal causal.
[26] Adapté de [firas].

du taux d'échantillonnage est effectuée sur chacune des voies. Un échantillon complexe de 32 bits de long (16 bits pour la voie I et 16 autres pour la voie Q) est ensuite acheminé vers le PC hôte via le port de communication (ici USB 2.0). On indique pour chaque entrée (I_0, Q_0, I_1 ... I_3, Q_3) quel CAN lui est connecté à l'aide de 4 bits (0, 1, 2, 3 ou 0xf "zéro"), soit 32 bits pour l'ensemble des huit entrées. La plupart du temps l'entrée Q de chaque DDC est positionnée à "zéro" (configuration standard du FPGA).

DDC3		DDC2		DDC1		DDC0	
Q_3	I_3	Q_2	I_2	Q_1	I_1	Q_0	I_0

Figure 18 : Représentation de la correspondance CAN/DDC

Lorsqu'il y a des canaux multiples (jusqu'à quatre), les voies sont entrelacées avant envoi sur le port USB 2.0. Par exemple, avec quatre canaux, la séquence envoyée sur le port USB serait I_0 I_1 Q_0 Q_1 Q_2 Q_3 I_2 I_3 Q_0 I_0 I_1 Q_1, …etc. De plus, tous les canaux d'entrée doivent être au même débit de données, ce qui signifie qu'ils doivent avoir subi le même facteur de décimation.

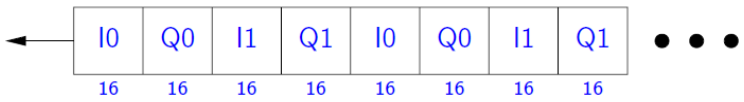

Figure 19 : Ordre de transmission des voies sur la liaison USB 2.0

En émission, les signaux I/Q bande de base sont transmis à la carte mère de l'USRP1. Le DUC interpole le signal numérique et le transpose en bande FI pour enfin l'envoyer au CNA. Les fonctionnalités DUC du circuit d'émission sont partagées entre le FPGA et les puces AD9862 qui intègrent deux filtres demi-bande décimateur d'ordre 2 (pour chaque voie) et qui intègrent également les CAN/CNA. Les seuls blocs de traitement du signal en émission implémentés par le FPGA sont les filtres CIC [hogenauer] interpolant dans la plage [1 ; 128]. La plage d'interpolation globale est ainsi de [4 ; 512]. À noter que du côté récepteur seul un filtre demi bande décimateur d'ordre 2 est implémenté dans les AD9862.

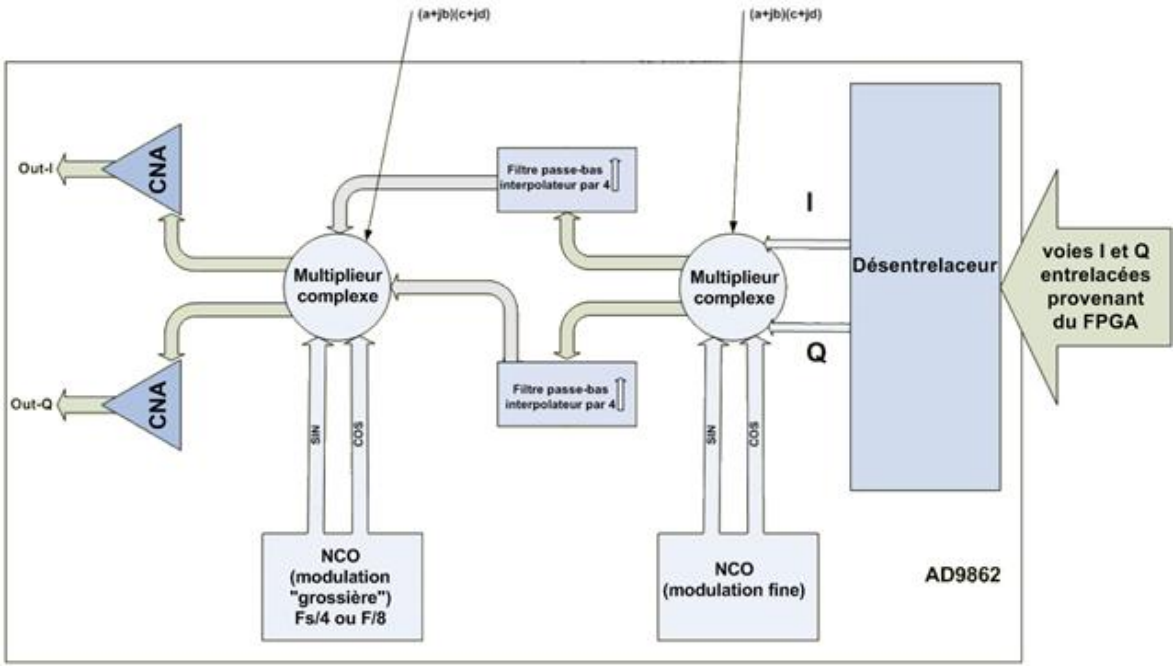

Figure 20: Implémentation d'un DUC d'AD9862[27]

S'il y a plusieurs canaux R_X (deux ou quatre), ceux-ci doivent avoir la même vitesse de transmission (c'est à dire le même taux de décimation). De même, les canaux de sortie T_X doivent avoir le même débit de données (donc le même taux d'interpolation). Notons que le taux T_X peut être différent du taux R_X. L'USRP1 peut fonctionner en *full duplex* avec des voies d'émission et de réception indépendantes, mais dans la limite du débit binaire maximal de la liaison USB 2.0. Le schéma suivant récapitule l'architecture fonctionnelle d'un USRP1.

[27] Adapté de [firas].

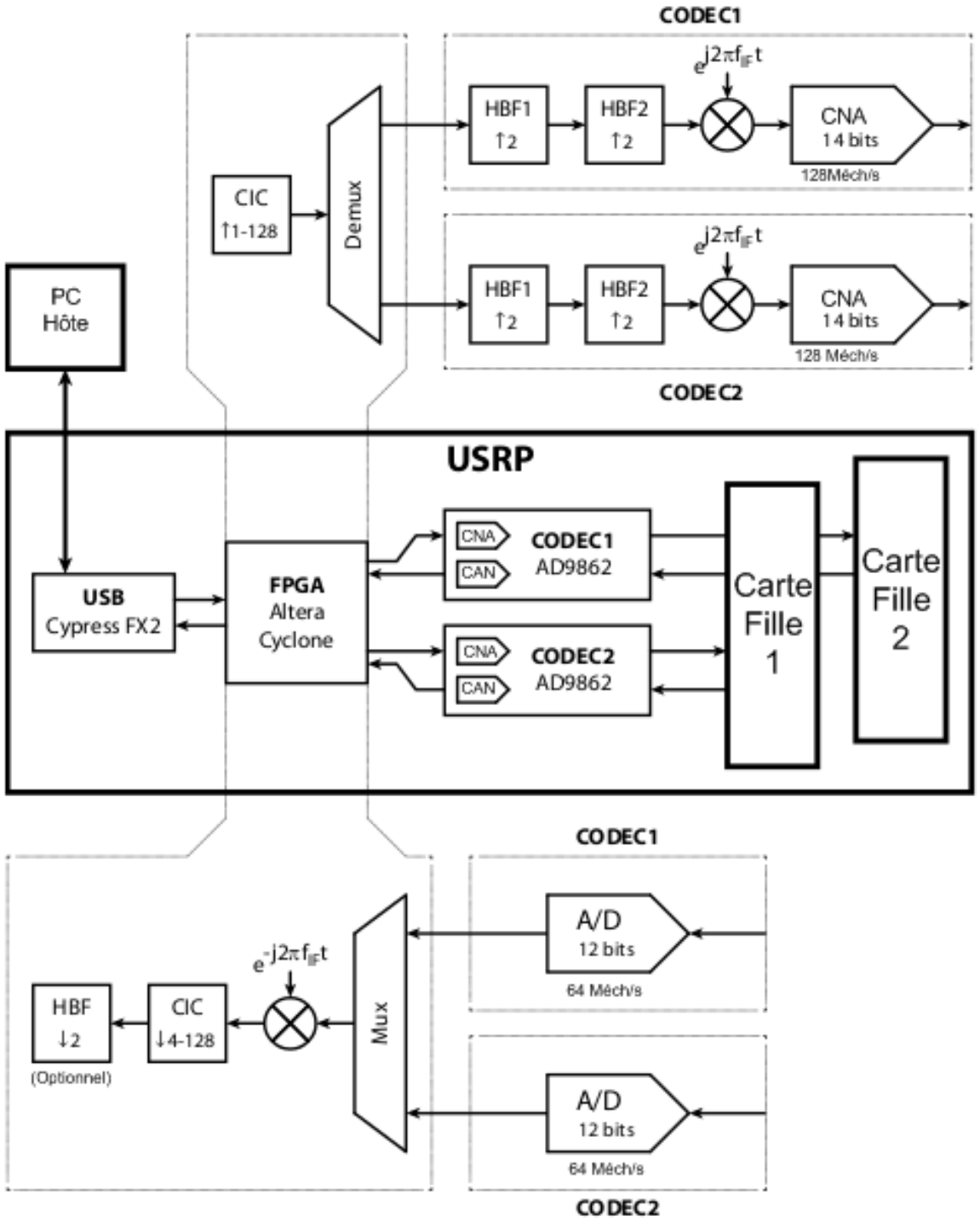

Figure 21 : Architecture fonctionnelle d'un USRP1

Comme nous pouvons le constater dans le tableau en page 44, la marge de manœuvre pour faire exécuter par le FPGA des opérations supplémentaires à celles prévues en configuration standard est faible. Il est donc peu envisageable, pour gagner en rapidité, d'effectuer d'autres traitements avant envoi sur le lien USB 2.0. La capacité de traitement du FPGA utilisé constitue l'un des principaux facteurs limitatifs de cette configuration, au même titre que la liaison USB 2.0. De plus, étant donné que la majorité

des traitements numériques des signaux est réalisée par l'ordinateur hôte, la puissance de traitement du (ou des) CPU doit également être suffisante pour ne pas devenir un facteur limitant du dispositif.

II.3.2 USRP2

Figure 22 : USRP2

L'USRP2, disponible depuis septembre 2008, est une évolution de l'USRP1, améliorant les fonctions de conversion A/N et N/A, le FPGA et le transfert des données avec l'hôte (lien Gigabit Ethernet).

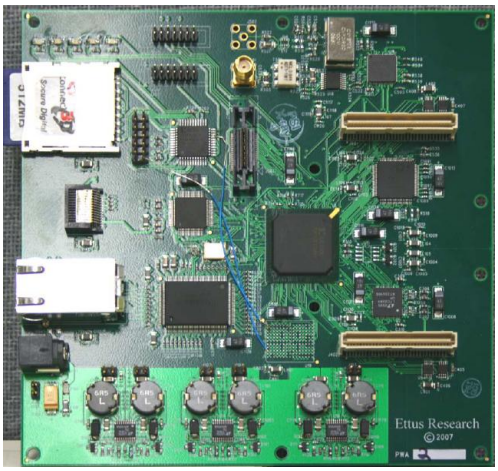

Figure 23 : Carte mère de l'USRP2[28]

L'USRP2, ne peut gérer qu'un module d'émission et qu'un module de réception. En revanche, il dispose d'un port Gigabit Ethernet permettant le traitement de jusqu'à 50 MHz de bande passante en mode full duplex (ou 100 MHz en mode simplex, avec un échantillonnage sur 8 bits au lieu de 16 bits), et 25 MHz en configuration standard. Remarquons au passage que la liaison Gigabit Ethernet, dont le débit théorique est de 1000 Mbit/s, autorise en principe une largeur de bande RF complexe de 31,25 MHz pour des échantillons sur 16 bits. Les performances des convertisseurs sont revues à la hausse par rapport à l'USRP1 : deux CAN 100 Méch/s, deux CNA 400 Méch/s (en sortie), le FPGA est plus performant (Xilinx Spartan 3) et la carte mère dispose d'un lecteur de cartes

[28] La composition matérielle de la carte mère de l'USRP2 est consultable en annexe D.

SD. Il est possible d'interconnecter plusieurs USRP2 pour former un système MIMO d'antennes (jusqu'à huit) parfaitement cohérent (l'USRP2 dispose d'un port d'extension spécifique MIMO en façade). L'oscillateur maître peut être verrouillé sur une référence externe 10 MHz, et il y a une entrée à une impulsion par seconde (1 PPS) pour les applications nécessitant un timing précis (connecteurs en façade). Le FPGA Xilinx Spartan 3 permet à des utilisateurs (expérimentés) de déplacer une partie des étapes de traitement du signal ordinairement réalisées par le PC hôte vers le FPGA (modification du *bitstream* FPGA). Dans l'USRP2, les traitements à haut taux d'échantillonnage sont réalisés par le FPGA. Les traitements à faible taux d'échantillonnage peuvent soit être réalisés par un PC, soit également au niveau du FPGA, celui-ci contenant un microprocesseur RISC 32 bits et suffisamment d'espace mémoire pour un fonctionnement en *standalone*. Le *firmware* et les données de configuration de l'USRP2 sont stockées dans une carte SD.

Le FPGA de l'USRP2 est un Xilinx Spartan 3-2000. Il est composé de 5120 CLB. Chaque CLB contient quatre blocs (ou *slices*) de deux LUT à quatre entrées. Le nombre de LUT de ce FPGA est environ 3,4 fois plus élevé que celui du FPGA utilisé dans l'USRP1. La mémoire dédiée est également trois fois plus importante. Ce FPGA implémente un microprocesseur *softcore* 32 bits AeMB qui gère la plupart des opérations internes de l'USRP2. En configuration standard l'AeMB ne réalise pas de fonctions DSP. Le tableau suivant décrit les principales caractéristiques du Spartan 3-2000 et les ressources utilisées en configuration standard par l'USRP2.

Tableau VIII : Ressources du FPGA de l'USRP2 utilisé en configuration standard[29]

	Capacité	Utilisés	%
Nombre de *slices*	20480	11104	54
Nombre de *slices* « *Flip Flop* »	40960	12657	30
Nombre de LUT à 4 entrées	40960	20212	49
Nombre de blocs RAM de 18 kbits	40	34	85
Nombre de blocs d'E/S	333	301	90
Nombre de multiplieurs 18*18	40	16	40
Nombre d'E/S d'horloge générale (GCLK)	8	6	75
Nombre de DCM[30]	4	1	25

[29] Adapté de [corgan].
[30] DCM (*Digital Clock Manager*) : utilisé pour l'élimination du décalage d'horloge, la synthèse de fréquence et le déplacement de phase à haute résolution [spartan3].

Le taux d'emploi des éléments logiques du FPGA de l'USRP2 en configuration standard laisse une certaine marge de manœuvre au niveau de l'implémentation de fonctions de traitement supplémentaires au sein du FPGA, mais le taux d'emploi des blocs de mémoire RAM (85 %) rend finalement cette marge de manœuvre assez restreinte. Le schéma suivant présente le diagramme par blocs de l'USRP2 avec FPGA en configuration standard.

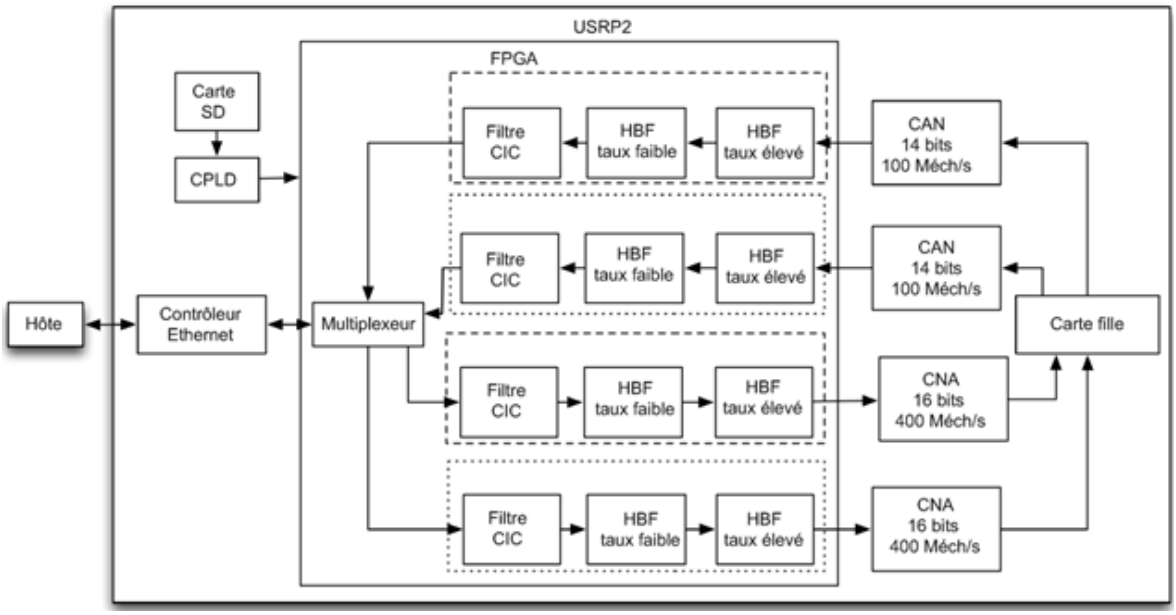

Figure 24 : Diagramme par blocs de l'USRP2

Les données I et Q transmises par le PC hôte sur l'interface Ethernet sont des mots binaires de 16 bits entrelacés. Un démultiplexeur sur le FPGA envoie ces données vers deux chaînes distinctes de filtrage. Chacun des deux DUC utilise un filtre CIC quatre étages et deux filtres HBF. Le HBF « taux élevé » comporte sept *taps* et interpole par 2. Le HBF « taux faible » comporte 31 *taps* et interpole aussi par 2. Le filtre CIC peut interpoler dans la plage [1 ; 128]. Le taux d'interpolation global est donc compris entre 4 et 512. Les données provenant du FPGA sont transmises vers le CNA à un rythme de 100 Méch/s. De même les données provenant du CAN sont transmises vers le FPGA à un rythme de 100 Méch/s. Chacun des deux DDC comporte un filtre CIC quatre étages et deux filtres HBF (mêmes caractéristiques que ceux des DUC). Les données sont ensuite multiplexées et envoyées à l'interface Ethernet. La plage de décimation globale est la même que celle de l'interpolation, c'est à dire [4-512].

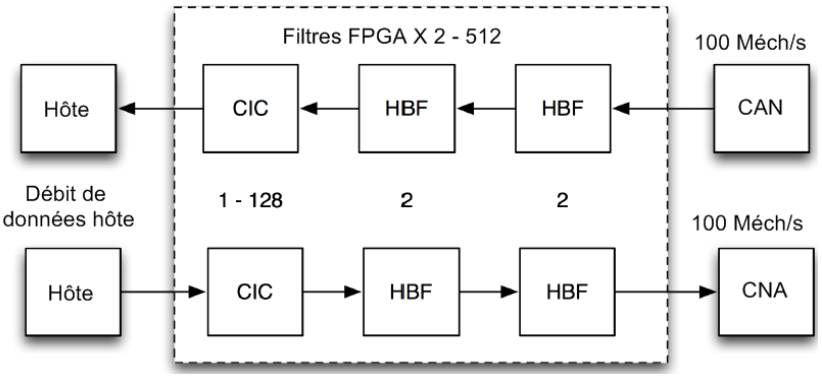

Figure 25 : Diagramme par blocs des filtres du FPGA de l'USRP2

Le débit de données entre le FPGA et le CNA (respectivement CAN) ne variant pas, le débit sur l'interface Ethernet est donc fonction du taux d'interpolation (respectivement décimation). Une valeur élevée de taux d'interpolation indique donc que le PC hôte doit envoyer moins d'échantillons. Une valeur élevée de décimation indique que le PC hôte reçoit moins d'échantillons. On a les relations :

`Taux d'échantillonnage PC hôte (en éch/s) = (taux du CAN / taux de décimation) (en éch/s)`

et

`Taux d'échantillonnage PC hôte (en éch/s) = (taux du CNA / taux d'interpolation) (en éch/s)`

A titre d'exemple un taux d'interpolation de 128 autorise un taux d'échantillonnage maximal « PC hôte » de `10^8 / 128` = 3,125 Méch/s.

Contrairement à l'USRP1, dans l'USRP2 les filtres d'interpolation et de décimation ainsi que le mélange numérique sont tous implémentés dans le FPGA Xilinx Spartan 3, tandis que la conversion numérique/analogique est assurée par un dual CNA Analog Devices AD9777 et la conversion analogique/numérique par un dual CAN Linear Technologies LTC2284, les deux étant configurés pour échantillonner à 100 Méch/s. On peut remarquer que d'après les spécifications techniques, les CNA on un taux d'échantillonnage de sortie de 400 Méch/s alors qu'ils ne reçoivent que 100 Méch/s du FPGA. En fait le composant AD9777 implémente un filtre d'interpolation d'ordre 4 au niveau analogique, simplifiant les contraintes des filtres de reconstruction analogique et améliorant la qualité des signaux transmis. Le schéma récapitule l'architecture fonctionnelle d'un l'USRP2.

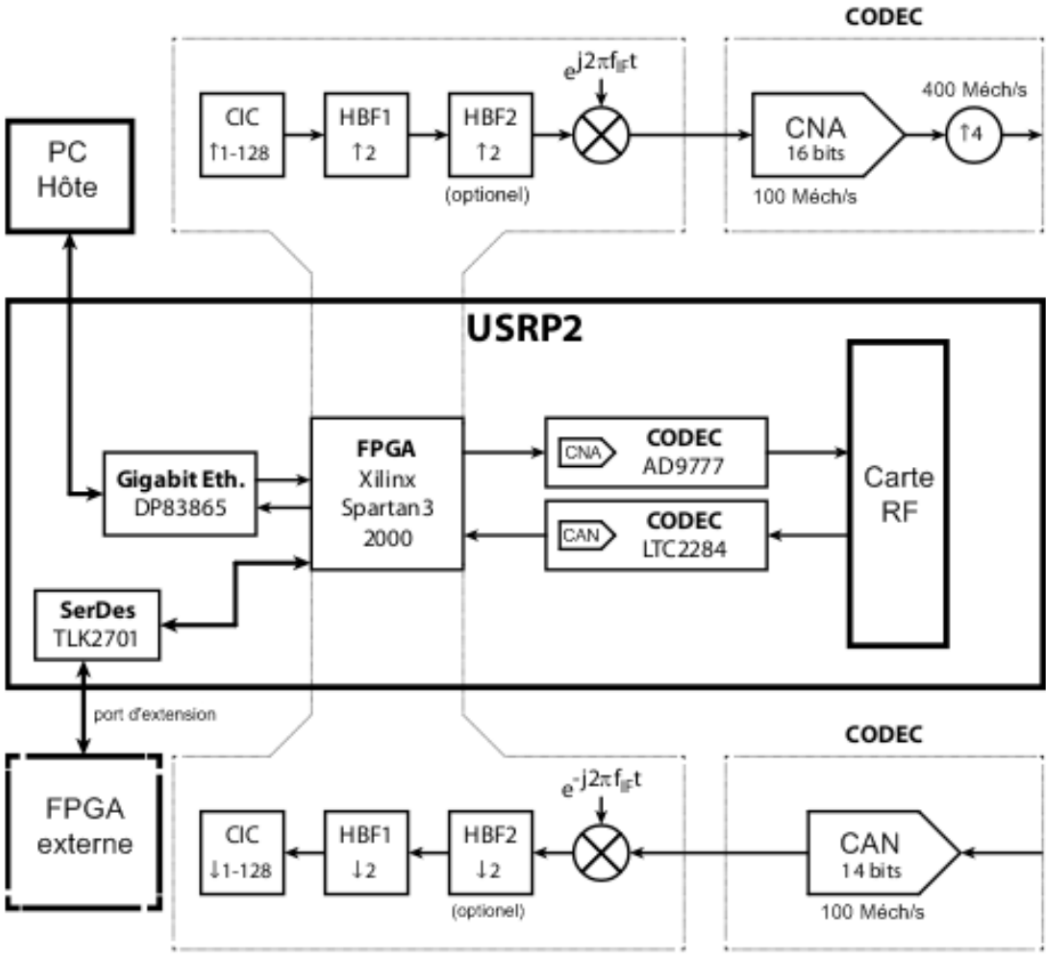

Figure 26 : Architecture fonctionnelle d'un USRP2

On remarquera une particularité intéressante de l'USRP2 : la possibilité de lui connecter un FPGA supplémentaire par l'intermédiaire de l'interface multigigabit (bande passante 2,16 Gbit/s) Texas Instruments TLK2701 [tlk2701]. Il est par exemple possible de relier l'USRP2 à un FPGA Xilinx Virtex 5 par l'intermédiaire de sa connexion RocketIO [johnston].

II.3.3 USRP1 vs. USRP2

L'USRP2 apporte de multiples améliorations par rapport à l'USRP1. La première différence notable est le lien Gigabit Ethernet avec l'hôte qui peut en théorie soutenir un débit de 125 Mo/s, 100 Mo/s en pratique. Dans le cas de l'USRP1 on dispose de 32 Mo/s. De plus le lien Gigabit Ethernet permet d'utiliser une longueur de câble plus élevée (plusieurs mètres). Les capacités de fonctionnement en MIMO de l'USRP2 sont plus importantes (8*8). Enfin, l'USRP2 comprend un mécanisme d'interconnexion haute vitesse

(2,16 Gbit/s) permettant de connecter un FPGA supplémentaire à celui de la carte mère, ouvrant la voie à la mise en œuvre de fonctionnalités temps réel.

II.3.4 UHD

Le rachat de la société Ettus Research par National Instrument impose aux produits Ettus une interopérabilité avec des solutions logicielles « libres » ou propriétaires telles que GNU Radio, LabVIEW et MATLAB/Simulink. C'est le rôle du pilote matériel universel UHD (*Universal Hardware Driver*), fonctionnant sous Linux, Windows et Mac OS, et compilable avec GCC, Clang, et Microsoft Visual C++. [uhd]

II.3.5 Nouveautés

L'USRP N210, une amélioration de l'USRP2 (dont la production est arrêtée en mars 2011) est disponible à la vente depuis décembre 2010. Les principales différences avec l'USRP2 résident dans le FPGA Xilinx Spartan 3A-DSP3400 (50 % de ressources supplémentaires) et une mémoire flash à la place du lecteur de cartes SD. L'USRP N210 fonctionne avec l'ensemble des cartes filles Ettus. Son prix est de 1 700 $. [usrpn200]

L'USRP E100, disponible depuis mi-décembre 2010, est une évolution de l'USRP1. C'est un système autonome (distribution Linux embarquée) composé d'une carte Gumstix Overo Tide embarquant un processeur Texas Instruments OMAP 3530 (composé d'un processeur ARM Cortex-A8 720 MHz avec extensions SIMD en virgule flottante, d'un DSP TMS320C64+ 520 Mhz et de 512 Mo de SDRAM), d'un lecteur de cartes µSD 4 Go, et d'un FPGA Xilinx Spartan 3A-DSP1800. L'USRP E100 fonctionne avec l'ensemble des cartes filles Ettus, dispose d'une horloge flexible et d'une interface Ethernet 10/100. Il est *a priori* possible d'y brancher un clavier et une souris. Il y a également une sortie HDMI pour brancher un écran et des entrées et sorties audio. Son prix est de 1 300 $. [usrpe100]

A terme il existera trois familles d'USRP : B (*Bus Connected*), N (*Network Connected*) et E (*Embedded*). Le premier digit correspond à la génération, le second au niveau d'options, et le troisième à une révision majeure. Sont prévus les USRP N200 (Spartan 3A-DSP1800, 1500 $) en avril 2011, et E110. L'E110 contiendra le même FPGA que le N210 (Spartan 3A-DSP3400), une horloge flexible, un bus haute vitesse entre le FPGA et l'OMAP, un lien Ethernet 10/100 avec le PC hôte, connecteurs audio In/Out,

vidéo HDMI, des fonctionnalités USB OTG[31], USB Host et USB Console, et coûtera 1 500 $. La famille des "E1x0" embarque une distribution Linux Angstrom.

II.3.6 Cartes RF Ettus

Du fait de leur flexibilité et de leur prix abordable, les USRP sont actuellement les SDR les plus populaires au sein de la communauté des utilisateurs non professionnels. Afin de proposer une solution de SDR complète Ettus Research LLC vend aussi des têtes RF, dites cartes filles, utilisables indifféremment sur USRP1[32] ou USRP2 [ettus2] [ettus3]. Les cartes filles ont pour principal objectif de recevoir et/ou de transmettre un signal analogique. Elles constituent le frontal RF de la radio logicielle, l'interface analogique entre l'antenne et la carte USRP. Elles effectuent notamment une transposition fréquentielle pour que les CAN et CNA des cartes USRP puissent travailler sur des fréquences plus basses que celles des signaux radioélectriques. Elles intègrent aussi des fonctions d'amplification et de filtrage. À noter que ce sont les cartes RF qui assurent également la modulation/démodulation I/Q. Chaque carte RF a accès via les USRP à deux convertisseurs A/N et/ou N/A (entrées des CAN pour les ports R_X et sorties des CNA pour les ports T_X), offrant en échantillonnage réel (pas de Q) deux chemins RF indépendants et deux antennes possibles. En échantillonnage complexe (I/Q) un seul signal RF par sens de transmission est supporté. Deux connecteurs SMA (*SubMiniature version* A) servent à connecter à un USRP les signaux d'entrée ou de sortie des cartes RF. Le schéma suivant présente l'architecture simplifiée typique des cartes RF utilisées avec les USRP.

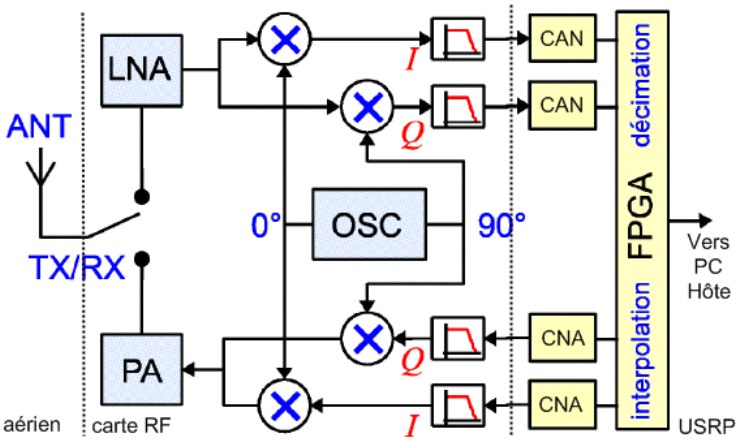

Figure 27 : Schéma simplifié de l'ensemble antenne/carte RF/USRP

[31] OTG (*On-The-Go*) : extension de la norme USB 2.0 qui permet aux périphériques USB d'avoir davantage de flexibilité dans la gestion des connexions USB.
[32] Hormis la carte SBX qui n'est pas utilisable avec un USRP1 dont le numéro de série est inférieur ou égal à 500.

Ettus Research LLC fournit trois différents types de cartes filles enfichables. Le premier type comprend les cartes BasicTX, BasicRX, LFTX et LFRX, lesquelles permettent un accès direct (via des câbles coaxiaux) au circuit de conversion A/N et N/A, autorisant ainsi l'emploi de frontaux RF différents de ceux proposés par Ettus. Les BasicRX, BasicTX, LFRX et LFTX ne disposent ni de circuits d'accord ni de gains programmables, et se décomposent en quatre sous-périphériques [dboards] :

- sous-périphérique A (respectivement B) : signal réel sur l'antenne (R/T)XA (respectivement (R/T)XB). Bande passante Basic(R/T)X : 250 MHz, bande passante LF(R/T)X : 33 MHz,

- sous-périphérique AB (respectivement BA) : signal complexe IQ (respectivement QI) utilisant les deux antennes. Bande passante Basic(R/T)X : 500 MHz, bande passante LF(R/T)X : 66 MHz

Le second type de carte RF comprend les récepteurs TVRX (basé sur un *tuner* TV analogique) et DBSRX. La TVRX (version 1) a une plage de gain en RF de -13,3 dB à 50,3 dB (dépend de la fréquence) et en FI de -1,5 dB à 32,5 dB. Le pas d'incrémentation de la fréquence d'accord est de 31,25 kHz. La DBSRX dispose de deux amplificateurs de gain variables, GC1 [0 dB – 56 dB] et GC2 [0 dB – 24 dB] et présente une bande passante instantanée variant de 8 MHz à 66 MHz. Le troisième type de carte RF comprend les émetteur/récepteurs WBX, RFX400, RFX900, RFX1200, RFX1800, RFX2200, RFX2400 et XCVR2450, couvrant au total les bandes de fréquences de 50 MHz à 2,9 GHz et de 4,9 GHz à 5,9 GHz. La WBX et les RFX disposent d'une sortie d'antenne en émission (T_X) et de deux entrées d'antenne en réception (T_X/R_X en *half-duplex* et R_X2 en *full duplex*). La WBX a un gain variable en émission de [0 dB – 25 dB] et en réception de [0 dB – 31,5 dB]. Les signaux reçus par les RFX et la WBX peuvent être amplifiés dans la plage [0 dB – 70 dB] (sauf pour la RFX400 où le maximum est à 45 dB). La WBX et les RFX ont une bande passante en émission et réception de 40 MHz. La XCVR ne supporte pas le mode *full duplex* et utilise le même OL pour les circuits d'émission et de réception. La XCVR2450 a un gain variable en émission de [0 dB – 35 dB] et en réception de [0 dB – 92,5 dB]. Sa bande passante en émission varie de 24 MHz à 48 MHz, et en réception de 15 MHz à 36 MHz.

Chaque carte fille, de conception totalement synchrone et compatible MIMO (sauf la XCVR2450), contient une EEPROM I2C (24LC024 ou 24LC025) pour s'identifier. Cela permet une configuration logicielle automatique du système en fonction de la carte fille

installée. Une EEPROM permet également de stocker des valeurs d'étalonnage comme des offsets de tension continue ou des déséquilibres I/Q. Si cette EEPROM n'est pas programmée, un message d'avertissement est affiché à chaque mise en route. Les cartes filles émettrices présentent en outre deux sorties analogiques différentielles (IOUTP_A / IOUTN_A et IOUTP_B / IOUTN_B) en sortie de courant et actualisées à 128 Méch/s. Les cartes filles réceptrices présentent deux entrées analogiques différentielles (VINP_A/VINN_A et VINP_B/VINN_B) échantillonnées à 64 Méch/s. Toutes disposent de 16 E/S numériques pour contrôler des équipements externes tels que des commutateurs d'antenne, ou pour donner accès à des signaux internes. L'ensemble de leurs fonctions est contrôlable par logiciel ou via le FPGA de la carte mère USRP. Le tableau suivant synthétise l'offre actuelle.

Tableau IX : Cartes RF Ettus[33]

Carte	Type	Fréquences	Prix	Commentaires
BasicTX	émetteur	[1 – 250 MHz]	75 $	Entrées CAN et sorties CNA directement couplées aux connecteurs SMA (impédance 50Ω) sans mélangeurs, filtres ou amplificateurs. Les BasicTX et BasicRX donnent un accès direct à tous les signaux (y compris aux bus haute vitesse 16 bits d'E/S, SPI et I2C, et aux CAN/CNA), utiles au développement de sa propre carte fille ou de son design FPGA.
BasicRX	récepteur			
LFTX	émetteur	[DC – 30 MHz]	75 $	De conception proche des BasicTX et BasicRX, les LFTX et LFRX s'en distinguent par une utilisation d'amplificateurs différentiels pour étendre la réponse en fréquence jusqu'à la composante continue, et de filtres passe-bas 30 MHz pour l'antirepliement.
LFRX	récepteur			
TVRX Version 2	récepteur	[50 – 860 MHz]	200 $ (v1 : 100 $)	Système de réception VHF/UHF basé sur un double *tuner* TV, avec une bande passante instantanée de 10 MHz et un facteur de bruit nominal de 5 dB (respectivement 6 MHz et 8 dB pour la version 1). Cette carte est compatible MIMO (mais pas la version 1). Elle est apparue en avril 2011. Les ventes de la TVRX v1 ont été *de facto* stoppées.
DBSRX Version 2		[800 – 2400 MHz]	150 $	Le DBSRX, capable d'alimenter une antenne active via le câble coaxial, présente un filtre de canal variable de 1 à 60 MHz contrôlable par logiciel. La plage de fréquences couverte permet d'accéder à de nombreuses bandes d'intérêt dont notamment : GPS, Galliléo, ISM [900-928 MHz], GSM, PCS, bandes de radioastronomie et DECT, mais pas la bande ISM [2,4 – 2,48 GHz]. Le

[33] La composition matérielle des cartes TVRX, DBSRX2, RFX900, RFX1800 et WBX est consultable en annexe D.

				DBSRX est compatible MIMO et peut alimenter une antenne active via un câble coaxial. Cette carte nécessite une modification du *bitstream* (via la carte SD) pour fonctionner avec l'USRP2.
RFX400	émetteur /récepteur	[400 – 500 MHz]	275 $	Sortie 100 mW (20 dBm), AGC 45 dB. Couvre notamment les bandes pour la TV. Cette carte n'est plus vendue depuis février 2011. Une petite modification matérielle lui permet de couvrir la bande [200- 800 MHz].
RFX900		[750 – 1050 MHz]		Sortie 200 mW (23 dBm). Synthétiseurs T_X et R_X indépendants. Couvre notamment la bande GSM 900. Modifiable en RFX1800 par changement du *firmware* et petite modification matérielle [discuss1], mais opération préférable dans l'autre sens [discuss2].
RFX1200		[1150 – 1450 MHz]		Sortie 200 mW (23 dBm). Figure de bruit : 6-10 dB [oz9aec]. Synthétiseurs T_X et R_X indépendants. Couvre notamment des bandes pour les transmissions satellites, des bandes radioamateurs, et la radionavigation.
RFX1800		[1500 – 2100 MHz]		Sortie 100 mW (20 dBm). Synthétiseurs T_X et R_X indépendants. Couvre notamment le GSM 1800 (DCS) et le DECT. Modifiable en RFX900 par changement du *firmware* et petite modification matérielle [discuss1].
RFX2200		[2000 – 2450 MHz]		Apparue fin novembre 2010. Sortie 50 mW. Permet notamment d'accéder à certaines liaisons mobiles satellites.
RFX2400		[2300 – 2900 MHz]		Sortie 50 mW (17 dBm), AGC 70 dB. Figure de bruit : 6-10 dB [oz9aec]. Synthétiseurs T_X et R_X indépendants. Couvre notamment la bande ISM (2400-2483 MHz), 802.11b/g/n et Bluetooth. Modifiable en RFX1200 par changement du *firmware* et petite modification matérielle.
XCVR2450		[2300 – 2900 MHz] et [4900 – 5900 MHz]	400 $	Sortie 100mW pour la première bande, 50 mW pour la seconde. Synthétiseur unique T_X et R_X. Couvre notamment les plages de fréquence des normes 802.11b/g/n.
WBX		[50 – 2200 MHz]	450 $	Sortie 30 à 100 mW (20 dBm). IIP2 40-55 dBm, IIP3 5-10 dBm et figure de bruit 5-6 dB [wbxrpp]. Sensibilité : -130 dBm [wbxrs]. Synthétiseurs T_X et R_X indépendants. Couvre un large spectre de fréquences dans lequel on trouve notamment celles du DBSRX plus les bandes de communications mobiles terrestres, réseaux de capteurs sans fil et normes de radiotéléphonie GSM 900, DCS 1800, et DECT. Nécessite une modification du *bitstream* (via la carte SD) pour fonctionner avec l'USRP2.
SBX		[400 MHz – 4,4 GHz]	475 $	Sortie 50 à 100 mW (20 dBm), AGC 32 dB. Synthétiseurs T_X et R_X indépendants. Contrôle de puissance d'émission. Elle est apparue en avril 2011

II.3.7 Autre carte RF compatible avec les USRP

Une entreprise s'est lancée dans la conception de cartes filles pour USRP. Il s'agit de la société EPIQ Solutions. Elle propose un récepteur RF configurable large bande, le Bitshark USRP RX (BURX). Un BURX coûte 750 $ (550 $ pour les étudiants) et est capable de recevoir dans la bande [0.3 GHz – 4 GHz] avec une bande passante instantanée de 50 MHz. La bande de réception englobe notamment celles des normes GSM (850 MHz, 900 MHz, 1800 MHz et 1900 MHz), CDMA2K/EVDO (*Evolution-Data Optimized*), UMTS (bandes I à XIV), Wi-Fi 802.11b/g, WiMAX/802.16 d/e et LTE (*Long Term Evolution*) (bandes 1 à 40). [burx]

II.3.8 GNU Radio et USRP

La GNU Radio (cf. §I.4.3) constitue le volet logiciel spécialement adapté aux USRP. Une configuration standard à base d'USRP et de GNU Radio est représentée dans le schéma suivant.

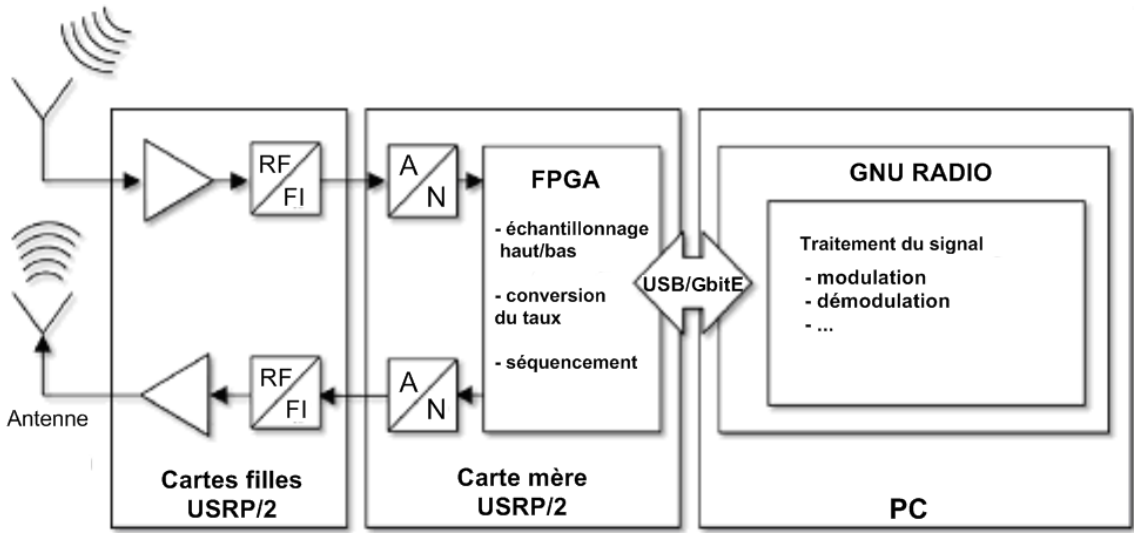

Figure 28 : Diagramme par blocs d'une radio logicielle composée d'un USRP et de la GNU Radio

La GNU Radio peut être interfacée avec d'autres plateformes matérielles mais sans garantie de fonctionnement optimal. A contrario, l'USRP peut être configuré à l'aide d'autres environnements logiciels que la GNU Radio, notamment LabVIEW, MATLAB/Simulink [mathworks2] [kit] et SCA (OSSIE [balister] [ossie] ou SCARI [scari]). Une liste non exhaustive des projets utilisant des USRP sous GNU Radio est consultable sur le site du *Comprehensive GNU Radio Architecture Network* [cgran] fondé par George Nychis.

Les avantages apportés par une plateforme GNU Radio sont multiples. Tout d'abord il s'agit d'une solution à faible coût. Comparée aux solutions professionnelles type banc de test, GNU Radio est une solution logicielle multiplateforme (en termes de système d'exploitation supporté pour l'ordinateur hôte) et gratuite (seul le matériel est payant). Ensuite l'environnement de programmation est flexible et « libre ». Certaines parties de l'implémentation matérielle sont « libres » et donc réutilisables voire modifiables. Mais il s'avère que contrairement à ce qu'affirme Ettus Research LLC, le design de ses équipements (USRP, cartes filles) n'est pas complètement « libre ». En effet, les sources du design des équipements ne sont pas disponibles. Seuls les schémas de brochage, *a priori* générés à partir du logiciel gEDA [geda] et pas nécessairement à jour, sont distribués. Le schéma des circuits imprimés et de l'implantation des composants n'est pas partagé. Le détail des spécifications techniques des cartes proposées par le fabricant [ettus] est très limité, varie selon la carte considérée et n'est en rien comparable à celui des équipements dits professionnels tels que ceux présentés au paragraphe II.1. Ensuite GNU Radio est un environnement de programmation sophistiqué nécessitant, en plus de compétences pointues en traitement numérique du signal (domaine de l'électronique), des connaissances en programmation Python et C++ (domaine de l'informatique), voire également une maîtrise des outils de simulation tels que MATLAB ou Octave. Enfin les performances de l'USRP1, et dans une moindre mesure celles de l'USRP2, ne sont généralement pas suffisantes pour réaliser des applications temps réel.

II.4 Plateformes de recherche

De nombreuses radios logicielles à vocation plus ou moins académique ont vu le jour. Une description de quelques-unes de ces plateformes est consultable en **annexe F**. Le tableau en page suivante dresse un comparatif entre les USRP et les plateformes de recherche les plus représentatives.

Tableau X : Comparatif de plates-formes SDR

	BEE2	CalRadio 1a	Chameleonic Radio	MARS	MARS 3	KUAR	NICT	SDR4ALL	SORA	USRP1	USRP2	WARP v2.0	WINC2R
Année de sortie	2005	2007	2008	2007	2009	2005	2005	2009	2009	2004	2008	2009	2005
Bande passante RF max (MHz)	20(3)	22	10	6	25	30	25	8	20	8	25	40	22
Plage(s) de fréquence (GHz)	2.4-2.5 autres	2.4-2.5	0.138-0.174 0.220-0.222 0.406-0.512 0.764-0.900 capable d'opérer dans les bandes 2.4 et 4.9 GHz	1.7- 2.5	1.7-2.5	5.25-5.85	1.9-2.4 5.0-5.3	2.4-2.5	2.4-2.5 4.9-5,875 autres(4)	Multiples (1)	Multiples (1)	2.4-2.5 4.9-5,875	2.4-2.5 4.9-5,875 autres(4)
Répartition du traitement numérique bande de base	Int.	Int.	Int	Ext.	Mixte	Int.	Int.	Ext.	Ext.	Ext.	Mixte	Ext	Ext
Architecture processeur(s)	5 FPGA	DSP	FPGA	GPP	GPP FPGA	GPP FPGA	GPP FPGA	GPP FPGA	GPP	GPP FPGA	GPP FPGA	GPP FPGA	GPP FPGA
Connectivité	Eth.	Eth.	Eth.	USB	PCIe GbEth	GbEth. PCIe	USB Eth.	USB	PCIe	USB	GbEth.	GbEth.	GbEth. PCIe
Nombre de voies RF	16	2	4	2	16	2	2	4	8	4	2	4	2
Prix (hors PC)	6000$ estimation	2499$	1200$ estimation	N/D	N/D	N/D	N/D	1000€ estimation	2700$	700$ (2)	1400$ (2)	9500$	N/D
Sources & schémas disponibles	oui	oui	non	non	non	non	non	non	oui	oui	oui	oui	non
Forces	Puissance de traitement. Communauté active	Bien documenté	Faible coût	Faible coût	BP large	BP large	Conformité à la norme	Conformité à la norme facilité d'utilisation	Support logiciel Microsoft	Intégration GNU Radio Communauté active	Intégration GNU Radio Communauté active BP large	Coopération avec Xilinx. Communauté active. Bien documenté BP large	Utilise GNU radio
Faiblesses	Prix	Plage de fréquences	BP limitée	BP limitée Plage de fréquences	Plage de fréquences	Plage de fréquences	Disponibilité limitée	BP limitée	Plage de fréquences	BP limitée	Complexité	Plage de fréquences. Prix	Disponibilité limitée

Légende:

(1) Grand choix de gammes de fréquences disponible jusqu'à 5.9 GHz.
(2) carte RF non comprise.
(3) par carte RF
(4) dans la plage globale [30 MHz – 6 GHz]

Abréviations

Int: Interne
Eth : Ethernet
BP : Bande passante
N/D : Non déterminé
Ext : Externe
GbEth : Gigabit Ethernet
PCIe : PCI Express

II.5 Voies d'amélioration des radios logicielles

L'intégration des nouvelles technologies de transmission radiofréquence telles que OFDM et WCDMA dans une plateforme SDR nécessite une augmentation des performances des interfaces, de la puissance des processeurs et des capacités de traitement du signal par les composants embarqués. L'USRP2 est un premier pas vers des SDR de nouvelle génération (FPGA performant, connexion gigabit Ethernet) qui seront en mesure de gérer ces technologies. Voici quelques améliorations possibles de l'état de l'art actuel.

II.5.1 Le défi de la numérisation haut débit

L'un des principaux objectifs de la radio logicielle est de positionner l'antenne au plus près d'un composant numérique reprogrammable. Un verrou technologique s'oppose encore à ce type de réalisation : pour couvrir une majorité de standards de transmission radiofréquence, le CAN doit être en mesure de présenter une résolution d'au minimum 17 bits et une fréquence d'échantillonnage de 10 GHz, ce qui est incompatible avec l'état de l'art actuel. Le laboratoire IMS de l'université de Bordeaux a eu l'idée de concevoir un composant analogique, le SASP (*Sampled Analog Signal Processor*) inséré entre le LNA et le CAN. Le SASP a pour rôle d'effectuer un prétraitement analogique du signal RF (récupération et numérisation de l'enveloppe) afin d'abaisser la fréquence de travail du CAN à 10 MHz [sasp].

II.5.2 Amélioration des performances des interfaces plateforme/PC

Une liaison PCI Express version 2.0 est optimisée pour le transfert de donnée en *streaming* et offre un débit utile de 1 Go/s par sens de transmission. Il est même possible de combiner plusieurs voies PCI Express pour augmenter le débit binaire. La plupart des ordinateurs disposent d'au moins deux voies sur un port d'extension. Un accès au bus graphique offre une disponibilité de 32 voies, soit 16 Go/s de données bidirectionnelles en PCIe 32x 2.0. Mieux, les spécifications de la version 3.0 de PCI Express prévue d'être commercialisée courant 2011, prévoient de doubler ces débits. Par ailleurs une liaison Gigabit Ethernet dernière génération offre jusqu'à 100 Gigabit/s de débit, ce qui est également suffisant pour la plupart des applications. On observe aussi une tendance au passage aux connexions optiques, avec les avantages que cela procure : isolation électrique et possibilité de placer les éléments RF loin de l'unité de traitement.

II.5.3 Augmentation des capacités de traitement embarqué

Le concept du placement de la majorité des traitements en embarqué (c.-à-d. hors PC) est motivé par le fait que les schémas de communication nécessitent des temps de réponse de plus en plus courts. La réalisation d'opérations de traitement du signal par des circuits embarqués spécialisés[34] type DSP et FPGA implémentant des *softcores*, permet d'envisager la mise en œuvre d'applications temps réel.

II.5.4 Divers types de processeurs au sein d'une même plateforme

Une implémentation typique de SDR contient un GPP, un DSP ou un FPGA, voire un FPGA embarquant des cœurs DSP. Les systèmes à base de FPGA offrent des performances intéressantes mais au prix d'une augmentation de la complexité de conception. Les GPP sont moins efficaces pour le traitement de la couche physique, mais excellent dans les couches supérieures et sont plus accessibles aux développeurs. Aucune solution n'est optimale, c'est pourquoi les processeurs dédiés aux applications de radio logicielle possèdent généralement une architecture hétérogène multicœur composée de FPGA(s), DSP(s) ou GPP(s) (exemple : le processeur Sandbridge Sandblaster qui contient plusieurs cœurs DSP et un processeur ARM 9). Une autre voie de recherche est l'utilisation de puces graphiques, particulièrement performantes dans le calcul à virgule flottante. Pour exemple les processeurs IBM CELL utilisés dans les Sony Playstation 3 atteignent près de 200 Gflops, puissance de calcul suffisante pour gérer n'importe quelle norme et configuration de transmission sans fil récente, à condition que cette capacité de traitement soit correctement exploitée[35].

[34] Cf. annexe B §B.9.2 à §B.9.4.
[35] Cf. annexe B §B.9.6.

Chapitre III

Radio logicielle et étude de protocoles sans fil

La liste des protocoles et types de réseaux sans fil utilisés tant au niveau national qu'international est particulièrement longue. Le tableau simplifié des allocations spectrales internationales, [tektronix], donne une illustration de cette diversité. Le rayon d'action des réseau sans fil est très variable : de quelques centimètres pour les technologies sans contact ou NFC (*Near Field Communication*) à une centaine de kilomètre pour les réseaux régionaux ou WRAN (*Wireless Regional Area Network*), pour des débits variant de quelques kilobit/s, par exemple en WCDMA en zone rural, à une dizaine de Gigabit/s, par exemple en liaison optique de type point à point ou FSO (*Free-Space Optics*). Tandis que les interfaces radio typiques telles que les adaptateurs Bluetooth ou Wi-Fi sont principalement implémentées au niveau matériel, les limitant au protocole pour lequel elles ont été conçues, les radios logicielles laissent à l'utilisateur final le soin de développer des programmes de traitement du signal afin d'émuler divers protocoles de radiocommunication et d'accéder à des fréquences arbitraires.

L'objectif de cette partie n'est pas de détailler l'ensemble des protocoles sans fil pouvant être étudiés avec des radios logicielles, ce qui représenterait un travail titanesque, mais plutôt de présenter un échantillon représentatif de protocoles pouvant être implémentés par des radios logicielles. Nous allons donc étudier quelques protocoles et réseaux sans fil ayant fait l'objet d'une implémentation radio logicielle à base de GNU Radio et d'USRP, hormis la norme DECT qui sera analysée en troisième partie dans le cadre d'une mise en œuvre pratique.

III.1 RFID

III.1.1 Présentation

La radio identification ou RFID (*Radio Frequency Identification*) est une technique de récupération et de mémorisation de données par voie aérienne sur de courtes distances (de quelques millimètres à environ quinze mètres). Des étiquettes radio ou transpondeurs (*tags*), objets de petite taille (quelques centimètres au maximum) composés d'une antenne associée à une puce électronique, captent et répondent aux requêtes radio émises par une station de base fixe ou mobile appelée interrogateur. Les RFID opèrent dans un spectre de fréquences s'étendant de quelques kilohertz à 5,9 GHz. Selon la technique utilisée le *tag*

peut être passif (l'étiquette n'intègre pas d'émetteur RF mais module l'onde issue de l'interrogateur pour s'alimenter et transmettre des informations), passif assisté par batterie (l'étiquette comporte une alimentation embarquée utilisée pour enregistrer les données lors des échanges radio) ou actif (l'étiquette embarque un émetteur RF et une source d'énergie. La communication avec l'interrogateur est de type pair à pair).

La RFID permet d'identifier des objets ou des personnes. Elle est notamment définie dans les normes ISO 10536, 1443 (cartes sans contact, portée 10 cm), 15693 (cartes sans contact, portée supérieure à 1,5 mètres), 11784/11785 et la famille des normes 18000 (étiquettes électronique). La régulation des puissances d'émission (pour la zone Europe) est précisée dans les normes ETSI EN 300-330 (fréquences entre 9 kHz et 25 kHz), EN 300-220 (fréquences entre 25 MHz et 1 GHz) et EN 300-440 (fréquences entre 1 GHz et 25 GHz). Selon l'emploi des étiquettes (la liste ci-après est non exhaustive) différentes fréquences de fonctionnement sont utilisées (en gras celles qui sont les plus utilisées) [rfidhandbook] :

- par couplage capacitif (portée jusqu'à 2 centimètres) : **125 kHz et 134,2 kHz** (LF ; ISO 18000-2 et 14223/1), technologie amenée à disparaître,

- par couplage inductif (portée jusqu'à plus de 1 mètre) : [3,155 MHz – 3,4 MHz], [6,765 MHz – 6,795 MHz], [7,4 MHz – 8,8 MHz], [**13,553 MHz – 13,567 MHz**] (HF ; ISO 18000-3, 10536, 14443 A/B, 15693 et 10373), [26,957 MHz – 27,283 MHz] : portique antivol, traçabilité d'objets, de plantes ou d'animaux, contrôle d'accès, surveillance, billetterie électronique, équipements de sécurité, gestion de stocks, instrumentation chirurgicale,

Figure 29 : *Tag* RFID LF

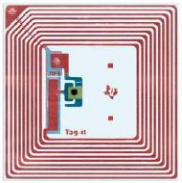

Figure 30: *Tag* RFID HF

- par propagation d'onde électromagnétique (portée: jusqu'à dix mètres, voire plus d'une centaine de mètres avec des RFID actifs) : 433 MHz (UHF, ISO 18000-7, portée jusqu'à une centaine de mètres), [860 MHZ - 960 MHz] (UHF, ISO 18000-6, 2W ERP[36] -

[36] ERP : *Effective Radiated Power*, ou puissance rayonnée effective. A ne pas confondre avec l'EIRP (*Equivalent Isotropically Radiated Power*) ou PIRE en français.

LBT[37]), [2,446 GHz - 2,454 GHz] (SHF, ISO 18000-4, portée jusqu'à plus d'une centaine de mètres), [5,725 GHz - 5,875 GHz] (SHF, ISO 18000-5) et 24.125 GHz: télépéage autoroutier, titres de transport, containers, bagages.

Figure 31 : *Tag* RFID UHF

Il y a six classes de *tags* RFID :

- classes 0 et 1 : *tags* passifs à lecture seule (de l'identifiant unique du *tag*),
- classe 2 : *tags* passifs disposant de fonctions additionnelles (écriture mémoire),
- classe 3 : *tags* passifs assistés par batterie,
- classe 4 : *tags* actifs avec communication large bande de type pair à pair,
- classe 5 : interrogateurs alimentant les *tags* de classe 0 à 3, et communiquant avec les *tags* de classe 4.

Les *tags* passifs sont largement majoritaires sur le marché actuel. Ils coûtent entre quelques centimes d'euro à une dizaine d'euros selon la technologie utilisée.

III.1.2 Aparté sur les services mobiles sans contact

L'intégration de la technologie RFID dans les téléphones est obtenue par la technologie sans contact NFC qui consiste à combiner les technologies d'identification RFID et SIM (*Subscriber Identification Module*). La carte SIM devient une puce sans contact capable d'émuler différentes cartes d'identification. Le téléphone peut ainsi rendre divers services tels que la dématérialisation de titres de transport, de moyens de paiement, de cartes de fidélité, tourisme, billettique, etc. Juniper Research et IMS Research estiment que d'ici 2014, un téléphone mobile sur six intégrera la technologie NFC. [arcepnfc]

III.1.3 Implémentations USRP/GNU Radio

III.1.3.1 Analyse d'un système de contrôle d'accès

En 2006, Henryk Plötz a utilisé un USRP1, la GNU Radio et l'outil de visualisation Baudline pour capturer et analyser le signal d'identification d'une carte RFID pour déclencher l'ouverture d'une porte dotée d'un système de contrôle d'accès RFID (porteuse

[37] LBT (*Listen Before Talk*) : un interrogateur doit vérifier la présence d'un autre signal dans sa bande de transmission avant de pouvoir l'utiliser.

120 kHz). Le processus d'identification a pu ensuite être rejoué à l'aide d'un iPod, quelques composants électroniques passifs et une bobine métallique [plötz].

III.1.3.2 Étude de l'EPC Gen2

L'EPC (*Electronic Product Code*) *Class*-1 *Generation*-2 (ou Gen2), notamment utilisé dans les passeports, permis de conduire et chaînes d'approvisionnement américains, est un standard RFID spécifié en 2004 dans la norme ISO 18000-6c et opérant dans la bande [860 MHz - 960 MHz]. Un transpondeur RFID EPC Gen2 est en principe lisible jusqu'à environ dix mètres d'un interrogateur. Début 2010, à l'aide d'un IM-ME (jouet de messagerie instantanée pour enfants), quelques amplificateurs, un USRP2 et une implémentation GNU Radio d'un lecteur/sondeur Gen2 [gnugen2], le chercheur américain Chris PAGET est parvenu à augmenter cette portée à 150 mètres pour un budget inférieur à 1 000 $, et affirme que cette portée peut être nettement plus importante (quelques kilomètres) avec des moyens conséquents. Durant la même période, deux personnels du *Department of Computer Science and Engineering* de l'Université de Washington ont utilisé un USRP2 pour surveiller (capture de signaux, décodage) un trafic RFID EPC Gen2 avec un taux de réussite de 99 % sur une distance de 3 mètres, actions qui n'étaient jusqu'à présent réalisables que par des équipements de tests particulièrement onéreux (plus de 50 k$) [Buettner].

III.2 802.15.4 / ZigBee

III.2.1 802.15.4

Le 802.15.4 (norme IEEE) est une couche protocolaire de niveau Liaison de données (niveau 2 dans le modèle OSI) destinée aux réseaux sans fils personnels à faible consommation énergétique, portée et débit (LR WPAN - *Low Rate Wireless Personal Area Network*). En Europe les plages de fréquence utilisées sont les bandes sans licence ISM 868,3 MHz (1 canal, 20 kbit/s) et [2405 MHz – 2480 MHz] (16 canaux, 250 kbit/s). La bande située à 2,4 GHz, sur laquelle les émetteurs/récepteurs 802.15.4 sont le plus souvent déployés, est découpée en canaux de 5 MHz avec une fenêtre spectrale de 2 MHz. La fréquence centrale des canaux est calculée avec la formule :

$$F_c(k) = 2405 + 5*(k - 11) \text{ MHz}$$

, où k est le numéro du canal (valeur comprise entre 11 et 26). Le schéma suivant montre l'occupation spectrale du 802.15.4 comparée à celle du 802.11 (constituant une source d'interférence potentielle).

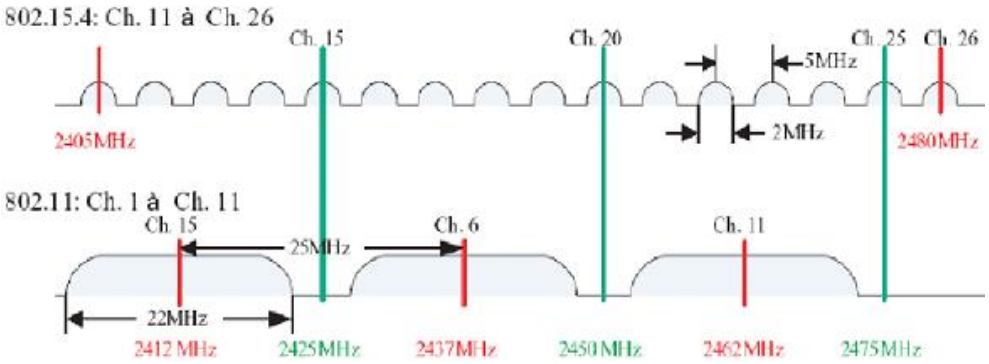

Figure 32 : Comparaison de l'occupation spectrale du 802.11 et du 802.15.4

Les données transmises sont d'abord converties en symboles de 4 bits, puis mélangées sur une séquence (*chip*) de 32 bits à un débit de 2 Mchip/s. Cette séquence est ensuite modulée en OQPSK (*Offset Quadrature Phase-Shift Keying* - déplacement de phase en quadrature à décalage), modulation utilisant une transition de phase d'au maximum de 90 degrés entre un symbole et le suivant. Étant donné que l'OQPSK transporte deux bits par symboles, le débit en symboles par canal est de 1 Msymbole/s. L'information est codée sur une porteuse par étalement de spectre à séquence directe ou DSSS (*Direct Sequence Spread Spectrum*). Cette technique permet une meilleure immunité au brouillage et le partage d'une fréquence porteuse par plusieurs liaisons (accès multiple par répartition de code), au détriment d'une largeur spectrale plus importante. La structure d'une trame 802.15.4 ou PPDU (*Physical Protocol Data Unit*) est représentée dans le schéma suivant. Elle peut embarquer de 0 à 104 octets de données utiles.

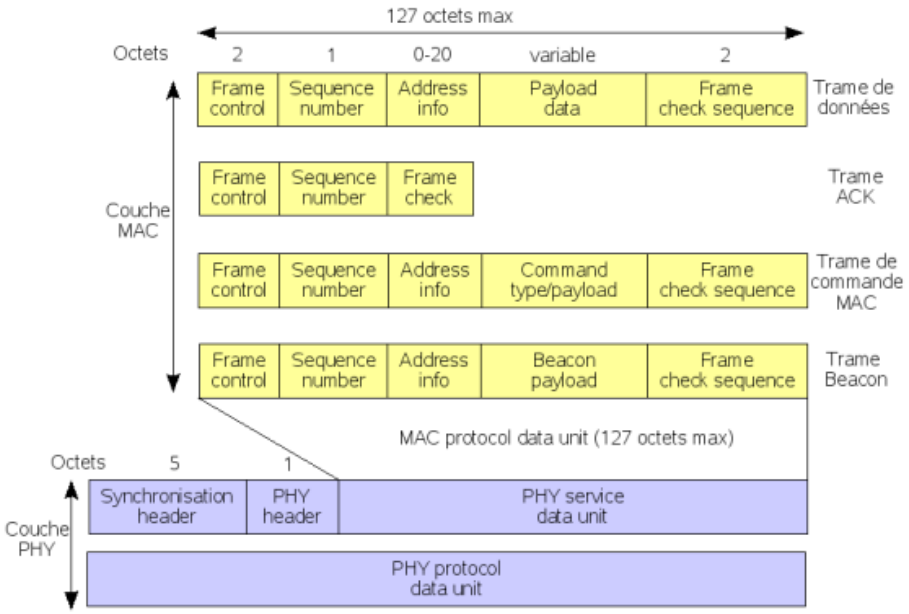

Figure 33: Format d'une trame 802.15.4

Il existe quatre types de trame : la trame de données, la trame ACK qui permet de garantir à l'expéditeur que sa trame a été reçue sans erreur, la trame de commande MAC qui permet le contrôle et la configuration à distance des nœuds par le coordinateur PAN et la trame de balisage (*beacon frame*) pour la transmission des adresses et la synchronisation des nœuds. A cela s'ajoutent deux méthode d'accès au canal : sans (CSMA/CA - *Carrier Sense Multiple Access - Collision Avoidance*) ou avec trame de balisage (GTS - *Guarantee Time Slots*). Le contrôle de l'accès au canal s'effectue par envoi de trames de balisage à intervalles réguliers (multiple de 15,38 ms, jusqu'à 252 s).

La trame MAC de données ou MPDU (*MAC Protocol Data Unit*) est composée, en plus de la charge utile, de deux octets de contrôle de trame ou FCF (*Frame Control Field*) spécifiant l'environnement réseau et quelques paramètres importants, d'un numéro de séquence sur un octet pour permettre au récepteur de vérifier que tous les paquets transmis ont été reçu, des adresses source et destination, de la charge utile, et enfin d'une séquence de contrôle de trame ou FCS (*Frame Check Sequence*) qui permet au destinataire de vérifier que le paquet reçu n'a pas été endommagé (CRC sur le MPDU). Cette trame MAC est annexé à un en-tête de synchronisation et un champ de longueur de trames (sur 7 bits, ce qui signifie que la MPDU a une longueur maximale de 127 octets) permettant au récepteur de reconnaître et de décoder de façon fiable le paquet reçu.

Différents protocoles de niveau supérieur utilisent le 802.15.4 et sa couche MAC : *Wireless* HART, ISA-SP100, IETF IPv6 – LoWPAN, DigiMesh (réseaux maillés) et le plus connu : ZigBee.

III.2.2 ZigBee

ZigBee est un standard de communication sans fil se reposant sur le 802.15.4 pour les couches basses et spécifiant les couches de niveau supérieur. Son principal objectif est de créer une topologie réseau permettant à de petites radios de communiquer entre elles sur de courtes distances. C'est une alternative à Bluetooth, moins chère et plus simple (deux fois moins cher et dix fois moins de code que le Bluetooth). Le ZigBee présente une vitesse de transfert plus faible (250 kbit/s), un rayon d'action de 100 mètres et peut gérer 2^{16} nœuds (contre 7 pour le Bluetooth). De par son faible prix de revient et sa très grande autonomie énergétique (plusieurs années), le ZigBee se retrouve dans les environnements embarqués, capteurs domotiques, contrôles industriels, réseaux de capteurs ou WSN (*Wireless Sensor Network*), applications militaires [orfidee], applications médicales (suivi

d'indicateurs physiologiques), télécommandes, détecteurs de fumées et d'intrusion, réseaux de distribution de l'électricité intelligents (s*mart grids*), localisation en temps réel et robotique. Les équipements conformes au standard sont certifiés par l'Alliance ZigBee, sont théoriquement interchangeables et peuvent communiquer ensemble. À savoir que nombre de vendeurs d'équipements ZigBee ne sont pas certifiés mais respectent la partie communication du standard. La version 1.0 a été ratifiée en décembre 2004. Il existe actuellement deux spécifications, le ZigBee 2007 et le ZigBee FR4CE. ZigBee utilise les couches physiques et MAC du 802.15.4 et intègre une structure de réseautique, de routage et de sécurité (gestion de clé et authentification).

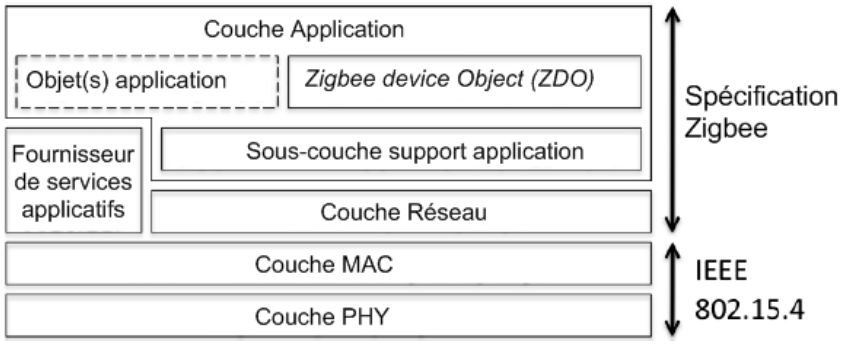

Figure 34 : Pile de protocoles 802.15.4/ZigBee

Les réseaux ZigBee sont en étoile ou maillés. Deux types de dispositif peuvent participer à un réseau :

- le FFD (*Full Function Device*), pouvant assurer trois rôles : coordinateur de réseau personnel ou PAN (*Private Area Network*), routeur ou dispositif relié à un capteur (plus petite fonction possible, appelé dispositif de terminaison),

- un RFD (RFD *: Reduced Function Device*) : dispositif de terminaison prévu pour des applications simples (signaler l'état d'un capteur, contrôler l'activation d'un actionneur).

Le coordinateur initie et contrôle le réseau. Il stocke des informations sur le réseau et agit notamment comme centre de confiance en étant le dépositaire des clés de sécurité. Le routeur étend l'aire de couverture du réseau, contourne de manière dynamique les obstacles et fournit des voies de secours en cas de congestion du réseau ou de défaillance du dispositif. Le dispositif de terminaison peut transmettre vers ou recevoir un message d'un coordinateur ou un routeur. Un FFD peut dialoguer avec des RFD et des FFD, tandis qu'un RFD dialogue avec un FFD uniquement. Une communication s'effectue sur un seul canal physique. Un module est associé au PAN par son coordinateur. Le coordinateur PAN choisit un identificateur de réseau unique sur 16 bits ou 64 bits.

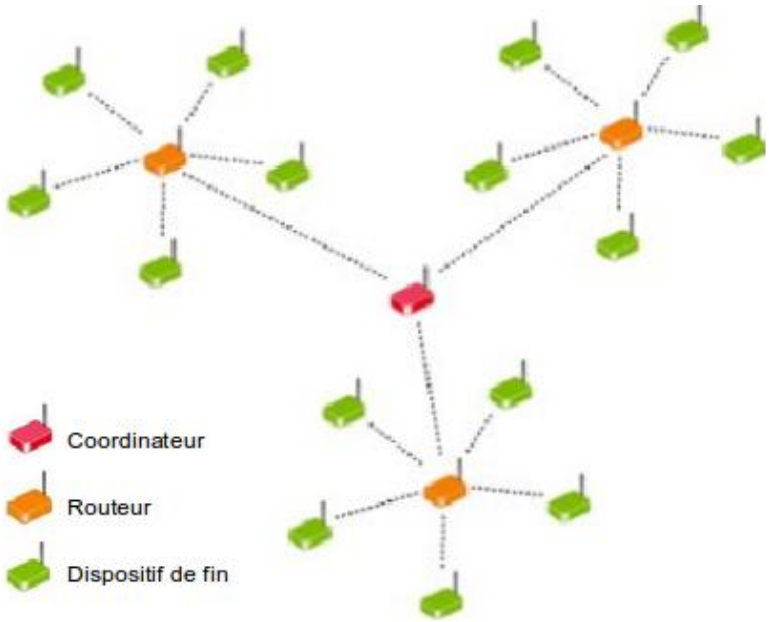

Figure 35 : Topologie d'un réseau ZigBee

III.2.3 Implémentations USRP/GNU Radio

III.2.3.1 Implémentation d'un émetteur/récepteur 802.15.4

En févier 2008, Stephan Knauth de l'université de Lucerne (Suisse) a présenté une implémentation de transmetteur 802.15.4 (pour un seul canal) sous USRP1 et GNU Radio, dont notamment un démodulateur OQPSK [knauth].

III.2.3.2 Projet UCLA

En novembre 2006 et en septembre 2007, Thomas Schmid, Tad Dreier et Mani B. Srivastava de l'Université de Californie ont présenté des travaux prouvant la faisabilité de communications de deux émetteurs à base d'USRP1/GNU Radio (l'un émettant à 430 MHz, l'autre à 2,4 GHz) implémentant les couches PHY et MAC 802.15.4, avec des détecteurs 802.15.4 du commerce (Mica2, MicaZ et Telos B) [schmid1] [schmid2]. Le code est « libre » et disponible à [uclazigbee]

En 2008, Leslie Choong et Mikhail Tadjikov, également de l'Université de Californie, ont essayé de décoder deux canaux 802.15.4 à l'aide d'un USRP1 mais sont parvenus au même résultat que Knauth, c'est-à-dire le décodage d'un seul canal, cette limitation étant causé par le goulet d'étranglement généré par le lien USB 2.0 reliant l'USRP1 à l'ordinateur hôte de la GNU Radio. [tadjikov]

En mars 2009, Leslie Choong a été en mesure, avec un USRP2, de démoduler en simultané cinq des seize canaux 802.15.4 de la bande ISM 2.4 GHz [choong]. Le traitement du signal relatif à la démodulation a été implémenté en GNU Radio et l'analyse

des paquets a été réalisée à l'aide d'une version modifiée du logiciel Wireshark. Il a été constaté que le PC utilisé était assez puissant pour démoduler quatre canaux, mais pas cinq, que l'architecture est facilement modifiable pour gérer les 16 canaux de la norme mais à condition de choisir un lien PCI Express à 1 Go/s et un traitement parallèle assuré par au moins deux processeurs Intel Core i7 (ou équivalent).

III.2.3.3 Implémentation d'une communication full duplex sur un même canal

En septembre 2010, Jung Il Choi, Mayank Jain, Kannan Srinivasan, Philip Levis et Sachin Katti de l'université de Stanford ont présenté les résultats d'une implémentation *full duplex* du protocole 802.15.4 sur une plateforme composée de deux USRP1, de quatre RFX2400 et de la GNU Radio, et en utilisant une technique d'annulation d'interférence d'antenne basée sur l'emploi de deux antennes d'émission pour une antenne de réception [mobicom10]. Les performances obtenues atteignent 92 % de celles d'un système *full duplex* idéal.

III.3 802.11

III.3.1 Présentation

L'IEEE 802.11, ou par abus de langage le Wi-Fi[38], est un ensemble de normes décrivant les caractéristiques des couches basses (physique et liaison de données) d'un réseau local sans fil ou WLAN (*Wireless Local Area Network*) à haut débit (jusqu'à 540 Mbit/s pour le 802.11n) sur un rayon de quelques dizaines de mètres en intérieur à plusieurs centaines de mètres en extérieur, essentiellement dans la bande ISM 2.4 GHz, mais aussi dans la bande des 5 GHz (802.11a/p).

Le standard 802.11 propose trois principales couches physiques : Infrarouge (obsolète), FHSS (*Frequency Hopping Spread Spectrum*) et DSSS *(Direct Sequence Spread Spectrum*), ainsi que des déclinaisons ou améliorations : HR (*High-Rate*) DSSS, ERP-PBCC (*Extended Rate Physical Layer – Packet Binary Convolutional Code*), OFDM, DSSS-OFDM et ERP-OFDM [std80211]. En FHSS, le 802.11 utilise une modulation GFSK (*Gaussian Frequency Shift Keying*) avec un étalement de spectre par saut de fréquence dans la bande ISM 2,4 GHz. Il divise cette bande en 79 canaux de 1 MHz et propose 78 séquences de saut en fréquence possibles (à un rythme d'un saut tout les 300 ms). Le DSSS utilise une modulation par déplacement de phase différentiel avec

[38] Du nom de l'organisme chargé de maintenir l'interopérabilité entre les équipements implémentant du 802.11 : Wi-Fi Alliance.

étalement de spectre à séquence directe également dans la bande ISM 2,4 GHz. Il divise cette bande de fréquences en quatorze canaux (dont treize sont utilisés en Europe) de 22 MHz (il y a donc recouvrement, sauf pour les canaux 1, 6 et 11), n'effectue pas de saut et peut utiliser deux schémas de modulation : DBPSK (déplacement de phase binaire, 1 Mbit/s) et DQPSK (déplacement de phase quadratique, 2 Mbit/s) avec un code de Barker.

La couche liaison de données est composée de la couche LLC (*Logical Link Control*) et de la couche MAC (*Media Access Control*). La couche MAC implémente les protocoles CSMA/CA (*Carrier Sense Multiple Access with Collision Avoidance*) et RTS/CTS (*Request To Send/Clear To Send*), protocole optionnel qui permet de réserver le canal sur lequel on souhaite transmettre.

Il existe deux modes de mise en réseau : le mode infrastructure, où les utilisateurs équipés d'une carte Wi-Fi accèdent au réseau filaire via un point d'accès ou AP (*Access Point*), et le mode *ad hoc* ou IBSS (*Independent Basic Service Set*) où les utilisateurs communiquent directement entre eux sans point d'accès ni réseau filaire. L'ensemble constitué d'un point d'accès et des postes mobiles s'y connectant se dénomme BSS (*Basic Service Set*). Un ensemble de plusieurs BSS forme un ESS (*Extended Service Set*). Les différentes normes 802.11 ne présentent pas les mêmes caractéristiques (modulations, débits, portées, etc.). Le tableau suivant synthétise les caractéristiques des principales normes 802.11 actuellement utilisées en Europe. Un récapitulatif de l'ensemble des standards, amendements et recommandations 802.11 est consultable à [wgpt80211].

Tableau XI : Caractéristiques de la couche physique (PHY) des principales normes 802.11 utilisées en Europe

Protocole 802.11	Fréquence (GHz)	Codage	Modulation	Débit nominal (Mbit/s)	Débit max. (Mbit/s)	Portée en intérieur (m)	Portée en extérieur (m)
Legacy	2,4 GHz	FHSS DSSS	2GFSK / 4GFSK DBPSK / DQPSK	1	2	~25	~75
a	5	OFDM	BPSK QPSK MAQ-16 MAQ-64	25	54	~25	~75
b	2,4	HR/DSSS	DBPSK DQPSK CCK	6,5	11	~35	~100
g	2,4	ERP-OFDM DSSS HR-DSSS	BPSK QPSK MAQ-16 MAQ-64	25	54	~25	~75
n	2,4	HT-OFDM		200	540	~50	~125

La norme originale (802.11 *legacy*), apparue en 1997, est qualifiée d'obsolète pour les déploiements GSM actuels mais est encore utilisée par certaines entreprises qui se sont équipées avec les premiers équipements Wi-Fi et n'ont pas suivi les évolutions. Ce mode permet un débit de 1 Mbit/s (en 2GFSK) ou 2 Mbit/s (en 4GFSK).

Le 802.11b utilise une extension du DSSS appelée HR/DSSS, qui emploie en plus des modulations DBPSK et DQPSK la technique de codage CCK (*Complementary Code Keying*), évolution du code de Barker basée sur l'utilisation de codes complémentaires multiphases permettant d'atteindre des débits de 5,5 Mbit/s ou 11 Mbit/s.

Le 802.11a utilise la bande 5 GHz et la technique OFDM (*Orthogonal Frequency Division Multiplexing*). L'OFDM divise la bande [5,15 GHz - 5,35 GHz] en huit canaux de 20 MHz contenant chacun 52 sous-canaux de 312,5 kHz. Les données sont transmises sur plusieurs sous-porteuses à l'aide de codes orthogonaux (pour éviter les interférences en cas de chevauchement). Le débit proposé est variable (1,5 Mbit/s à 54 Mbit/s) selon le type de modulation utilisé (BPSK, QPSK, MAQ-16 ou MAQ-64), le ratio de correction d'erreur FEC (*Forward Error Correction*) utilisé (1/2, 2/3 et 3/4) et la largeur des canaux (5, 10 ou 20 MHz).

Le 802.11g est une application de l'OFDM dans la bande des 2,4 GHz. Le débit proposé est variable (de 1 Mbit/s à 54 Mbit/s, adaptation aux caractéristiques du canal de propagation) selon le codage (DSSS, HR/DSSS, ou ERP-OFDM) et la modulation utilisée (BPSK, QPSK, MAQ-16 ou MAQ-64).

Le 802.11n utilise à la fois les bandes 2,4 GHz et 5 GHz (il est rétro-compatible 802.11a et 802.11b) en HT-OFDM (*High-Throughput OFDM*, ou OFDM haut débit), et s'appuie notamment sur la technologie MIMO pour augmenter le rapport signal à bruit, et *in fine* le débit binaire [80211n].

III.3.2 Implémentations USRP/GNU Radio

III.3.2.1 Implémentation de la couche MAC IEEE 802.11

En octobre 2010, le laboratoire de recherche Uwicore de l'Université Miguel Hernández de Elche (Alicante) présente une implémentation de la couche MAC IEEE 802.11 (avec une expérimentation en 802.11a), entièrement configurable et modifiable [agullo]. Cette couche MAC, implémentée en Python selon le modèle de machine à état proposé par Cisco [cisco], intègre la fonction de coordination distribuée ou DCF (*Distributed Coordination Function*), variante améliorée de la méthode d'accès CSMA/CA

qui permet d'éviter les collisions lors d'une transmission par ralentissement aléatoire après chaque trame (*back-off*). La plateforme utilisée est composée d'un USRP2, d'une Carte RF Ettus XCVR2450, et de la GNU Radio et de Wireshark s'exécutant sous Linux avec un PC doté de 2 Go de RAM et d'un microprocesseur Intel Core 2 cadencé à 2 GHz. Les résultats mettent en lumière le fait que même si le taux d'échantillonnage de l'USRP2 est suffisant pour supporter les débits requis par la norme 802.11a, les temps de traitement logiciel des couches MAC et PHY ne permettent pas d'atteindre les performances des équipements commerciaux (l'étude précise qu'une augmentation des ressources processeur permettrait de réduire ces temps de traitement, mais ne donne pas d'ordre de grandeur).

III.3.2.2 Choix d'un schéma de modulation

Dans sa thèse [kushal] Kushal Y.SHAH a cherché à estimer la complexité calculatoire de fonctions de traitement du signal mises en œuvre par une radio logicielle (plateforme USRP et outils logiciels GNU Radio). Pour cela il s'est focalisé sur le protocole 802.11b et a implémenté différents schémas de modulation (GMSK, DBPSK, DQPSK en émission/réception et aussi QAM en émission). Ont notamment été utilisés les outils de simulation/développement MATLAB et Simulink, ainsi que l'outil de contrôle de performance système Oprofile. Il s'avère que les schémas de modulation sophistiqués sont préférables (meilleurs rendements) car ils délivrent plus de données en moins d'instructions. Mais ceci est obtenu au détriment d'un taux d'erreur binaire plus élevé et une consommation de puissance instantanée plus importante (plus grand nombre d'instructions par seconde). Le choix d'un schéma de modulation se fera donc en fonction des exigences de performance de l'application ainsi que des ressources énergétiques disponibles.

III.3.2.3 Encodeur de trames OFDM compatible 802.11a/g/p

Le centre de recherche en télécommunication de Vienne [ftw] a développé sous GNU Radio un encodeur capable de générer des trames conformes aux standards IEEE 8002.11a, g et p. Son rôle est de générer à partir du SDU de la couche MAC une trame modulée en OFDM en représentation bande de base numérique complexe exploitable par l'USRP2. [ofdmtx]

III.3.2.4 Autres tentatives d'implémentation du 802.11

La plateforme Hydra développée par l'Université du Texas d'Austin est une plateforme de test de transmissions sans fil à saut de fréquence utilisée pour étudier le 802.11n en MIMO [hydra]. Elle est composée d'un frontal USRP1 et d'un PC qui exécute

les couches Réseau, MAC et PHY à l'aide de trois logiciels : routeur modulaire Click, GNU Radio et IT++.

Le projet ADROIT (*Adaptive Dynamic Radio Open-source Intelligent Team*) a également implémenté la couche PHY et une partie de la couche MAC du standard 802.11b sur un USRP2 avec un fonctionnement exclusif en émission ou réception [adroit]. Hamed Firooz a proposé une implémentation où le désétalement est réalisé par le FPGA de l'USRP2 au lieu du PC hôte (implique une modification du code du FPGA Altera) [firooz]

III.4 GSM

III.4.1 Présentation

Le GSM (*Global System for Mobile Communication*[39]) est une norme numérique de seconde génération (dite « 2G ») pour la téléphonie mobile élaborée par l'ETSI au cours des années 80 et 90 et qui a connu une ascension fulgurante en nombre d'utilisateurs depuis. Acteur majeur de la téléphonie mobile mondiale, la norme GSM est utilisée dans 219 pays ou territoires. Au deuxième quadrimestre 2009, la GSM Association a dénombré plus de 3,4 milliards d'usagers du GSM [gsma] (à comparer aux 1,3 millions d'abonnés en 1994). Plusieurs extensions de la norme GSM ont été définies, principalement pour augmenter le débit binaire, dont notamment l'HSCSD (*High Speed Circuit Switched Data*), le GPRS (*General Packet Radio Service*) et l'EDGE (*Enhanced Data rates for GSM Evolution*). EDGE est le standard actuel GSM de 2,75ième génération, et a pour particularité, outre de fournir des débits plus élevés, d'opérer sur divers réseaux de données tels que Internet. Deux principaux types de communications sont proposés par le GSM : la téléphonie et la transmission de données. Ainsi qu'une variété de services : téléphonie classique, SMS, fac-similé, boîte vocale, transfert d'appel, etc.

III.4.2 Architecture (simplifiée) d'un réseau GSM

Les communications GSM sont basées sur un système cellulaire, c'est-à-dire que chaque région couverte est divisée en zones appelées cellules. Ce concept de périmètre géographique permet la réutilisation de fréquences. Une cellule correspond généralement à la région couverte par une station de base ou BTS (*Base Transceiver Station*) identifiée par un numéro à quatorze chiffres, le CGI (*Cell Global Identification*). La taille d'une cellule est d'autant plus petite que la densité surfacique des usagers du réseau est élevée. Le

[39] Historiquement, GSM signifiait « Groupe Spécial Mobile ».

téléphone portable ou station mobile (MS, *Mobile Station*) choisit une station de base en fonction de la puissance des signaux reçus (il choisira celle pour laquelle il aura la meilleure réception). Il est composé d'un terminal mobile (ME – *Mobile Equipment*) identifié par un code unique IMEI de 15 chiffres[40] (*International Mobile Equipment Identity*) vérifié à chaque utilisation, et d'une carte à puce SIM contenant dans sa mémoire différentes informations telles que :

- le code IMSI[41] (*International Mobile Subscriber Identity*) sur 15 chiffes (ou moins) identifiant l'abonné ainsi que les services auxquels il a droit,

- le code TMSI (*Temporary Mobile Subscriber Identity*), identifiant temporaire transmis au MS par le réseau et remplaçant l'IMSI pour assurer l'anonymat des utilisateurs sur l'interface air,

- des clés de chiffrement (clé secrète Ki, clé de session Kc),

- les réseaux interdits, la région de repérage courante, etc.

Une région de repérage ou LA (*Location Area*) est un groupe de cellule dans lequel on localise un abonné. Chaque LA est associée à un contrôleur de station de base ou BSC (*Base Station Controller*) dont le rôle est de gérer les ressources radio (canaux, *handover*,...) des stations de base qui lui sont rattachées. L'ensemble "BTS+BSC" constitue le sous-système radio ou BSS (*Base Station Subsystem*) dont le rôle est de gérer la ressource radio au cours des transmissions radioélectriques. Plusieurs BSC sont reliés à un commutateur de service mobile ou MSC (*Mobile Switching Center*) dont le rôle est de gérer les appels ainsi que tout ce qui est lié à l'identité des abonnés, leur enregistrement et leur localisation. Un module de transcodage ou TRAU (*Transcode Rate and Adaptation Unit*) est généralement interfacé entre le BSC et le MSC pour convertir l'encodage vocal RPE-LPC (*Regular Pulse Excited Long-term Prediction Code*, 13 kbit/s) de l'interface air en encodage vocal PCM *(Pulse Code Modulation*, 64 kbit/s) de l'interface « terre ». Chaque MSC est relié à :

- Un registre des abonnés locaux ou HLR (*Home Location Register*), base de données (une par fournisseur d'accès) contenant les informations sur les abonnés appartenant à la région desservie par le MSC (dont leur position courante). Le HLR

[40] Sur la plupart des téléphones GSM, le code IMEI peut être obtenu en entrant la séquence *#06#

[41] L'IMSI est constitué de trois champs : le MCC (*Mobile Country Code*) constitué de trois chiffres et définissant le pays, le MNC (*Mobile Network Code*) constitué de deux chiffres et indiquant le réseau, et le MSIN *(Mobile Subscription Identification Number*) constitué d'au maximum dix chiffres et identifiant l'abonné.

contient notamment l'association entre les IMSI et les numéros de téléphone ou MSISDN (*Mobile Subscriber ISDN*) ;

- Un registre des abonnés visiteurs ou VLR (*Visitor Location Register*), base de données interne contenant des informations sur les abonnés dits « de passage ». Ces informations sont transmises une seule fois par le HLR de rattachement de l'abonné et ne sont effacés que lorsque ce dernier éteint son appareil ou quitte la région du MSC courant ;

- Un commutateur d'entrée de service mobile ou GMSC (*Gateway MSC*), interface entre le réseau cellulaire et le réseau téléphonique publique ;

- Un centre d'authenticité ou AuC (*Authentication Center*), base de données protégée contenant une copie de la clé secrète inscrite sur la carte SIM de chaque abonné, clé utilisée pour vérifier l'authenticité de l'abonné et aussi pour chiffrer les données envoyées ;

- Un registre d'identification d'équipement ou (EIR – *Equipment Identity Register*) contenant la liste des codes IMEI (donc des terminaux) valides.

- Une unité de transfert GSM (GSM *Internetworking Unit*), interface réseau vers divers réseaux supportant divers services de données (RNIS, RTCP,...).

L'ensemble constitué par le MSC et les équipements gravitant autour constitue le sous-système réseau ou NSS (*Network SubSystem*). Il assure l'établissement des appels et la gestion de la mobilité intercellulaire des terminaux. Un NSS contrôle plusieurs BSS. Le BSS et le NSS sont contenus dans un PLMN (*Public Land Mobile Network*), réseau d'un opérateur GSM particulier sur un territoire donné. Le tout est également muni d'un système d'exploitation et de maintenance (O.S.S, *Operation Sub-System*), par lequel l'opérateur administre son réseau. Une passerelle (GMSC - *Gateway Mobile Switching Centre*) assure le routage des communications entre PLMN ou entre un PLMN et le RTCP.

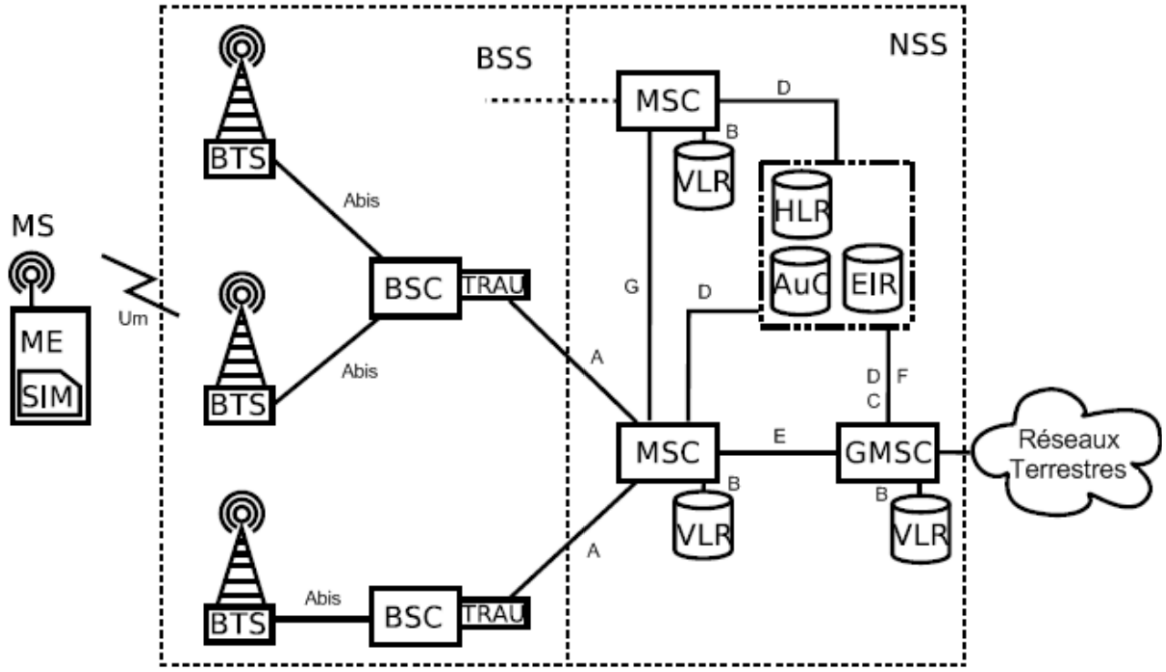

Figure 36 : Architecture d'un PLMN

Plusieurs interfaces sont définies au sein du réseau GSM. Celles qui relient le terminal mobile au réseau fixe (interfaces Um, Abis, A et E) intègrent à la fois des canaux pour le trafic (voie, données) et des canaux de contrôle (données de signalisation, métadonnées). Parmi celles-ci, une peut être exploitée par une radio logicielle : l'interface air (Um interface).

III.4.3 Interface radio

III.4.3.1 Allocation des fréquences

En Europe, la norme GSM a connu deux générations : le GSM-900 et le GSM-1800 ou DCS (*Digital Communication System*). Les deux sont actuellement employées. Chaque communication entre MS et BTS utilise deux canaux physiques (un par sens de transmission) situés dans des bandes de fréquences distinctes. Plusieurs techniques d'accès sont utilisées : accès multiple à répartition dans l'espace (SDMA – *Space Division Multiple Access*) du fait du concept cellulaire, à répartition en fréquence (FDMA – *Frequency Division Multiple Access*) et dans le temps (TDMA – *Time Division Multiple Access*). Le tableau suivant indique les principales caractéristiques des générations GSM utilisées en Europe :

Tableau XII : Principales caractéristiques (interface radio) des générations GSM utilisées en Europe

	GSM 900	GSM 1800
Bande spectrale - Liaison montant (MS → BTS)	935 à 960 MHz	1805 à 1880 MHz
Bande spectrale - Liaison descendante (BTS → MS)	890 à 915 MHz	1710 à 1785 MHz
Écart duplex (ou *offset*) (espacement entre les canaux d'un couple)	45 MHz	95 MHz
Nombre de canaux physiques (multiplexage FDMA)	124	374
Largeur des canaux physiques	200 kHz	200 kHz
Multiplexage TDMA (nombre de canaux logiques par canal physique)	8	8
Nombre de canaux logiques	992	2992

III.4.3.2 Multiplexage fréquentiel (FDMA)

Pour le GSM 900, chaque bande de 25 MHz contient 124 fréquences porteuses espacées de 200 kHz, et chacune est identifiée par un numéro correspondant à un numéro de canal comme suit :

```
fn = 935 + (0,2 * n)
```

, pour n allant de 0 à 124, pour la voie descendante. Les fréquences de la voie montante sont obtenues par ajout d'un écart duplex de -45 MHz.

Pour le GSM 1800, chaque bande de 75 MHz contient 374 fréquences porteuses également espacées de 200 kHz, et identifiées comme suit :

```
fn = 1805 + (0,2 * (n - 512))
```

, pour n allant de 512 à 885, pour la voie descendante. Les fréquences de la voie descendante sont obtenues par ajout d'un écart duplex de -95 MHz.

III.4.3.3 Multiplexage temporel (TDMA)

Chaque porteuse constitue un support dont l'utilisation est répartie suivant des intervalles de temps appelés *slots* (créneaux), qui accueillent chacun un élément de signal radioélectrique appelé *burst*. La durée d'un *slot* en GSM 900 est fixée à (75/130) ms, soit environ 576,9 µs. Huit *slots* consécutifs constituent une trame dont la durée est de 8 * 576,9 = 4,6152 ms. Un canal physique (dédié à un usager) est ainsi constitué par la répétition périodique d'un *slot* dans la trame TDMA à une fréquence donnée. Les concepteurs du GSM ont prévu la possibilité d'allouer à un usager un *slot* toutes les deux

trames (demi débit). On considère aussi les multitrames (durée : 120 ms ou 235 ms), les super trames (6,12 s) et les hyper trames (environ 3h30), selon les relations suivantes :

`Une hyper trame = 2048 super trames = 2048 * 51` (pour les canaux de trafic, ou 26 pour les canaux de contrôle) `multitrames = 2048 * 51 * 26 trames TDMA` (soit 2715648 dans tous les cas).

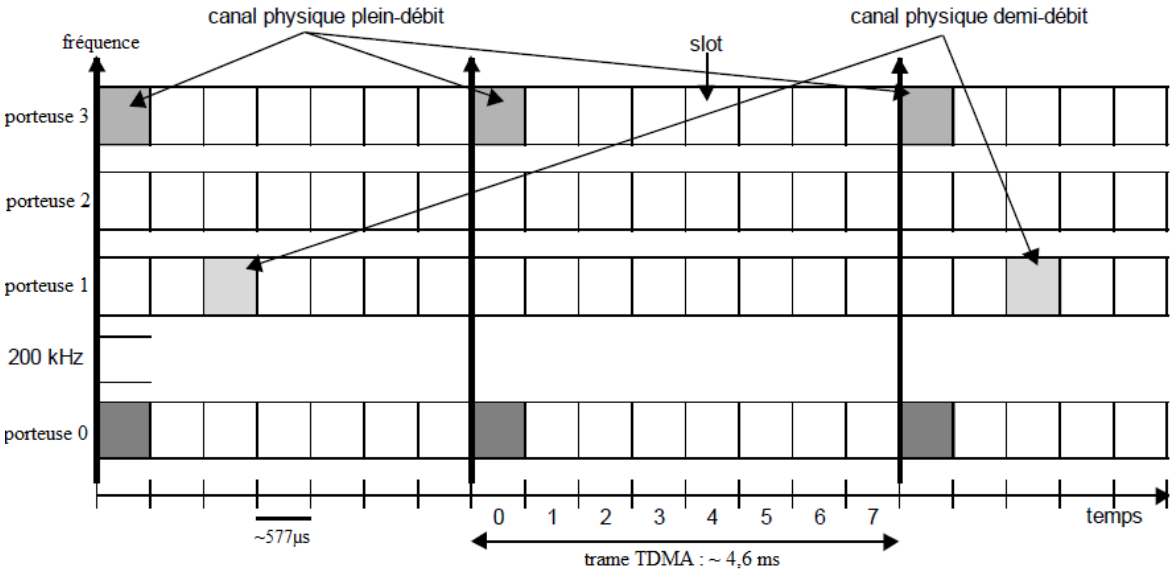

Figure 37 : Canaux physiques GSM simplex plein et demi débit

III.4.3.4 Saut de fréquence lent

L'option de saut de fréquence lent ou SFH (*Slow Frequency Hopping*) est utilisée par l'interface radio GSM pour lutter contre les interférences et n'est activée que lorsque la charge du réseau est importante. Elle consiste à changer de fréquence à chaque trame TDMA selon une séquence cyclique ou pseudo aléatoire générée par un algorithme défini dans la norme. Le saut de fréquence est reconnu par la station mobile à partir de paramètres diffusés par la BTS lors de l'allocation d'un canal de transmission. Un canal physique est identifié par un numéro de *slot* (entre 0 et 8, dans une trame TDMA) et un numéro de porteuse (ou de loi de saut de fréquence si le SFH est activé).

III.4.3.5 Chaîne de transmission

Le synoptique suivant représente les phases successives de transformation de l'information source (exemple de la parole) dans les circuits d'émission et de réception GSM.

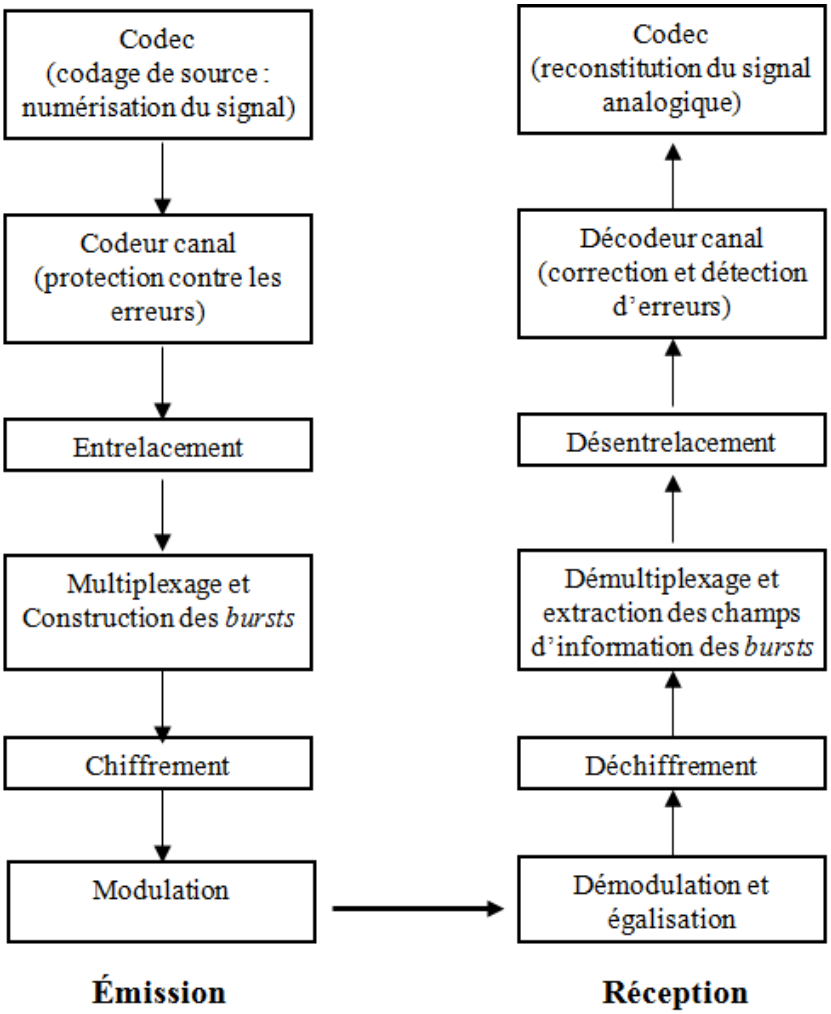

Figure 38 : Chaîne de transmission numérique du GSM

Remarques

- Codage de source : l'algorithme de codage de la parole utilisé en GSM est le RPE-LPT (*Regular Pulse Excitation – Long Term Prediction*). Il transforme des segments de 20 ms de parole en blocs de 260 bits (et inversement en réception), ce qui correspond à un débit de 13 kbit/s.

- Le codage canal utilisé est le codage NRZ (*No Return to Zero*). Il est associé à un codage en bloc avec ajout d'un bit de parité, ainsi qu'avec un codage récurrent via l'algorithme de Viterbi.

- L'entrelacement consiste à répartir des blocs de 464 bits selon une méthode prédéfinie.

- Le *burst* : la structure générale d'un *burst* comporte une séquence d'apprentissage, des bits de données et quelques bits supplémentaires. Un *burst* a une durée élémentaire de

577 µs. Chaque *slot* dans lequel il prend place a une "durée" de 156,25 bits. Il existe quatre types de *burst* en GSM :

- le *burst* normal, qui transporte les messages,
- le *burst* de synchronisation, qui contient des informations sur la localisation et les fréquences utilisées,
- le *burst* d'accès, envoyé par les mobiles lorsqu'ils veulent entrer en contact avec le réseau,
- le *burst* de correction de fréquence,
- le *burst* de bourrage (*dummy packet*) qui est placé dans les espaces vides s'il n'y a pas de donnée à envoyer.

Le format d'un *burst* normal est donné sur la figure suivante :

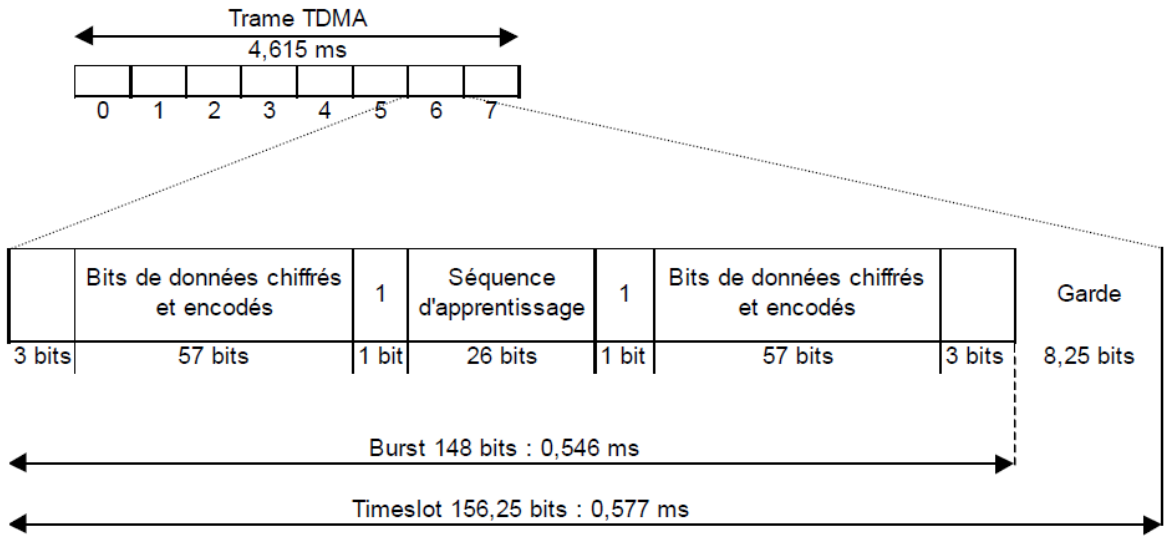

Figure 39 : Structure d'un *burst* normal

On remarque qu'il y a une période de garde de 8,25 bits (soit 30,5 µs) correspondant à la différence de durée entre un *burst* et un *slot*. On peut remarquer aussi la position centrale de la séquence d'apprentissage. Le chiffrement/déchiffrement est assuré par un « ou exclusif » de 114 bits utiles avec une séquence pseudo aléatoire générée à partir du numéro de trame et d'une clé de communication, préétablie via la signalisation. La modulation utilisée dans le GSM pour porter le signal à haute fréquence est la modulation GMSK (*Gaussian Minimum Shift Keying*) avec un produit BT[42] de 0,3. Le

[42] Cf. page 115 pour une explication du produit BT.

débit binaire est de 270 kbit/s. Cette modulation introduit un déphasage de ±π/2 pour la transition des symboles binaires. Le rôle du filtre gaussien est de rendre les transitions de phase moins brutales.

III.4.3.6 Canaux logiques

Pour assurer la qualité des liaisons radioélectriques, le GSM prévoit diverses fonctions de contrôle (choix d'une BTS, contrôle de la communication, gestion du *handover*, etc.) par le biais d'informations introduites au sein même des flux de parole transmis, d'où la notion de canaux logiques. Ceux-ci permettent la gestion des différentes phases d'une liaison radio, que ce soit en communication ou à l'état de veille. Un canal logique est formé par un ensemble de *slots* transportant des informations de contrôle, et prenant place au sein des trames TDMA selon une périodicité déterminée. On définit alors la structure multitrame comme la succession d'un *slot* donné sur des trames TDMA successives formant le canal physique. Le schéma qui suit illustre le principe de multitrame.

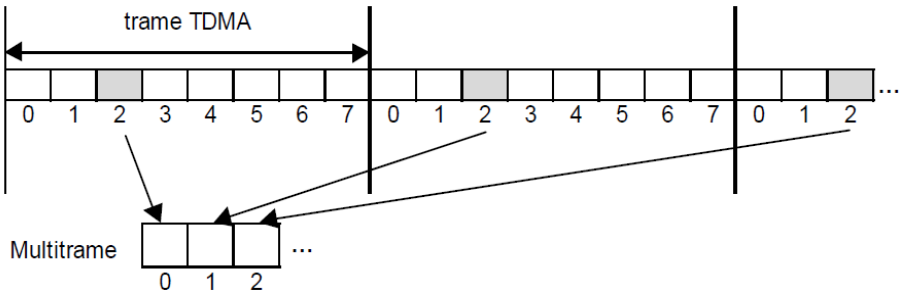

Figure 40: Principe de multitrame

Dans le GSM il existe deux types de canaux logiques :

- Le canal logique dédié (duplex) : dans une cellule donnée, une paire de *slots* (montant et descendant) est attribuée à un mobile déterminé, au sein d'une structure multitrame. Seul un mobile peut transmettre ou recevoir dans le même *slot* et à la même fréquence. À noter également que pour un même usager, les *slots* entre les liaisons montantes et descendantes sont décalés de trois *bursts* ;

- Le canal logique commun (simplex), partagé par un ensemble de mobiles à son écoute (sens descendant) ou en accès multiple (sens montant, avec résolution des collisions).

Le tableau suivant présente les principaux canaux logiques du GSM.

Tableau XIII : Principaux canaux logiques GSM

Type	Nom	Fonction
Unidirectionnel en diffusion (voie balise) *Broadcast Channel* (BCH) ↓	*Frequency Correction Channel* (FCCH) ↓	Corrige la fréquence porteuse
	Synchronization Channel (SCH) ↓	Donne l'identité de la BTS (BSIC) et synchronise la TDMA
	Broadcast Control Channel (BCCH) ↓	Information sur la cellule
Commun (accès partagé) *Common Control Channel* (CCCH) ↓↑	*Paging Channel* (PCH) ↓	Alerte le mobile
	Random Access Channel (RACH) ↑	Permet l'accès au réseau
	Access Grant Channel (AGCH) ↓	Allocation de ressource
	Cell Broadcast Channel (CBCH) ↓	SMS
Dédié *Dedicated Control Channel*	*Stand-alone Dedicated Channel* (SDCCH) ↓↑	Signalisation (1/8 TCH)
	Slow Associated Control Channel (SACCH) ↓↑	Contrôle la qualité reçue et la puissance
	Fast Associated Control Channel (FACCH) ↓↑	Information de *Handover*
Trafic	*Traffic Channel* (TCH) ↓↑ – pour voix codée – pour données	Plein débit : 22,8kbit/s Demi-dédit : 11,4kbit/s Débit utilisateur 13kbit/s

III.4.3.7 Le concept de voie balise

La voie balise est une fréquence porteuse caractéristique de la station de base qui l'émet. Choisies parmi les canaux fréquentiels dont dispose le GSM, les voies balises sont émises à puissance constante dans le sens descendant par chacune des stations de base du réseau. Elles transportent des informations de contrôle du système. Un portable reste en permanence à l'écoute des voies balise. Une phase de scrutation, dite de *monitoring*, est activée entre l'émission et la réception des *bursts*. Une voie balise supporte entre quatre et sept *slots* dédiés par trame TDMA. Plus particulièrement, un ensemble de canaux logiques, implantés sur le *slot* 0, permettent au mobile de se caler en fréquence (canal FCCH), de se synchroniser sur le réseau (canal SCH) et de récupérer les informations locales du système (canal BCCH). Des *bursts* de bourrage sont introduits sur des *slots* de la voie balise pour maintenir la puissance d'émission constante.

III.4.3.8 Sélection d'une cellule

Après la mise sous tension, l'état de veille du terminal mobile signifie son aptitude à recevoir des appels. Cependant, il doit d'abord savoir avec quelle BTS communiquer pour pouvoir établir la communication. Commence alors le processus de sélection de cellule qui comprend deux étapes : établissement d'une liste de voies balises dites candidates, et sélection d'une de ces voies pour l'inscription du terminal dans la cellule correspondante. Une cellule convenable (*suitable cell*) est sélectionnée si son champ électrique est le plus fort, si elle est incluse dans le PLMN sélectionné, si elle n'est pas interdite par le réseau ou

ne figure pas dans une liste de zones de localisation interdites et si l'affaiblissement entre la BTS et le terminal est en dessous d'un seuil déterminé par l'opérateur.

III.4.4 Implémentations USRP/GNU Radio

La GNU Radio, de par la limitation de ses fonctionnalités aux traitements de base de la couche physique, n'est pas vraiment adapté à l'analyse de trafic GSM (cette constatation peut être généralisée à la majorité des protocoles sans fil). Elle permet néanmoins d'effectuer un prétravail en identifiant les voies balises des BTS [fitzsimons], et ses résultats peuvent ensuite être exploités par d'autres logiciels tels que par exemple Airprobe.

III.4.4.1 Airprobe

Le projet Airprobe est un projet « libre » dont l'objectif est d'implémenter les briques logicielles permettant d'analyser le trafic GSM transitant sur l'interface air reliant les MS aux BTS. Le fonctionnement d'Airprobe s'articule en trois phases : acquisition des signaux radio, démodulation, analyse de protocole et décodage à l'aide principalement d'un USRP, de la GNU Radio et de Wireshark. Airprobe est en mesure d'identifier divers canaux de signalisation, mais étant donné que les fonctionnalités de saut en fréquence, de déchiffrement, et d'analyse de la liaison montante ne sont pas implémentées [airprobe], son utilisation en conditions réelles est limitée. À noter que la communauté de développeurs sur Airprobe n'est pas particulièrement active et beaucoup de développement est encore nécessaire pour que cet outil soit en mesure de recevoir et d'interpréter tous les différents types de *burst* GSM [airprobecode]. Divers documents permettent la prise en main rapide de ce projet [airprobeht] [airprobeht2]. La fonctionnalité de saut en fréquence implémentée par la majorité des BTS est difficilement réalisable avec une radio logicielle bon marché type USRP. Pour recevoir une conversation complète lorsque le saut en fréquence est activé, il est nécessaire de collationner tous les *bursts* des différentes fréquences utilisées. Ainsi deux méthodes d'acquisition sont possibles : soit le canal de réception est modifié de façon synchrone avec la séquence de saut en fréquence du mobile ciblé, soit l'intégralité de la bande GSM est capturée et un traitement est effectué *a posteriori*. Chaque saut de fréquence SFH d'un USRP ne provoque la perte que d'au plus un *slot* par trame. Il faut donc juste faire en sorte que le *slot* perdu ne soit pas celui qui doit être récupéré. Cette solution est réalisable avec un USRP2 à la seule condition que l'ordinateur hôte soit capable de traiter un débit de données de `25 MHz * 2 * 16`, soit 100 Mo/s.

Chapitre IV

Réalisations pratiques

Dans cette dernière partie nous allons implémenter plusieurs plateformes de test à l'aide d'une configuration USRP2 + GNU Radio. Dans une première partie nous verrons comment exploiter les signaux reçus, en se focalisant sur l'emploi de la TVRX v1 (à titre didactique) et de la RFX1800 (qui sera également utilisée lors de l'étude du DECT). Cette partie nous amènera à découvrir la présence de signaux internes perturbateurs au niveau du matériel étudié. Nous terminerons par la réalisation d'un système d'identification de stations de base DECT.

IV.1 Remarques préalables

La réalisation d'une plateforme de test implique au préalable une phase d'installation et de paramétrage global à la fois de la GNU Radio et modules associés, et des USRP. La plateforme de test utilisée est composée d'un USRP2, d'une carte RF, d'un ordinateur portable (RAM 2Go et processeur Intel Core 2 duo T7250 2 GHz) embarquant un OS Linux (Ubuntu v10.10 Maverick, noyau Linux 2.6.35-24generic) et de la GNU Radio (version 3.3.0). Parmi les quelques programmes en mode console de GNU Radio il en existe quatre particulièrement utiles :

- `find_usrps` : cette commande permet de vérifier si l'USRP est bien reconnu par l'ordinateur hôte, exemple (détection d'un USRP2) :

```
$ sudo find_usrps
00:50:c2:85:3b:4b hw_rev = 0x0400
```

- `gnuradio-config-info` : cette commande fournit quelques informations relatives à la version GNU Radio utilisée :

```
$ sudo gnuradio-config-info --h
Program options: gnuradio [options]:
  -h [ --help ]         print help message
  --prefix              print gnuradio installation prefix
  --sysconfdir          print gnuradio system configuration directory
  --prefsdir            print gnuradio preferences directory
  --builddate           print gnuradio build date (RFC2822 format)
  -v [ --version ]      print gnuradio version

$ sudo gnuradio-config-info -v
3.3.0
```

- `usrp2_fft` : ce programme Python permet d'afficher la transformée de Fourier rapide du signal reçu et numérisé par l'ensemble "carte RF + USRP2", permettant un

affichage type analyseur de spectre. Divers paramètres peuvent lui être transmis tels que la décimation (pour régler la largeur de bande fréquentielle à acquérir), la fréquence centrale d'acquisition ou le gain global du dispositif de réception. Plusieurs options en ligne de commande sont possibles (rajouter –h à la suite de la commande pour en obtenir la liste), dont l'option –W pour visualiser en mode *waterfall* et –S pour passer en mode oscilloscope :

```
$ sudo python '/usr/local/bin/usrp2_fft.py' -h
Usage: usrp2_fft.py [options]

Options:
  -h, --help            show this help message and exit
  -e INTERFACE, --interface=INTERFACE
                        select Ethernet interface, default is eth0
  -m MAC_ADDR, --mac-addr=MAC_ADDR
                        select USRP by MAC address, default is auto-select
  -d DECIM, --decim=DECIM
                        set fgpa decimation rate to DECIM [default=16]
  -f FREQ, --freq=FREQ  set frequency to FREQ
  -g GAIN, --gain=GAIN  set gain in dB (default is midpoint)
  -W, --waterfall       Enable waterfall display
  -S, --oscilloscope    Enable oscilloscope display
  --avg-alpha=AVG_ALPHA
                        Set fftsink averaging factor, default=[0.1]
  --ref-scale=REF_SCALE
                        Set dBFS=0dB input value, default=[1.0]
  --fft-size=FFT_SIZE   Set number of FFT bins [default=1024]
```

- `usrp2_probe` : cette commande permet de s'assurer que la carte RF est bien reconnue, et fournit diverses informations sur les performances de l'ensemble "USRP2 + carte RF". Le schéma suivant présente un exemple de détection `usrp2_probe` de l'USRP2 et de la TVRX étudiée ci-après.

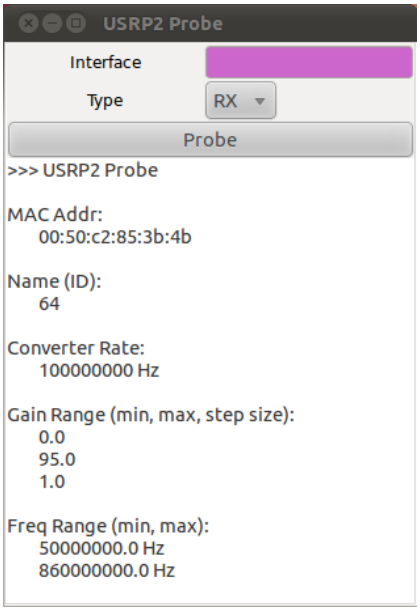

Figure 41 : Détection usrp2_probe de l'USRP2 et de la TVRX

IV.2 Plateforme n°1 : Étude des performances de l'USRP2 associé à certaines cartes RF

L'un des principaux avantages des USRP et des cartes RF associées est de proposer une architecture de radio logicielle relativement flexible et peu onéreuse (comparé aux solutions professionnelles). Mais on n'a rien sans rien et on se doute bien que la qualité des traitements du signal réalisés par ces équipements est plus ou moins liée à la qualité de ses constituants, généralement très liée à leur prix de vente.

Avant de mettre en œuvre des scénarios d'étude de protocoles de transmission radiofréquence, il est quasiment incontournable de déterminer, au-delà des quelques informations disponibles sur le site d'Ettus [ettus], les performances techniques des équipements utilisés. Il s'agit donc de procéder à un relevé des performances de ces équipements. L'étude qui suit se focalisera principalement sur l'USRP2, équipement relativement récent (2008) et encore peu documenté, associé aux différentes cartes RF mises à disposition, et la GNU Radio.

D'après [mari] l'USRP1 présente un certain nombre d'anomalies (non-linéarités, bogues probables dans le code source du pilote) dont certaines découlent des choix d'implémentation matérielle. Par exemple l'OL numérique de l'USRP1 utilise l'algorithme de Cordic basé sur une recherche dichotomique des valeurs de cosinus et sinus d'un angle donné. Cette approximation génère des distorsions entraînant notamment des phénomènes d'intermodulation. De manière générale les non-linéarités apportées par les circuits d'amplification, de multiplication ou de filtrage tant analogiques que numériques sont susceptibles de générer de l'intermodulation et autres effets non désirés. Les choix d'implémentation de fonctions de traitement numérique du signal au sein de l'USRP2 sont sensiblement les mêmes que pour l'USRP1. On risque donc de constater les mêmes phénomènes.

IV.2.1 Prise en main de l'outil : étude de l'USRP2 + carte RF Ettus TVRX

La partie la plus critique d'un système de transmission sans fil est souvent le récepteur car il a la lourde tâche d'extraire le signal désiré parmi d'autres signaux, interférences et bruit. La carte fille TVRX v1 est une carte de réception RF construite autour du tuner Microtune 4937 D15, composant présentant une bande passante de 6 MHz. Elle dispose de deux entrées de contrôle automatique de gain (AGC – *Automatic Gain Control*) permettant de régler le niveau du signal reçu : une plage en RF de 50 dB et une

plage en FI de 33 dB. Les étages d'amplification sont initialisés ensemble via la fonction `set_gain(gain en dB)`. Le schéma suivant présente les deux étages d'amplification de la TVRX.

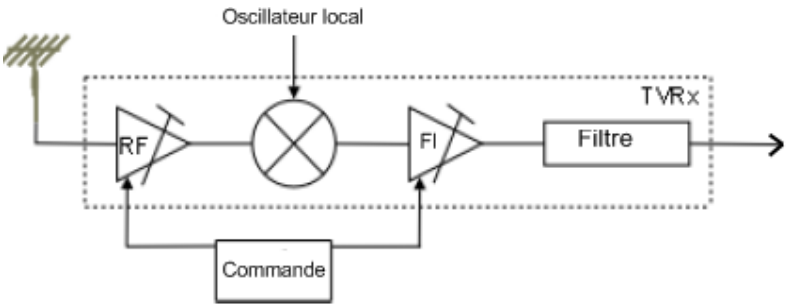

Figure 42 : Diagramme par bloc des étages d'amplification de la TVRX

La carte TVRX permet notamment d'analyser la bande FM [88 MHz – 108 MHz]. Sur les figures suivantes, obtenues avec le programme usrp2_fft, on distingue clairement l'activité des stations radio.

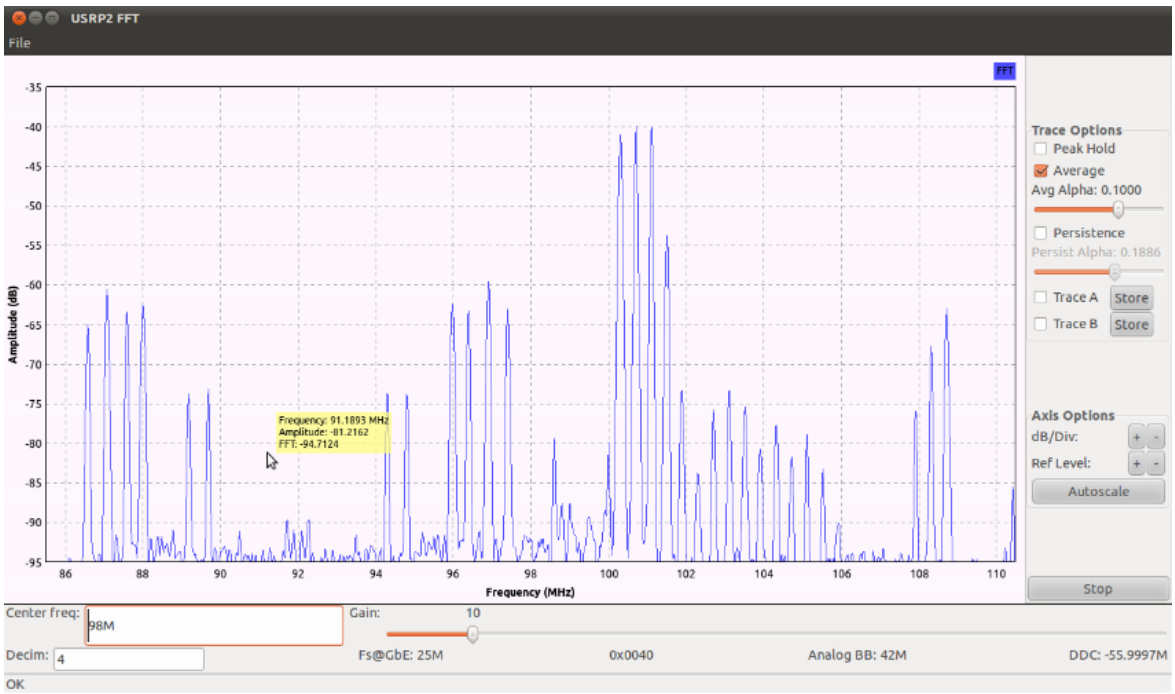

Figure 43 : Diagramme FFT (usrp2_fft) de la bande FM

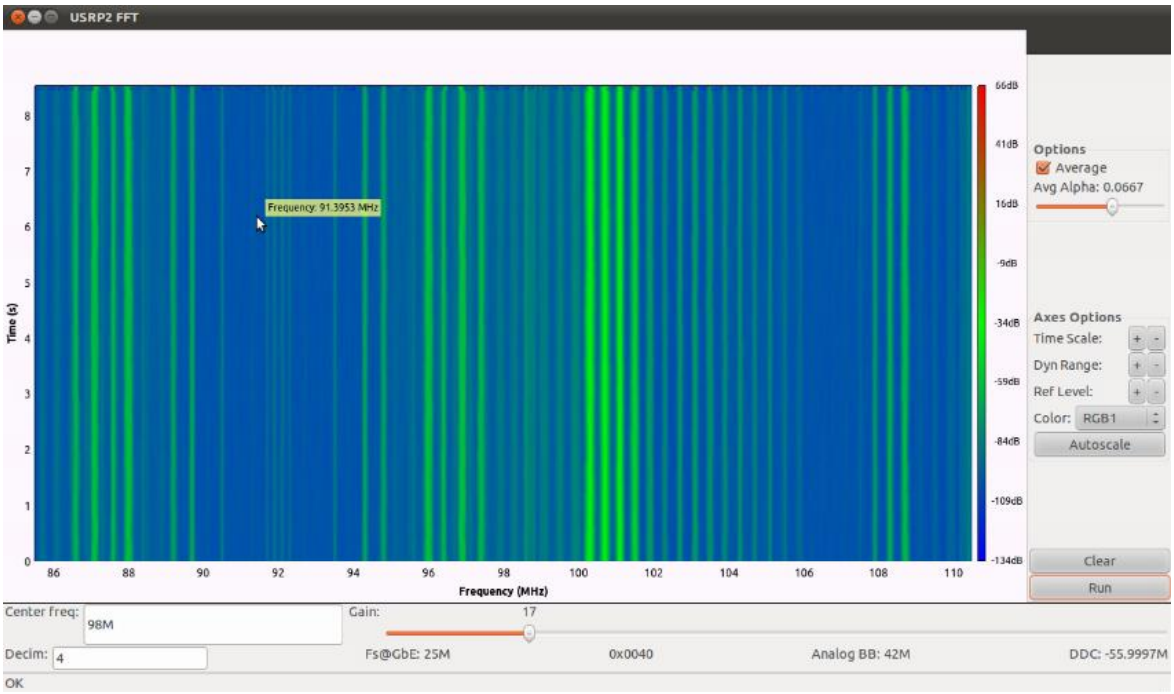

Figure 44 : Spectrographe 2D (usrp2_fft) de la bande FM

La bande passante de la TVRX permet également d'étudier les canaux TV (c'est principalement son rôle). La figure suivante met en exergue le canal 27.

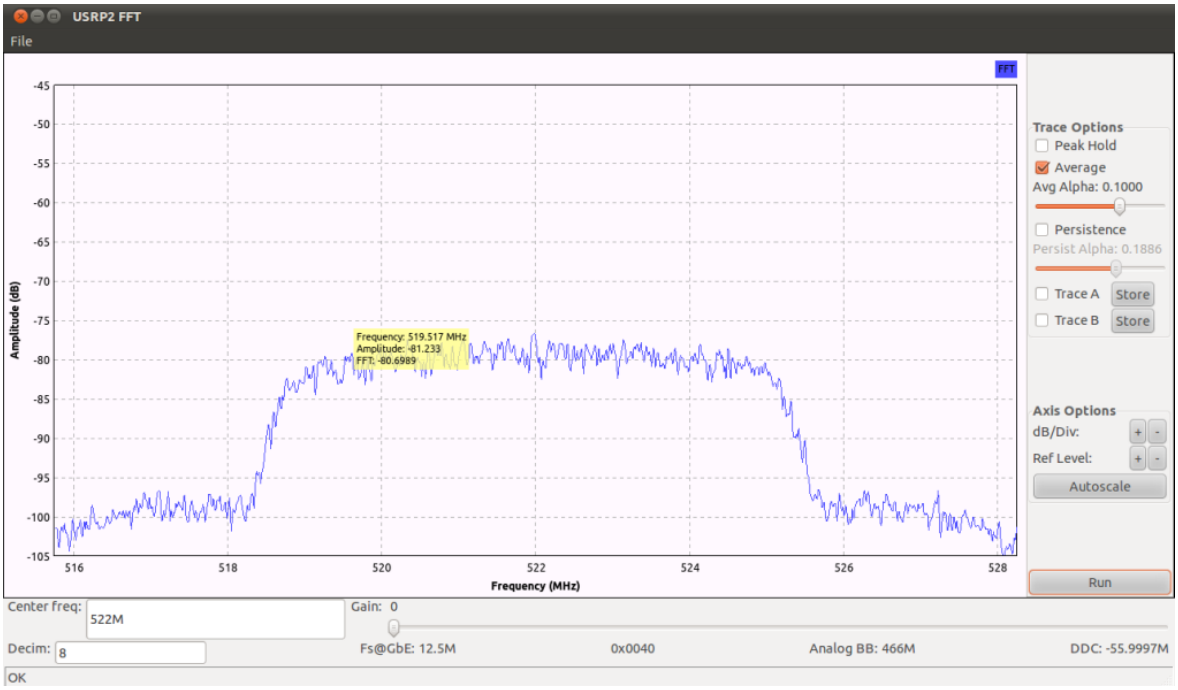

Figure 45 : usrp2_fft : Bande TV canal 27

IV.2.2 Étude de l'USRP2 associé à la carte RFX1800

Après avoir manipulé les différentes possibilités d'affichage (FFT, *waterfall*, etc.) des signaux traités en réception par l'USRP2, focalisons-nous sur l'étude de l'ensemble "USRP2 + carte RFX1800". Cette étude, initialement dédiée à la visualisation de l'activité dans la bande couverte par la carte RFX1800, a rapidement évolué vers une analyse du comportement de l'ensemble lorsqu'il est employé avec un gain élevé afin de mettre en évidence un phénomène pouvant être gênant lors de l'exploitation de signaux faibles.

La carte RFX1800 est utilisable dans la bande [1.5 GHz – 2.1 GHz]. Cette bande de fréquences est notamment utilisée par les réseaux DCS et DECT. La figure suivante présente une activité DCS « liaisons montantes » (mobile vers station de base).

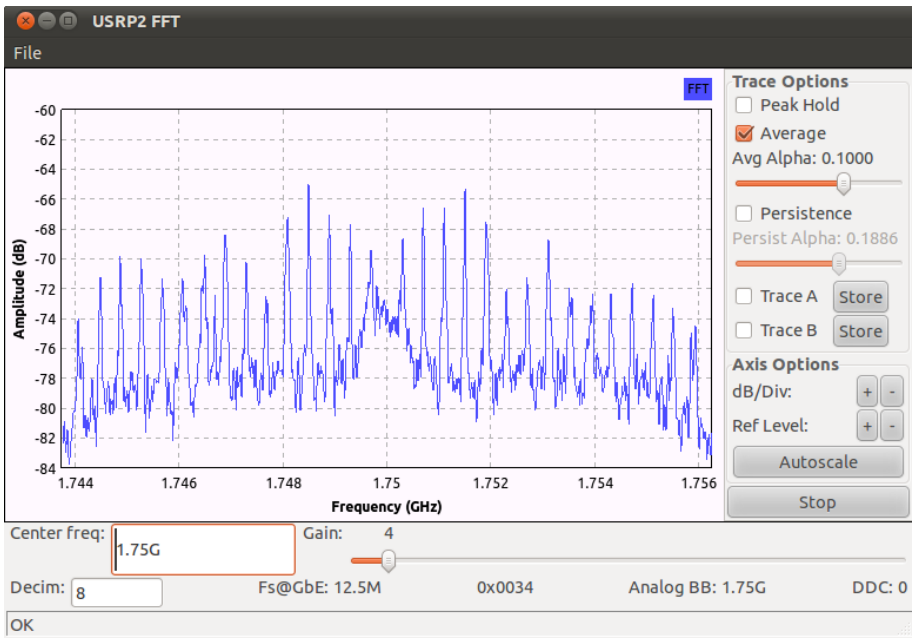

Figure 46 : Signaux DCS « liaisons montantes »

Le plancher de bruit en réception peut être évalué avec le programme usrp2_fft mais est variable selon les paramètres d'acquisition entrés (décimation, gain et fréquence centrale). Diverses mesures indiquent qu'il varie de -90 dBm à -140 dBm. À noter que l'amplitude mesurée sur le graphique du programme usrp2_fft ne correspond pas à des dBm, mais plutôt à un niveau de comparaison évalué en décibels (dB). Au niveau relevé il faut soustraire le gain rajouté par le dispositif (valeur du curseur Gain de l'interface graphique, comprise entre 0 dB et 70 dB pour la RFX1800) et ajouter l'atténuation globale apportée par les différents circuits passifs du dispositif d'acquisition et de numérisation des signaux. Le plus simple pour évaluer cette atténuation est d'effectuer une mesure préalable

sans événements perturbateurs (donc typiquement en cage de Faraday) en injectant directement en entrée de la carte RF, à l'aide d'un générateur de signaux, une sinusoïde à un niveau donné et une fréquence correspondant à la fréquence centrale de travail, et ce avec les paramètres d'affichage voulus. La figure suivante illustre ce procédé avec un signal d'entrée de niveau -70 dBm, ce qui donne pour résultat une atténuation d'environ 10 dB. Diverses mesures indiquent que cette atténuation varie de 1 dB à 12 dB. On remarque également sur cette figure que la porteuse est détectée à environ 1,750006 GHz au lieu des 1,75 GHz indiqués par le générateur (soit un décalage d'environ 3,4 ppm[43]). Ce décalage peut avoir plusieurs origines : soit le générateur de signaux ne délivre pas une fréquence exacte (dérive depuis la dernière calibration), soit il est provoqué par les approximations induites par le calcul de la FFT pour l'affichage, soit l'ensemble "carte RF + USRP2" introduit un biais dans la mesure, ou autre. Dans le cas présent, ce décalage fréquentiel est principalement dû à la première hypothèse car une mesure du signal injecté à l'aide d'un analyseur de spectre récemment calibré a présenté quasiment le même décalage fréquentiel (décalage de +5kHz, soit environ 2,9 ppm). On en déduit que le dispositif de mesure "USRP2 + carte RFX1800 + usrp2_fft" est particulièrement précis concernant la restitution de l'information fréquentielle.

Figure 47: Injection en entrée de l'USRP2 d'une sinusoïde de fréquence 1,75 GHz et de niveau -70 dBm

[43] Abréviation de « partie par million », soit un rapport de 10^{-6}.

La mise en évidence de signaux de faible amplitude peut être problématique car si l'on augmente le gain du dispositif, des raies parasites se forment. Le phénomène est d'autant plus marqué si le signal d'entrée est faible et le gain élevé. La figure suivante illustre le cas extrême où l'on visualise une raie parasite (de fréquence 1,7 GHz) dont le niveau de puissance est plus élevé que celui du signal utile (de fréquence 1,701 GHz et de niveau -90 dBm). Au vu du niveau du signal injecté, on peut en déduire que le niveau de cette raie est d'environ -76 dBm. Selon le protocole analysé, et notamment sa robustesse vis à vis des perturbations, la gêne occasionnée par ces raies parasites peut ou non être bloquante.

Figure 48 : Visualisation d'une raie parasite de niveau supérieur au signal mesuré

La présence de ces raies parasites nécessite toutefois une explication : d'où viennent-elles et comment sont-elles générées ? Sont-elles ou non dépendantes du signal injecté ?

Une seconde expérimentation a consisté à appliquer en entrée de réception de l'USRP2 un bouchon adapté à son impédance d'entrée, à savoir 50 ohms, toujours en étant dans une cage de Faraday. Ceci permet de déterminer la présence ou non de raies parasites en l'absence d'élément perturbateur externe. Les différents relevés réalisés confirment la présence de raies parasites si le gain utilisé est quasi maximal. Certaines d'entre elles semblent provenir de la saturation de certains composants du circuit de réception. Comme le montre la figure suivante, leur niveau est toutefois assez faible (ici environ -110 dBm).

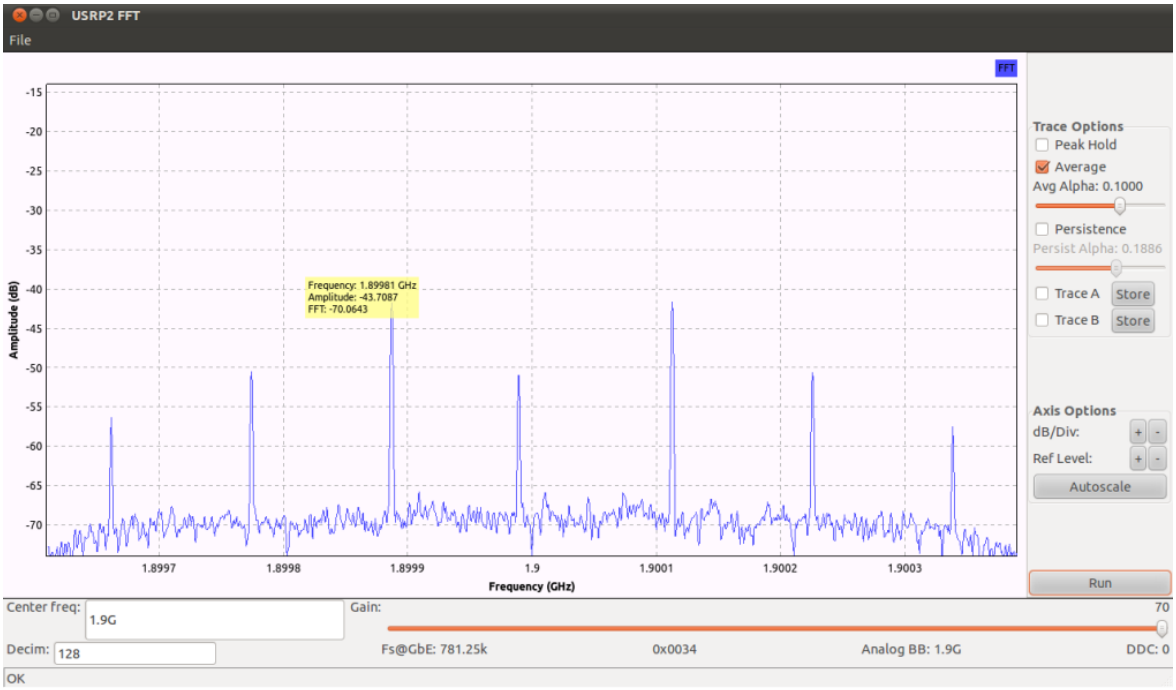

Figure 49 : Mesure effectuée avec bouchon de 50 Ω et fréquence d'accord 1.9 GHz

Une fréquence d'accord proche d'un multiple de 100 MHz révèle des raies parasites présentant un niveau non négligeable (de l'ordre de -70 dBm sachant que l'on n'applique aucun signal à l'entrée de la carte RF !). La figure suivante montre une de ces raies.

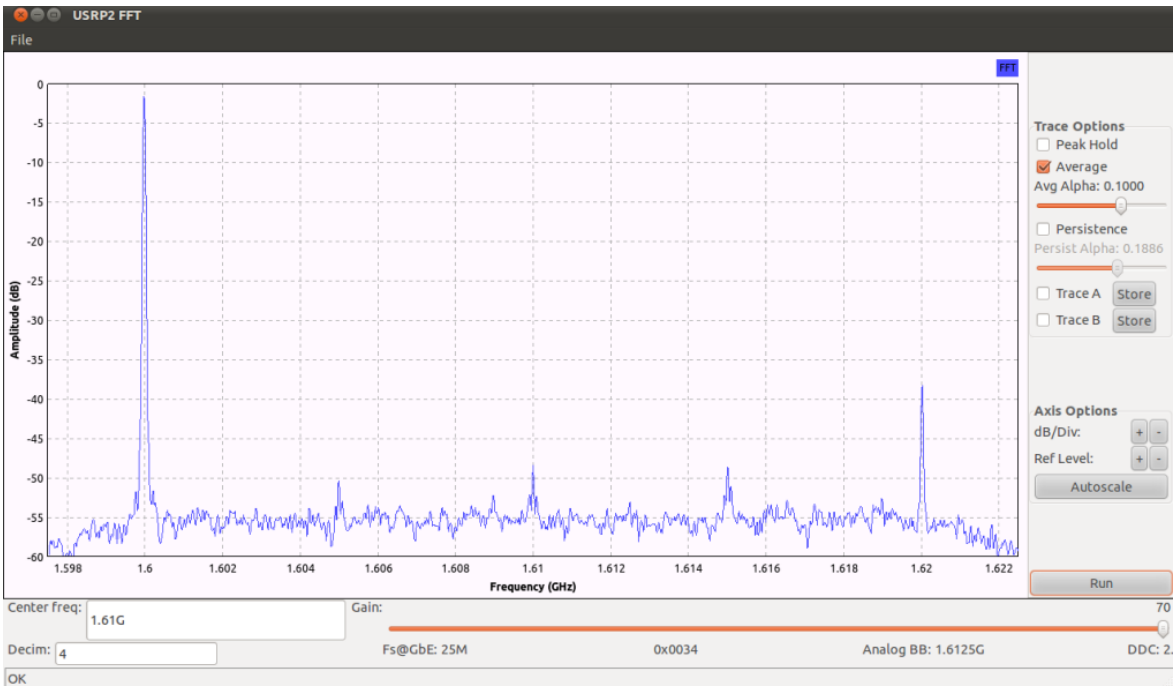

Figure 50 : Mesure effectuée avec bouchon de 50 ohms et fréquence d'accord 1.61 GHz

Curieusement ce phénomène n'est constaté que si l'on choisi une fréquence d'accord non exactement égale à un multiple de 100 MHz. Quoi qu'il en soit, ces raies se retrouvent

à tous les multiples de 100 MHz dans la plage de fonctionnement de la carte RF utilisée, et quelle que soit la carte RF utilisée. Tout semble indiquer que ces raies sont en fait des harmoniques d'un composant rayonnant à 100 MHz et polluant à la fois la carte RF et l'USRP2.

Une troisième expérimentation a consisté à procéder à des relevés de rayonnement électromagnétique à l'aide d'une sonde de champ proche couplée à un analyseur de spectre au dessus de l'USRP2 (sans carte RF puis avec carte RF). Les relevés sans carte RF révèlent une raie principale à 100 MHz et chacune de ses harmoniques dans la bande passante de la sonde utilisée. L'origine de la raie principale semble correspondre à un rayonnement de l'oscillateur VCXO 100 MHz [crystek] de l'USRP2. En ajoutant la carte RF on constate le même phénomène, mais avec des niveaux de puissance un peu plus élevés.

L'utilisation d'une sonde de champ proche de précision a ensuite permis de localiser le composant fautif. En effet, lors du passage de la sonde sur les cartes en fonctionnement, il a été constaté un pic de rayonnement aux abords de l'oscillateur VCXO 100 MHz de l'USRP2. Cela confirme l'hypothèse selon laquelle ce composant serait à l'origine des raies parasites multiples de 100 MHz. Une mesure de la composante alternative de la tension d'alimentation 6 V alimentant les différents composants de l'USRP2 à l'aide d'un oscilloscope a permis de mettre en évidence un signal de faible amplitude (environ 30 mVcc) et de fréquence principale 100 MHz. Sa présence indique que la quasi-porteuse générée par le VCXO (celui-ci ne génère effectivement pas une porteuse pure) fuie dans l'alimentation, et que le filtrage de cette fréquence de référence n'est pas correctement réalisé, notamment au niveau des circuits d'alimentation. La non-linéarité de certains composants et la présence de circuits d'amplification et de transposition fréquentielle expliquent la présence de ces fréquences harmoniques.

Une solution possible pour limiter l'apparition de ces raies serait d’effectuer un filtrage efficace, voire de pouvoir modifier indépendamment le gain des différents circuits d'amplification du dispositif pour éviter les phénomènes de saturation. Les méthodes de contrôle de gain fournis par la GNU Radio permettent d'ajuster les gains disponibles dans les circuits d'émission et de réception. Ces gains dépendent des spécificités des implémentations matérielles utilisées (type de carte RF). Bien qu'un matériel spécifique contienne des réglages de gain à plusieurs endroits, tels qu'au niveau de l’amplificateur à gain programmable, des atténuateurs variables et autres circuits, l'interface matérielle de

contrôle de la carte ne fournit qu'un paramètre de contrôle du gain. Il appartient au logiciel implémentant l'interface matérielle de déterminer comment répartir le gain désiré dans tout le système. De plus, contrairement à l'USRP1 où l'interface matérielle prévoit un contrôle du gain de ses CAN (de 0 dB à 20 dB), la GNU Radio ne fournit pas, au niveau applicatif, de fonctions pour contrôler le gain de l'USRP2. En comparant par exemple le gain contrôlable de la TVRX et le gain consolidé affiché par usrp2_probe, on en déduit que le gain global de l'USRP2 en réception est d'au plus 12 dB, ce qui est relativement peu comparé au gain global de 95 dB du dispositif. Quand l'interface matérielle a besoin de régler le gain du circuit de réception, celui de la carte RF est ajusté en premier. Quand il atteint son maximum réglable, celui de l'USRP2 est ensuite utilisé. Malheureusement, de multiples mesures permettent de constater que la valeur du gain consolidé du dispositif, essentiellement fournit par la carte RF, n'a que peu d'impact sur le niveau des raies parasites. Plusieurs solutions existent néanmoins pour réduire voire annuler ces dernières :

- Isoler le composant fautif et le remplacer par une horloge externe à alimentation séparée. La présence d'un connecteur pour horloge externe de 10 MHz en façade de l'USRP2 (100 MHz en modifiant le *bitstream*) permettrait la correction. Cependant cette référence n'est utilisable que comme source de synchronisation et non comme horloge de système principale [extclock]. Cette solution ne peut donc être retenue ;

- Alimenter l'OL par une alimentation distincte (solution assez contraignante compte tenu de la taille réduite des broches du composant) ;

- Mettre un filtre passe-bas sur l'alimentation, au plus près de l'oscillateur (là aussi une telle intervention exige des doigts de fée lilliputienne compte tenu du degré de miniaturisation des cartes).

Des solutions existent donc mais leur mise en œuvre exige de disposer d'équipements de soudure extrêmement précis.

IV.3 Plateforme n°2 : Système d'identification de stations de base DECT

Dans cette partie nous allons présenter la réalisation d'un dispositif permettant d'effectuer de l'écoute passive sur des transmissions DECT afin de pouvoir identifier les stations de base captées. Cette plateforme implémente un démodulateur et un module de traitement pour effectuer une acquisition de données utilisateur et de données de contrôle transmises par un système DECT. L'étude se décompose en deux parties. La première

partie consiste en l'étude du DECT, restreinte aux couches basses et focalisée sur l'aspect identification des équipements. La deuxième partie décrit la configuration de la plateforme utilisée, les outils développés et présente les résultats obtenus.

IV.3.1 Le DECT

IV.3.1.1 Présentation

Le DECT (*Digital Enhanced Cordless Telecommunications*) est un standard de radiocommunication développée par l'ETSI (*European Telecommunications Standard Institute*, référence ETSI : EN 300 175) afin de fournir une technologie d'accès radio générale pour les télécommunications sans fil dans le but d'accéder par voie aérienne et par l'intermédiaire d'une station de base, à divers réseaux de télécommunication (LAN, RTCP, RNIS, GSM, UMTS, SIP, etc.). En Europe, le DECT est utilisé dans la bande de 1880 MHz à 1900 MHz. Les fréquences DECT sont disponibles dans plus de 100 pays et supportent des applications de transmission de la voix, de transmission de données et de mise en réseau, avec une portée atteignant 500 mètres en espace libre. Cette norme fait partie des interfaces radio de l'«*International Mobile Telecommunications* 2000" (IMT-2000) sous la dénomination «IMT-2000 FDMA/TDMA». Elle supporte la téléphonie bande étroite (3,1 kHz), bande large (7 kHz) et super large (jusqu'à 14 kHz). Le DECT supporte la transmission de données en mode circuit et paquet avec un débit maximal de 844,8 kbit/s pour une modulation à 2 niveaux, et jusqu'à 5,0688 Mbit/s pour une modulation multiniveau (4-aire, 8-aire, 16-aire et 64-aire). Ces débits peuvent être augmentés à l'aide de techniques de parallélisation de canaux (cf. norme NF EN 301649). Une extension ultime du DECT, nommée DECT *Broadband*, permet même d'atteindre un débit binaire brut de 20 Mbit/s. Une connexion DECT correspond à la transmission de *bursts* de données dans des *time-slots* définis. La communication peut être unidirectionnelle (*simplex*) ou bidirectionnelle (*duplex*).

Le DECT est principalement utilisé dans les systèmes de téléphonie sans fil des particuliers et petites entreprises, et derrière les commutateurs privés ou PABX (*Private Automatic Branch eXchange)* des moyennes et grandes entreprises. Dans ce cas un certain nombre de points d'accès (ou bornes) sont disposés dans les bâtiments de façon à offrir un réseau microcellulaire. Il est possible alors d'offrir des fonctions de type *handover* pour permettre de maintenir les communications tout en se déplaçant dans les locaux. En milieu professionnel, le déploiement de solutions de mobilité basées sur le DECT est facilité par le fait que le DECT dispose de sa propre bande de fréquences contrairement au Wi-Fi

confiné dans la bande ISM 2,4 GHz très utilisée par de multiples systèmes (Wi-Fi, Bluetooth, Four à micro-ondes, …). Le DECT peut en outre être utilisé pour fournir un accès GSM, CTM (*Cordless Terminal Mobility*) ou à un réseau local supportant la téléphonie, le fax ou divers services Internet. Le DECT est également employé en extension de radio cellulaire ou de réseau public local, par exemple en boucle locale radio sur le dernier kilomètre séparant le système de l'utilisateur. Le DECT est populaire en Europe. Pour exemple, plus de 30 millions d'équipements DECT sont déployés en Allemagne.

Un système DECT est composé d'une partie fixe (FP – *Fixed Part*), utilisant une ou plusieurs stations de base (RFP – *Radio Fixed Part*)[44], et un ou plusieurs terminaux portables (PP - *Portable Part*). Pour la plupart des réseaux DECT, le FP correspond à la partie fixe du téléphone sans fil, connectée au réseau téléphonique public ou autre service IP, tandis que le PP est le téléphone mobile proprement dit. En raison de l'utilisation des méthodes d'accès MC (*Multi Carrier* – multiporteuse), TDMA (*Time Division Multiple Access* - accès multiple à répartition temporelle), TDD (*Time division Duplex* - duplex temporel) et de la sélection et l'allocation dynamique des canaux (DCSA - *Dynamic Channel Selection and Allocation*), le DECT offre une grande qualité de service sans planification des fréquences.

La norme DECT couvre uniquement l'interface air (CI – *Common interface*) entre un RFP et un PP. La topologie DECT basique est celle en étoile. Il existe également des topologies « PP à PP », « FP à FP » et « communications distribuées ». [presdect]

[44] Un FP DECT peut avoir un ou plusieurs RFP et un RFP ne peut soutenir qu'un canal RF. Les téléphones sans fil n'ont qu'un RFP par FP, donc un seul RFP est implémenté.

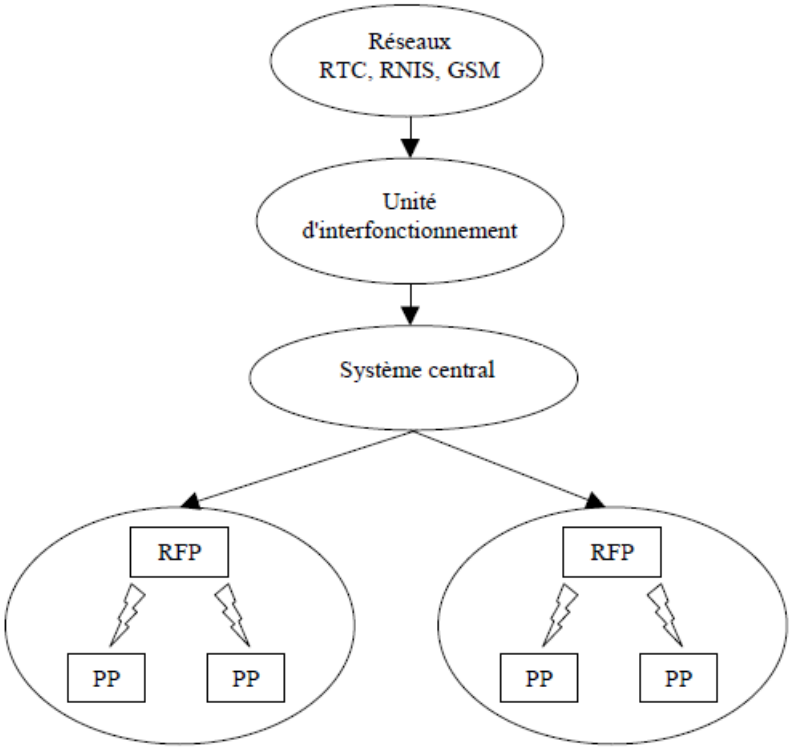

Figure 51 : Modèle d'architecture du système DECT [terre]

La norme DECT dans son ensemble étant très ouverte, un certain nombre de profils ont été définis dans les couches hautes de la pile de protocole DECT pour assurer l'interfonctionnement des équipements. Les profils les plus connus sont :

- GAP (*Generic Access Profile*, référence ETSI EN 300 444), service de transport de la téléphonie (classique ou de voix sur IP) sur l'interface air, obligatoire dans tout appareil DECT depuis 1997 pour permettre l'interopérabilité des fonctions de base (établissement de communication, etc.) de matériels provenant de différents constructeurs. [gap] ;

- CAP (*Cordless Terminal Mobility Access Profile*), permettant "l'itinérance" (*roaming*) entre réseaux ;

- RAP (*Radio Local Loop Access Profile*) pour la définition de la « Boucle Locale Radio ».

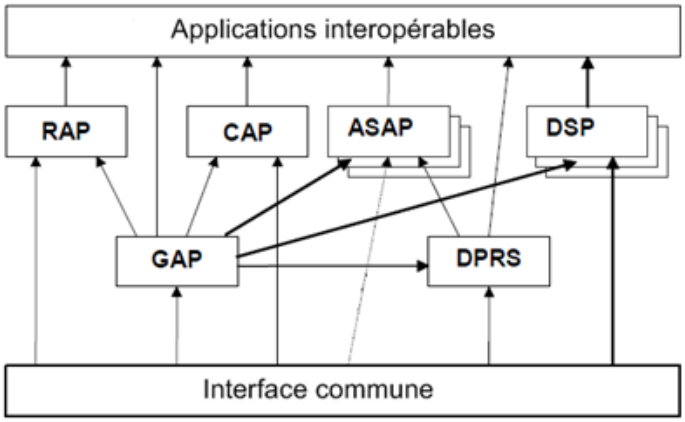

Figure 52 : Vue générale des principaux profils DECT

IV.3.1.2 Description du spectre radio

L'allocation standard des fréquences du DECT utilise 10 fréquences porteuses dans la gamme [1880 MHz - 1900 MHz] (cf. tableau en annexe C, page XLI). Le spectre temporel est subdivisé en trames se répétant toutes les 10 ms. Une trame temporelle est composée de 24 intervalles de temps ou *time slots* accessibles individuellement et pouvant être utilisés en émission ou réception. C'est le principe d'accès multiple à répartition temporelle ou TDMA (*Time Division Multiple Access*). Les trames sont composées de 12 *time slots* pour la liaison descendante (transmission FP vers PP) et les 12 suivants sont utilisés pour la liaison montante (transmission PP vers FP), d'où une capacité de 12 transmissions duplex sur une même porteuse.

Une station de base DECT émet constamment sur au moins un canal. Diverses informations telles que l'identité unique et les capacités de la station de base sont transmises dans des messages de diffusion (*broadcast*). Les PP analysent les informations diffusées par les RFP pour savoir s'ils y ont droit d'accès, déterminent si les capacités de RFP correspondent avec leur besoin en services et détectent les FP disposant de liens radio disponibles. Les appareils DECT analysent leur environnement au moins tous les 30 secondes. Ce faisant, ils reçoivent et mesurent la force du signal RF sur tous les canaux et créent une liste des canaux libres ou liste RSSI (*Radio Signal Strength Indicator*).

Ainsi, le PP ou FP est en mesure de choisir le meilleur canal pour une nouvelle liaison de communication. Le PP vérifie en permanence les canaux de la station de base présentant la meilleure valeur de RSSI et pour laquelle il a droit d'accéder. Une faible valeur de RSSI indique des canaux libres et sans interférence, tandis qu'une valeur élevée de RSSI indique si des canaux sont occupés ou soumis à des interférences. La DCSA

garantie ainsi que les liaisons radio sont toujours activées sur les canaux disponibles ou ceux subissant le moins d'interférences [dectforum].

Un appel peut être initié par un PP ou par un FP. Dans le premier cas, le PP choisit le meilleur canal disponible et accède au FP sur ce canal. Dans le deuxième cas un message "page" (*paging message*) contenant l'identité unique du portable destinataire est envoyé par le FP. Lorsque ce message est reçu, le PP établit une liaison radio sur le meilleur canal disponible. La partie initiant l'appel envoie un message {CC-SETUP} contenant diverses informations dont son identité [dect5]. Si une quelconque demande d'établissement ne peut aboutir ou si le message {CC-SETUP} contient des erreurs ou des incohérences, la partie destinataire de l'appel envoie un {CC-RELEASE-COM} pour rejeter l'appel. Si l'appel peut être confirmé, un message {CC-CONNECT} est envoyé à l'initiateur de l'appel. La procédure de communication initiée par un PP peut contenir les messages suivants :

- {CC-SETUP} est envoyé par le PP pour initier un appel au travers du FP. Ce message contient toujours les identifiants uniques du PP et du FP et peut également contenir d'autres informations ;

- {CC-CONNECT} est envoyé par le FP vers le PP pour indiquer son acceptation de l'appel. Il peut contenir diverses informations tels que le code d'identification du fabricant de l'équipement ou code EMC (*Equipment Manufacturer Code*) ;

- {CIPHER-REQUEST} est envoyé par le FP vers le PP pour déclencher le chiffrement. Il contient d'autres informations sur le type d'algorithme de chiffrement et de clé de chiffrement ;

- {AUTHENTICATION-REQ} est envoyé par le FP ou le PP pour authentifier l'autre partie ;

- {AUTHENTICATION-REP} est envoyé par le FP ou le PP pour prouver son authenticité.

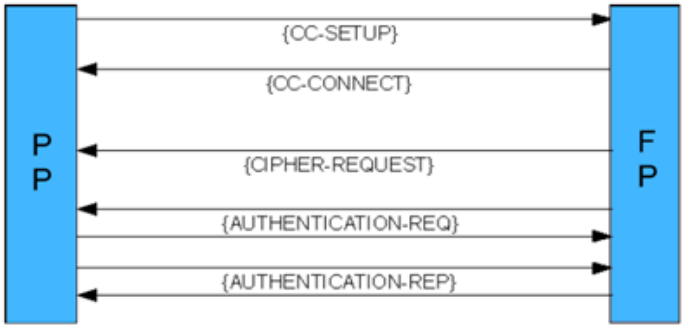

Figure 53 : Initiation par le PP d'un appel sortant

Concernant la gestion des identités, chaque FP transmet en *broadcast* une classe d'identité de droit d'accès ou ARI (*Access Rights Identity*) globalement unique. À chaque ARI sont associés des services, des protocoles et éventuellement des clés d'authentification et de chiffrement. De même, chaque PP a une ou plusieurs clés de droits d'accès ou PARK *(Portable Access Rights Keys*). Une PARK concerne un FP ou un groupe de FP appartenant au même opérateur. A chaque PARK sont associés des ARI de FP correspondants, des services, des protocoles et éventuellement des clés d'authentification et de chiffrement.

A l'instar d'autres technologies de transmission radiofréquence, des interrogations subsistent sur les risques sur la santé de l'exposition aux rayonnements électromagnétiques induits par les systèmes DECT. Non pas du côté terminal, où les puissances émises sont de l'ordre de 10 mW, mais plutôt côté station de base. En effet une station DECT émet en permanence une balise dans un des *slots* (4 ms toutes les 100 ms), à une puissance de 10 mW à 120 mW. Une étude de l'ARCEP concernant le Wi-Fi, ayant un mode de fonctionnent similaire, montre que le niveau d'exposition radioélectrique demeure inférieur aux normes même si les équipements sont très près des utilisateurs. Le principe de précaution conduit toutefois à recommander d'éloigner autant que possible les bornes DECT des endroits où les personnes séjournent de façon prolongée (lit, canapé, bureau,…). Apparus fin 2008, de nouveaux modèles de téléphones DECT dits "DECT Eco" ajustent (à la baisse) la puissance d'émission en fonction de la distance entre la station de base et le téléphone. Le tableau suivant résume les caractéristiques principales de la norme DECT.

Tableau XIV : Caractéristiques techniques du DECT (pour la zone Europe)

Modulation	Essentiellement GFSK (Gaussian Frequency-Shift Keying) Mais aussi π/2-DBPSK, π/4-DQPSK, π/8-D8PSK, 16-QAM et 64-QAM
Technique d'accès	FDMA : 10 porteuses (canaux) de 1880 MHz à 1900 MHz (bandes [1900 MHz-1920 MHz] et [1910 MHz-1930 MHz] également disponibles mais non utilisées), de largeur 1,728 MHz, espacées de 1,728 MHz, à allocation dynamique. TDMA : trames de 10 ms composées de 24 intervalles de temps plein ou *full slots* (12 dans chaque sens de transmission) pouvant être groupés pour offrir un débit binaire supérieur. Chaque *full slot* peut être découpé en deux *half slots*, ou être regroupé deux par deux en *double slot*. A titre d'exemple un *double slot* en modulation 64-aire offre un débit binaire de 480 kbit/s. Il est possible de regrouper au maximum 11 *double slots* et atteindre ainsi un débit binaire de 5280 kbit/s.
Débit binaire brut	1152 kSymboles/s (1152 kbit/s, 2304 kbit/s, 3456 kbit/s ou 6192 kbit/s pour respectivement les modulation 2-,4-,8,-16- et 64-aire).
Puissance d'émission moyenne	PP : 10 mW RMS (max 250 mW) RFP (résidentiel) : max 60 mW RFP (autre): max 250 mW
Portée	Jusqu'à environ 500 mètres en espace libre et 50 mètres en intérieur.
Codecs audio supportés	G.726, G.711, G.722, G.729.1 (large bande) et MPEG-4 ER LD AAC (bande large et bande super large)
Sécurité	L'algorithme de chiffrement du DECT est le DSC (DECT *Standard Cipher*). Il est sensé assurer la protection des communications entre un terminal mobile et une station de base. Le DSC repose sur un vecteur d'initialisation de 35 bits et un chiffrement du flux de voix sur 64 bits. L'algorithme d'authentification du DECT est le DSAA (DECT *Standard Authentication Algorithm*). Il est utilisé pour l'attribution de clé et l'authentification d'un FP et d'un PP. Les spécifications du DSC et du DSAA ne sont diffusées aux fabricants qu'après signature d'un accord de non-divulgation.
Protocole de niveau 2	LAPC (*Link Access Protocol Control*), basé sur l'HDLC.
Protocoles de niveau 3	*Call Control* (CC), *Call Independent Supplementary Services* (CISS), *Connection Oriented Message Service* (COMS), *Connectionless Message Service* (CLMS), *Mobility Management* (MM). Ces protocoles communiquent entre eux via le *Link Control Entity* (LCE).

IV.3.2 Plateforme de test

IV.3.2.1 Architecture matérielle

L'objectif de cette étude est de réaliser un outil logiciel permettant d'utiliser l'USRP2 et la carte RFX1800 pour procéder à la récupération de diverses informations associées aux systèmes DECT détectés, dont notamment les identifiants de stations de base DECT ou RFPI. Une étude pratique du DECT est consultable en **annexe C**.

La plateforme de test est composée des équipements cités au paragraphe IV.1. La carte RF est une carte RFX1800 connectée à une antenne VERT900 dédiée aux bandes

900 MHz et 1800 MHz [ettus]. Nous avons également utilisé trois équipements DECT différents, placés à environ deux mètres de l'USRP2, afin de pouvoir mesurer des signaux DECT relativement proches : un ensemble "RFP + PP" Philips Onis 2 mémo, un ensemble "RFP + PP" Onis Vox, et un ensemble "RFP + deux PP" Logicom Riva.

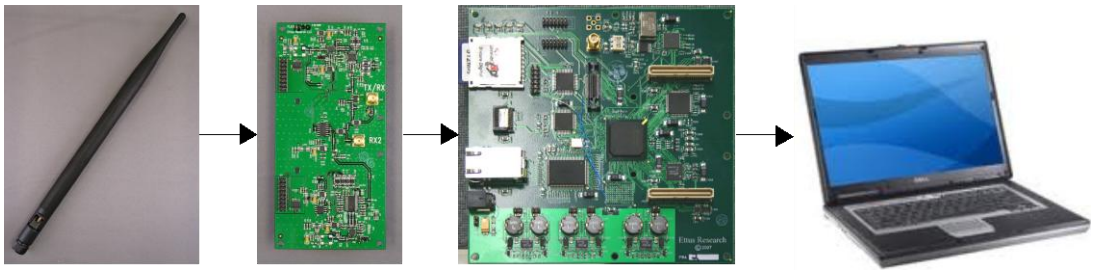

Figure 54 : Architecture matérielle de la plateforme de test DECT

Rappelons que les CAN de l'USRP2 ont une résolution de 14 bits et opèrent à 100 Méch/s (soit 1.4 Gbit/s). Étant donné que l'interface Gigabit Ethernet opère à un débit maximum de 1 Gbit/s, le FPGA doit réduire le taux d'échantillonnage pour le circuit de réception (décimation), et l'augmenter pour l'émission (interpolation).

IV.3.2.2 Implémentations logicielles

IV.3.2.2.1 Programme « déDECTeur »

La première implémentation a consisté à modifier et améliorer le programme proposé par le projet gr_dect. Cet ensemble de programmes, conçu en langages Python et C++, consiste principalement à récupérer les informations des champs **A** véhiculés sur un canal physique choisi. Il souffre de nombreuses limitations et n'implémente en réalité pas toutes les fonctionnalités précisées sur le site Internet dédié au projet [grdect]. Il n'effectue notamment pas d'analyse de champs **B** (données) et n'effectue pas d'enregistrement des données collectées. Les informations collectées sur les champs **A** s'affichent en continu, au fur et à mesure de l'acquisition des signaux par le matériel. De plus, son développement semble avoir été brutalement interrompu en novembre 2008, et n'est plus maintenu. En lisant le code on constate que d'autres fonctionnalités étaient prévues mais n'ont pas pu être implémentées. gr_dect ne fonctionne que sur USRP1, aussi son portage sur USRP2 a-t-il nécessité la modification et l'ajout de nombreuses lignes de code. La figure suivante présente un extrait de résultats obtenus avec ce nouveau programme, nommé « déDECTeur ».

```
Numero d'adresse MAC USRP2:  00:50:c2:85:3b:4b
Taux du CAN (en Mech/s): 100M
Taux de decimation: 40
Debit binaire: 1.152M
Nombre d'echantillons par symboles: 2.17014
Frequence RF: 1.8887G
Nombre de taps du filtre de canal:  23
>>> gr_fir_ccf: using SSE
>>> gr_fir_fff: using SSE
bits per symbol = 1
M&M clock recovery omega = 2.170139
M&M clock recovery gain mu = 0.175000
M&M clock recovery mu = 0.500000
M&M clock recovery omega rel. limit = 0.005000
frequency error = 0.000000

Circuit de reception:
Gain Rx:         35
Modulation:      gmsk_demod
Debit binaire:         1.152Mb/s
Nombre d'echantillons par symbole:  2.17013888889
Taux de decimation:            40
Frequence Rx:    1.8887G
mainloop started
Frequence centrale: 1.89562G
Canal physique: 1

En-tête de paquet d'identité (canal logique de type N):  01101110
Canal physique:  1
Identifiant de RFP (RFPI): 1a93e5c8
Pourcentage des paquets avec CRC correct (FER*100):  100.0  %

En-tête de paquet d'identité (canal logique de type N):  01101110
Canal physique:  1
Identifiant de RFP (RFPI): 1a93e5c8
Pourcentage des paquets avec CRC correct (FER*100):  100.0  %

Diffusion par la RFP de paquets d'informations systeme (canal logique de type Q)
Canal physique:  1
En-tête:  10001110
Bits de contrôle: 304110ca40
Canal logique de signalisation type Q (informations systeme et multitrame)  0011

En-tête de paquet d'identité (canal logique de type N):  01101110
Canal physique:  1
Identifiant de RFP (RFPI): 1a93e5c8
Pourcentage des paquets avec CRC correct (FER*100):  100.0  %

En-tête de paquet d'identité (canal logique de type N):  01101110
Canal physique:  1
Identifiant de RFP (RFPI): 1a93e5c8
Pourcentage des paquets avec CRC correct (FER*100):  100.0  %

  ...

En-tête de paquet d'identité (canal logique de type N):  01101110
Canal physique:  1
Identifiant de RFP (RFPI): 1a93e5c8
Pourcentage des paquets avec CRC correct (FER*100):  100.0  %
Diffusion par la RFP de paquets d'informations systeme (canal logique de type Q)
Canal physique:  1
En-tête:  10001110
Bits de contrôle: 803ff0102
Canal logique de signalisation type Q (informations systeme et multitrame)  0000
Informations systeme statiques
Slots Numero 8 20
Nombre de transmetteurs de la RFP: 1
Informations de porteuse RF etendues 1=oui:  0
Toutes les porteuses sont disponibles
Numero de porteuse utilisee 1
Numero de porteuse en ecoute sur trame suivante 2

En-tête de paquet d'identité (canal logique de type N):  01101110
Canal physique:  1
Identifiant de RFP (RFPI): 1a93e5c8
Pourcentage des paquets avec CRC correct (FER*100):  100.0  %

 ...

En-tête de paquet d'identité (canal logique de type N):  01101110
Canal physique:  1
```

Figure 55 : Extrait d'affichages du programme déDECTeur

La réalisation de cette implémentation a permis de montrer la faisabilité de l'acquisition de trames DECT. `déDECTeur` a pour principal avantage de donner un aperçu de l'activité d'un ou plusieurs FP sur un canal physique donné. Parmi ses inconvénients, `déDECTeur` ne peut traiter qu'un canal à la fois et n'effectue pas de traitement *a posteriori*, notamment la récupération des informations pertinentes (RFPI par exemple), sans redondance d'affichage.

IV.3.2.2.2 Programme « dect_scan »

La modification du code de `déDECTeur` pour lui assurer un traitement multicanal s'avérerait particulièrement difficile compte tenu du fait que le code C++ de certains blocs de traitement numérique du signal de GR_DECT n'est pas fourni, seule leur transcription en python par l'outil SWIG étant disponible en ligne. Cette transcription a pour particularité d'être difficilement exploitable. Il a donc été décidé de réaliser ces fonctions en utilisant l'outil GNU *Radio Companion* (GRC) pour l'élaboration d'un schéma de flux de traitement en temps réel des signaux reçus, et en implémentant un programme en langage C pour le traitement *a posteriori* des informations collectées.

Dans un premier temps nous avons procédé à la mise en place des PP dans le logement des RFP prévus à cet effet, ces derniers étant quant à eux reliés directement au secteur. Dans cette disposition, les RFP sont déjà en train d'émettre des paquets d'information. Plusieurs relevés réalisés avec l'outil usrp2_fft ont permis de mettre en évidence cette activité. À noter que les pics d'émission sont très rapides car transmis pendant un *slot*, aussi leur capture nécessite-t-elle de bons réglages. La figure suivante montre une activité sur les canaux[45] 3 et 6.

[45] Cf. tableau en annexe C, page XLI.

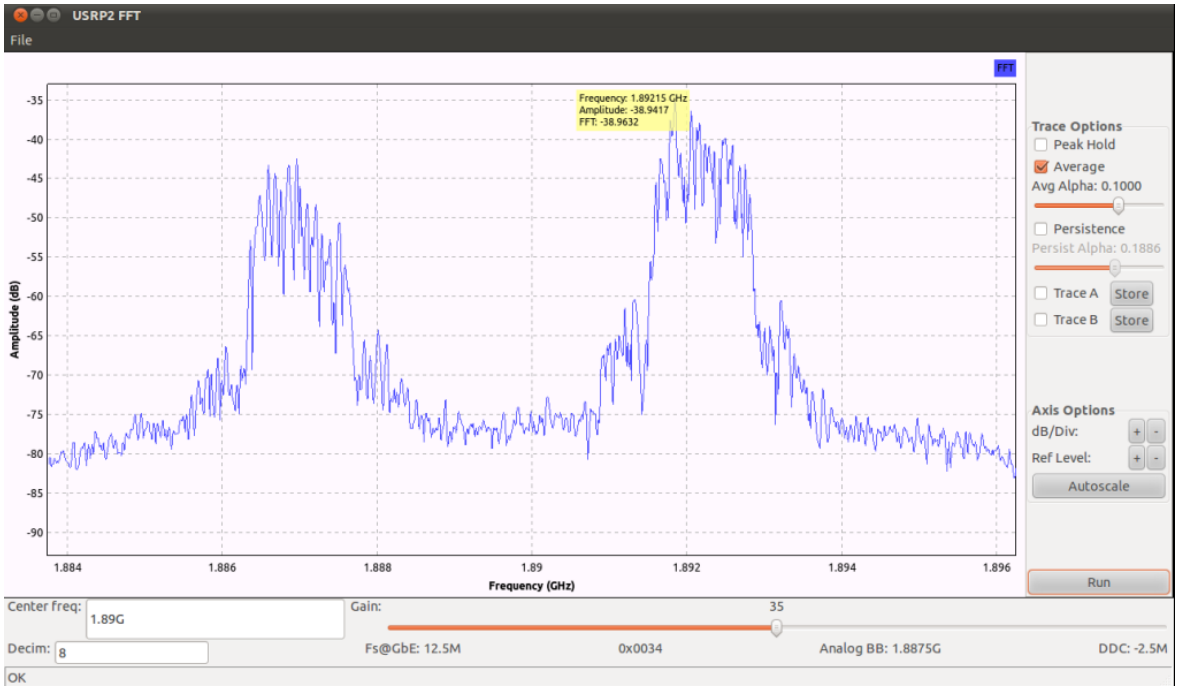

Figure 56: Canaux 3 et 6 DECT

Un autre relevé, effectué sur les canaux 2 (1893,888 MHz) et 3 (1892,160 MHz), montre également la présence de l'une des raies parasites (1,9 GHz) que nous avions mis en évidence au paragraphe IV.2.2.

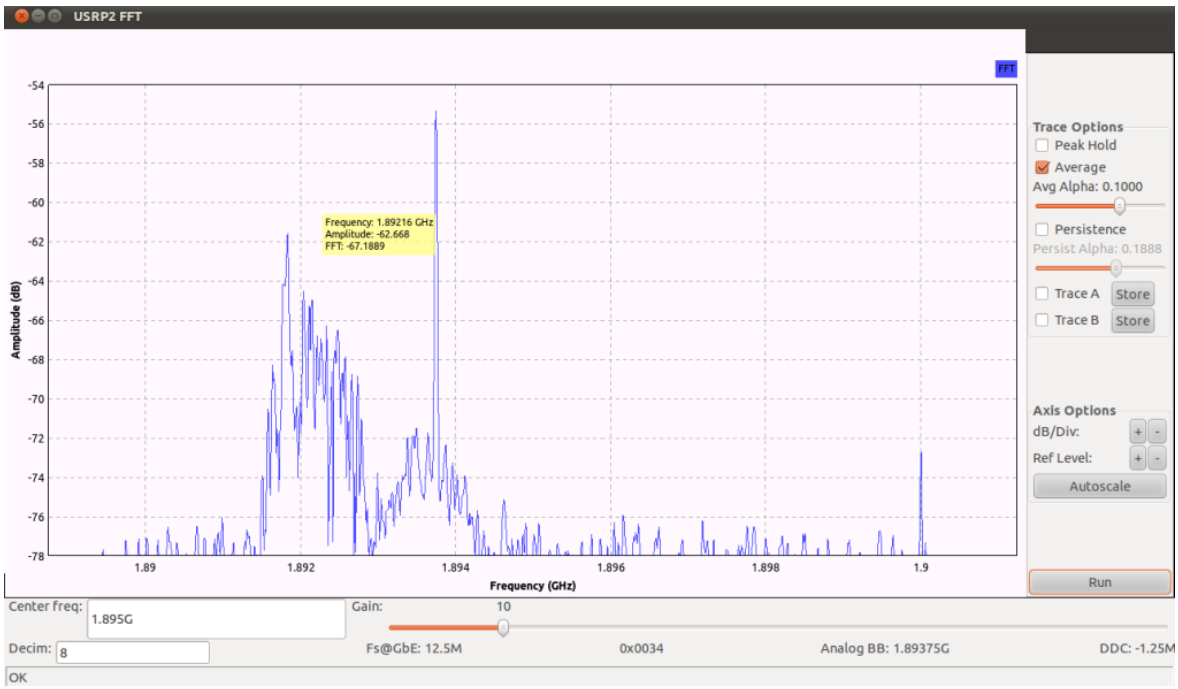

Figure 57 : DECT canaux 2 et 3, et raie parasite 1,9 GHz

Il est temps à présent d'utiliser les fonctionnalités de l'outil GRC pour réaliser différents traitements sur les signaux reçus, et notamment un filtrage de canal. Comme nous l'avions brièvement présenté au paragraphe I.4.4.4, GRC propose un certains nombre de blocs, notamment de traitement numérique du signal, de fonctions d'enregistrement, de déclaration de variables et de visualisation de courbes graphiques. Nous allons utiliser GRC pour d'une part effectuer un enregistrement des données collectées par l'USRP2 sur quelques secondes (au-delà d'environ une vingtaine de secondes en décimation 40, le PC hôte sature et se retrouve dans l'incapacité de traiter les informations arrivant de l'interface Gigabit Ethernet. Ce comportement se traduit par un affichage ininterrompu de ‘S’ en mode console), ensuite rejouer l'acquisition pour en visualiser le spectre à l'aide des blocs FFT *Sink* et *Waterfall*, puis effectuer un filtrage canal à l'aide d'un filtre FIR avec un paramétrage adéquat, utiliser un ré-échantillonneur rationnel pour obtenir un échantillonnage synchronisé sur le débit symbole, utiliser le démodulateur GMSK proposé pour récupérer le flux binaire utile, et enregistrer le résultat dans un fichier pour une exploitation *a posteriori*.

IV.3.2.2.2.1 Bloc source GRC USRP2

Tout graphe de flux exploitant les données issues d'un USRP2 utilise un bloc dit bloc source USRP2. Ce bloc contient un certain nombre de paramètres de contrôle de l'USRP2 (ceux qui sont marqués en rouge dans la fenêtre *Properties* de GRC sont obligatoires) :

- *Output Type* : ce paramètre permet de choisir le type de données en sortie,
- *Interface* : notation Linux de l'interface sur laquelle se connecte l'USRP2,
- MAC Addr : adresse MAC de l'interface Ethernet de l'USRP2,
- *Decimation* : facteur de décimation interne de l'USRP2 (entre 4 et 512),
- *Frequency* : fréquence centrale de réception de l'USRP2 (obligatoire),
- *LO Offset* : offset de fréquence appliqué sur l'OL du circuit réception de la carte RF,
- *Gain* : gain du récepteur (obligatoire).

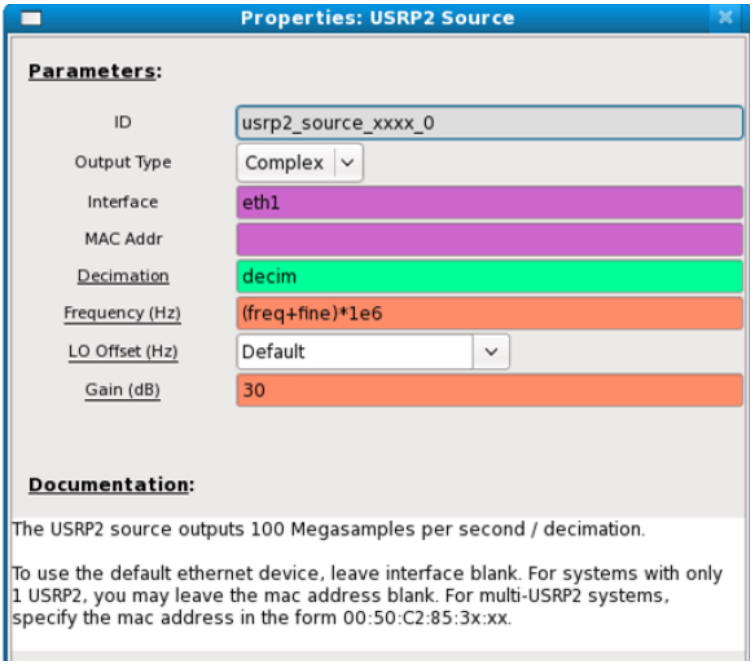

Figure 58 : Propriétés du bloc USRP2

Dans GRC la couleur des connecteurs de bloc indique le type des données utilisées, notamment : rose : *Byte* (8 bits) ; jaune : *Short* (entier sur 16 bits) ; vert : *Int* (entier sur 32 bits) ; orange : *Float* (virgule flottante sur 32 bits) et bleu : *Complex* (64 bits). Les paramètres d'un bloc GRC peuvent contenir soit des valeurs fixes, soit des variables (définies dans un bloc spécifique appelé « Variable »).

IV.3.2.2.2 Dimensionnement des paramètres RF

Pour mémoire les fréquences centrales des différents canaux DECT vérifient la relation :

$F_C = F0 - (c * 1,728\ MHz)$, où F_0 = 1897,344 MHz et c = 0, 1, …, 9.

Le taux d'échantillonnage des CAN de l'USRP2 est de 100 Méch/s, le débit brut du DECT en GFSK[46] est de 1,152 Msymbole/s (ou Mbit/s dans le cas présent).

IV.3.2.2.3 Calcul du taux de décimation du FPGA

Afin de ne pas perdre d'information pendant la phase d'échantillonnage le critère de Nyquist impose que le nombre d'échantillons par symbole (appelons-le `n`) doit être au moins égal à deux. Sachant que `n` correspond au rapport du taux d'échantillonnage en bande de base par le débit symbole brut du DECT, on en déduit que le taux d'échantillonnage en bande de base doit être supérieur à : `2 (échantillons par`

[46] En configuration 1a, cas le plus courant. Cf. tableau en annexe C page XLVI.

`symbole) * 1,152 Msymbole/s`, soit 2,304 Méch/s. Sachant également que le taux de décimation correspond au rapport du taux d'échantillonnage du CAN par le taux d'échantillonnage en bande de base, le taux de décimation doit être inférieur à : `100 Méch/s / 2,304 Méch/s`, soit environ 43,4. Compte tenu des valeurs utilisables dans l'USRP2, il est possible de choisir une valeur de décimation paire comprise entre 4 et 42. On choisira un facteur de décimation de 40 si l'on veut ne récupérer qu'un canal, et de 4 si l'on veut récupérer tous les canaux DECT.

IV.3.2.2.2.4 Acquisition d'un canal

Dans une première expérimentation nous allons appliquer sur le bloc source USRP2 une décimation de 40 (largeur de bande spectrale d'acquisition : 2,5 MHz) et une fréquence centrale de 1 893,888 MHz (canal 2), après avoir remarqué de l'activité sur ce canal à l'aide de `déDECTeur`. La figure suivante, obtenue en sortie du bloc source USRP2 et visualisée par un bloc FFT *sink* correctement paramétré, confirme l'utilisation du canal 2 par l'un des RFP utilisé (en vert la courbe des valeurs maximales ou *peak hold*).

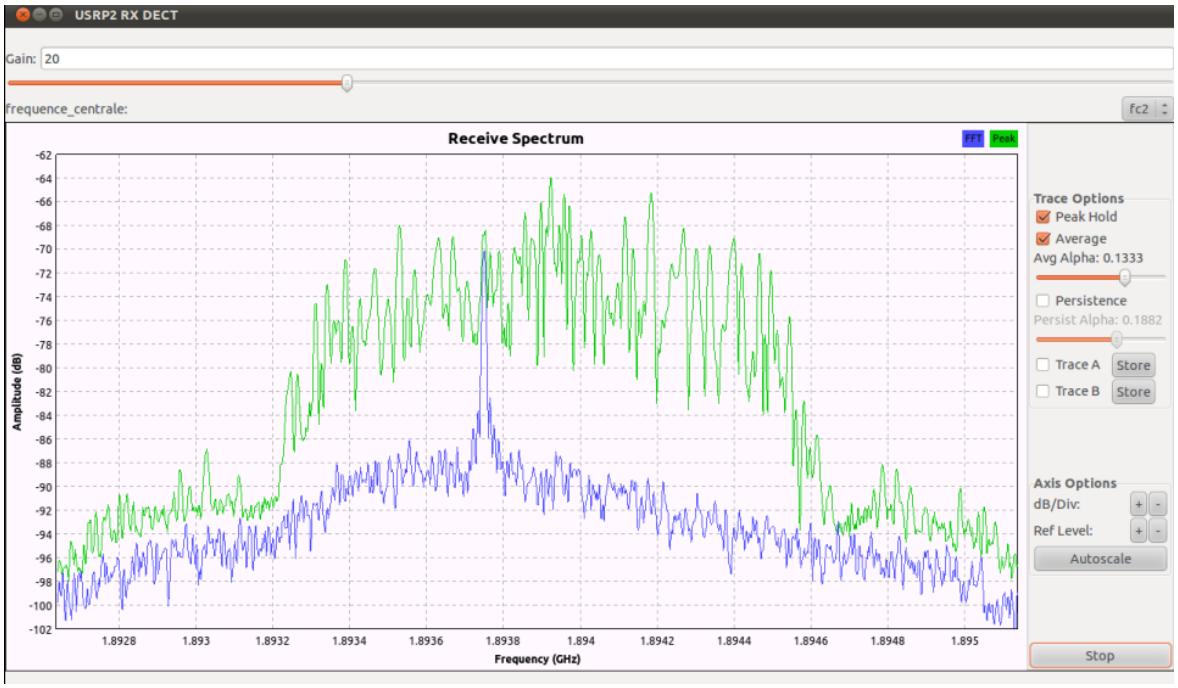

Figure 59 : Visualisation d'une activité sur canal 2 DECT à l'aide de GRC

Une opération identique a été réalisée sur le canal 5 pour visualiser la signature au spectrographe 2D des signaux DECT. Ce relevé fut particulièrement difficile à réaliser car on constate une saturation de l'ordinateur hôte au niveau de l'affichage graphique (l'écran se grise et une erreur OpenGL est générée) lorsque l'on cherche à obtenir une fenêtre de

visualisation verticale inférieure à cinq secondes. La figure suivante présente un des résultats obtenus. Les paramètres d'affichage ont été choisis de manière à clairement distinguer les pics d'activité de la (ou des RFP) sur ce canal.

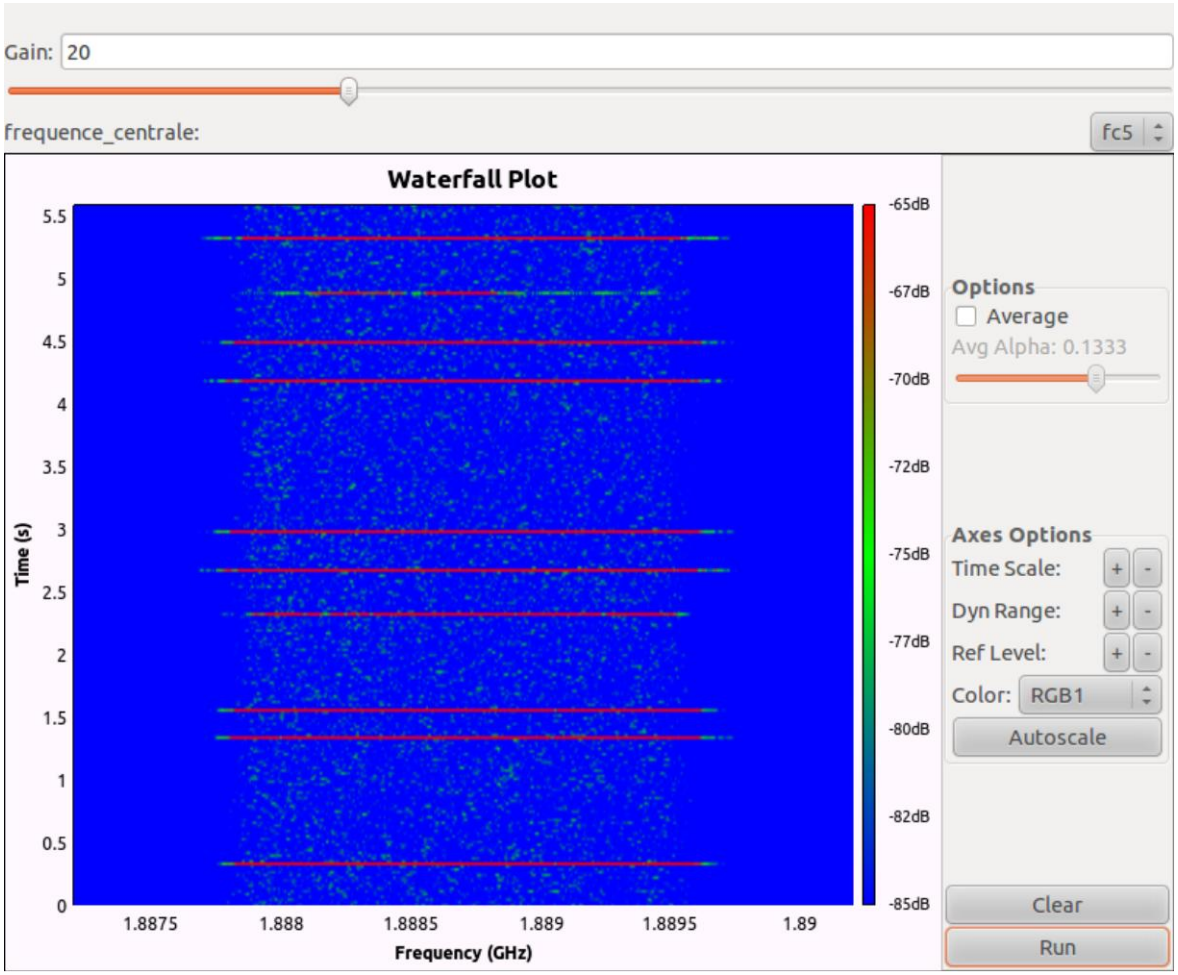

Figure 60 : Diagramme *waterfall* d'une activité DECT

IV.3.2.2.2.5 Filtrage de canal

Le filtre de canal utilisé est un filtre passe-bas FIR à décimation. Le nombre et la valeur des *taps* du filtre est obtenue à l'aide de la fonction `optfir.low_pass()` importée du répertoire `/gnuradio-core/src/python/gnuradio`. Cette fonction prend pour paramètres :

- le gain : 2 dB,

- la largeur de bande d'un canal : 1728 kHz + 100 kHz (marge de biais fréquentiel), soit 1828 kHz,

- la largeur de bande occupée : débit symbole * 1,03 (filtre Gaussien de BT = 0,5), soit 1186,56 kHz + 100kHz (marge de biais fréquentiel) = 1286,56 kHz,

- l'ondulation maximale dans la bande passante : 1 dB,

- et l'atténuation dans la bande coupée : 60 dB.

L'utilisation d'un bloc FFT *sink* en sortie du FIR permet de visualiser l'effet du filtre sur le spectre du signal. On distingue nettement dans la figure suivante (fréquence d'accord centrée sur le canal 8) la forme caractéristique de ce filtre ainsi que l'action principale de celui-ci, à savoir une forte atténuation hors de la bande d'intérêt[47].

Figure 61 : Effet du filtre de canal FIR

IV.3.2.2.2.6 Utilisation d'un ré-échantillonneur rationnel

Les valeurs de décimation applicables au FPGA de l'USRP2 étant entières, il n'est pas possible d'obtenir directement une valeur d'échantillonnage de 2,304 Méch/s. Pour obtenir cette valeur à partir des 2,5 Méch/s découlant d'une décimation de valeur 40, il est nécessaire d'appliquer en sortie de filtre FIR un ré-échantillonneur rationnel effectuant une décimation d'ordre 625 et une interpolation d'ordre 576. On obtient ainsi bien un échantillonnage à `2,5 Méch/s *(565/625)`, soit 2,304 Méch/s.

IV.3.2.2.2.7 Démodulation GFSK

[47] La courbe bleue correspond à de l'absence d'activité sur le canal. La courbe verte correspond au *peak hold* (valeurs maximales mesurées) et traduit donc une activité à certains instants. En l'absence de filtre, la courbe bleu serait quasi-monotone (faibles variations autour de -90dB dans le cas présent).

La modulation GFSK utilisée dans le DECT est une variante de la modulation à saut de fréquence FSK (*Frequency Shift Keying*), et plus précisément une variation de la modulation par saut de fréquence à variation continue de phase (CPFSK – *Continuous-Phase Frequency Shift Keying*). La FSK affecte à chaque symbole numérique une valeur de fréquence différente. Pour un nombre m de symbole, on parle de modulation FSK-m. En DECT (configuration 1a), m = 2. Une modulation à variation continue de phase permet de s'affranchir des variations brutales d'amplitude du signal, génératrices de signaux parasites.

A la différence de la modulation FSK, en GFSK le signal bande de base passe par un filtre passe-bas à forme gaussienne et à phase linéaire de manière à obtenir au niveau du spectre fréquentiel un lobe principal étroit et de faibles lobes adjacents, de façon à optimiser l'efficacité spectrale. On caractérise généralement le filtre gaussien par la valeur du produit $B*T_S$ (ou généralement écrit BTs, voire même BT), où Ts représente la durée d'un symbole, et B la fréquence de coupure à -3 dB du filtre gaussien. Pour la norme DECT, le produit BT est égal à 0,5.

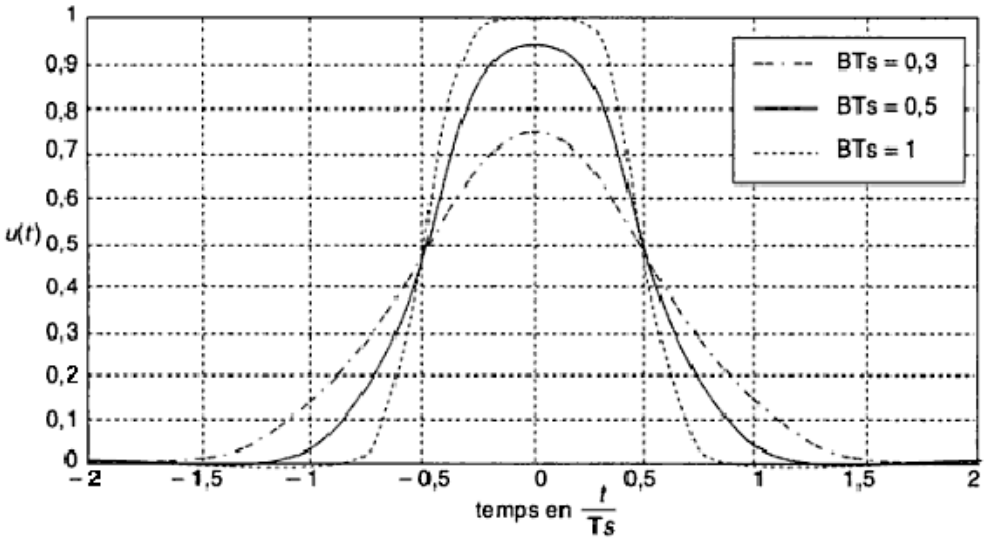

Figure 62 : Réponse d'un filtre Gaussien

Les algorithmes de démodulation des signaux modulés FSK sont applicables à ceux modulés en GFSK. Ils s'appuient sur la mise en œuvre de filtres adaptés, filtres dont la réponse en fréquence correspond exactement au spectre fréquentiel du signal d'entrée. Il existe deux types d'algorithmes de démodulation FSK : la démodulation synchrone (cohérente) et la démodulation asynchrone (non cohérente). En démodulation FSK synchrone, les réponses en amplitude et en phase du filtre adapté sont nécessaires pour démoduler le signal reçu. La connaissance de la phase du signal d'entrée est obligatoire.

Elle s'obtient par des techniques de corrélation. En démodulation asynchrone, seule la réponse en amplitude est nécessaire. La démodulation cohérente est plus performante mais plus complexe à mettre en œuvre.

Le module GRC de GNU Radio, pas plus que GNU Radio dans son ensemble, ne propose pas de démodulateur GFSK. Par contre il propose un démodulateur GMSK, c'est-à-dire un démodulateur MSK associé à un filtre passe-bas à forme gaussienne. Les modulations dites à saut de fréquence minimales ou MSK (*Minimum Frequency Shift Keying*) sont des modulations FSK particulières, généralement à quatre états, et qui n'autorisent que les transitions d'un état à un état voisin (+/- 90 °). Les deux fréquences instantanées de la porteuse modulées sont `f1 = f0 -1/4T` et `f2 = f0 + 1/4T`, où `f0` est fréquence centrale et `T` la durée d'émission d'un élément binaire. Les modulations MSK peuvent donc être considérées en première approximation comme des FSK-2 à phase continue. Dans le cas du DECT configuration 1a, 1/4`T` vaut `(1,152 MHz)/4`, soit 288 kHz, ce qui correspond exactement à la déviation fréquentielle nominale (cette déviation fréquentielle peut varier de 200 kHz à 400 kHz selon les motifs binaires transmis, cf. annexe C §C.2.3, raison pour laquelle on ne peut assimiler exactement une GFSK à une GMSK). Ce qui signifie que l'on peut utiliser ce démodulateur GMSK pour effectuer une démodulation GFSK, mais en prenant en considération qu'à rapport signal à bruit identique, le taux d'erreur binaire devrait logiquement être un peu plus élevé.

Le démodulateur GMSK proposé par GRC n'est quasiment pas documenté [reynwar]. Il s'avère toutefois qu'il s'agit d'un démodulateur FM non cohérent utilisant un système de récupération d'horloge basé sur la méthode de Mueller et Müller [gmskcr] [mueller]. Une sortie dure (*hard decision*) avec seuil fixe est utilisée aux instants d'échantillonnage pour récupérer les valeurs binaires [msg14933]. L'entrée est le signal complexe modulé en bande de base. La sortie est un flux de bits regroupé par octets et dont seul le LSB contient l'information utile. Les paramètres du démodulateur donnant les résultats les plus probants sont ceux de la configuration standard, présentés dans la figure suivante :

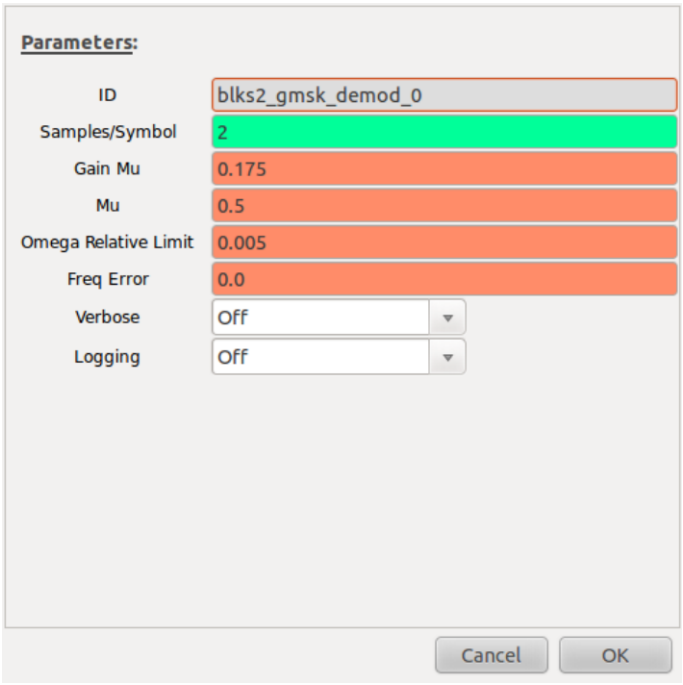

Figure 63 : Paramètres optimaux du démodulateur GSMK

Il s'avère que la modification de certains paramètres augmente le nombre de bits en sortie du démodulateur, le paramètre le plus sensible étant l'erreur en fréquence. Mais ces modifications n'apportent pas d'information supplémentaire et s'accompagnent d'une augmentation du taux d'erreur binaire. La figure suivante présente l'un des schémas GRC utilisés pour la démodulation d'un canal DECT.

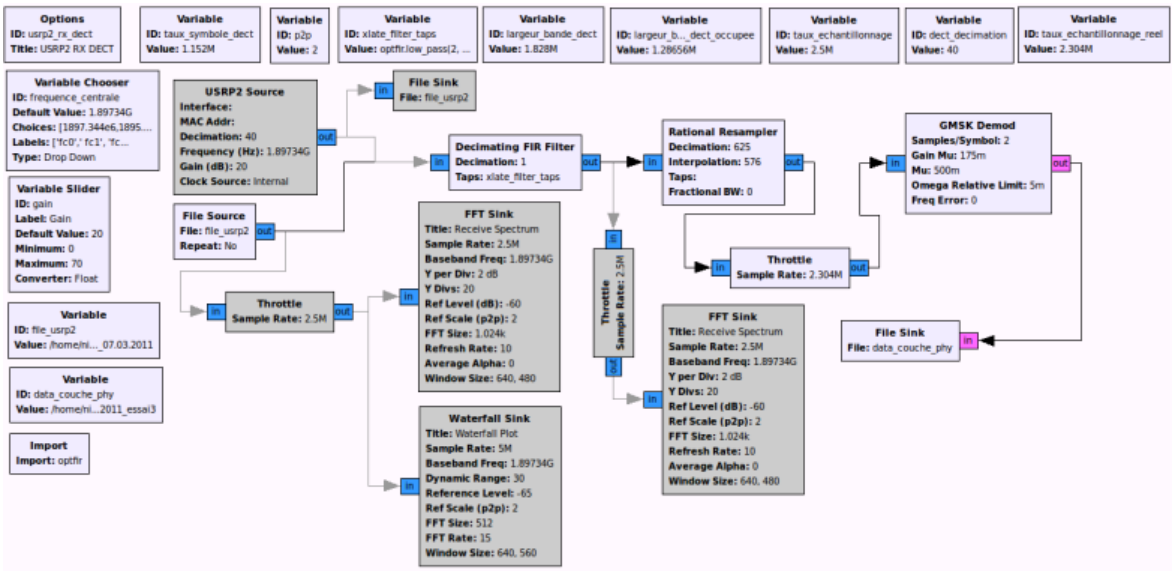

Figure 64 : Diagramme de flux GRC d'une démodulation de canal DECT

L'interprétation du fichier binaire obtenu à l'aide d'un éditeur hexadécimal a permis de mettre en évidence la forte récurrence du motif de synchronisation[48] (champ **S**) des RFP. La figure suivante en présente un exemplaire.

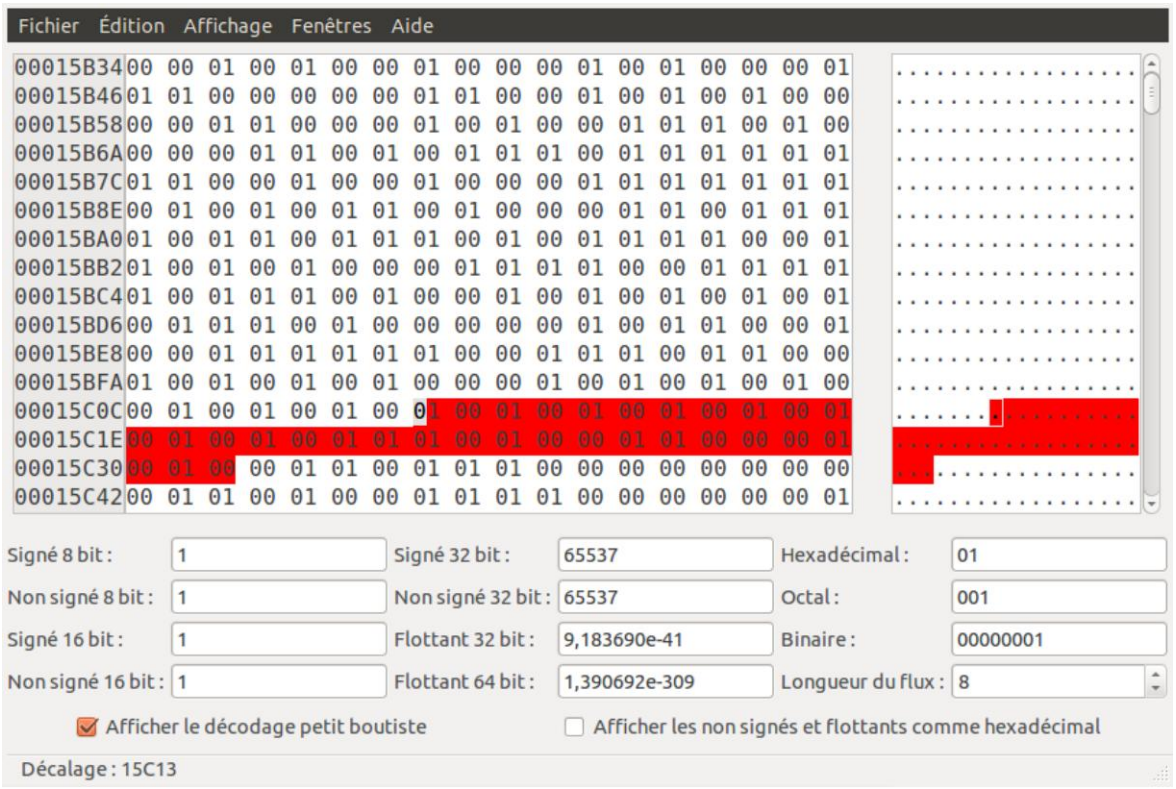

Figure 65 : Identification d'un champ S avec un éditeur hexadécimal

IV.3.2.2.2.8 Récupération de l'ensemble des canaux physiques DECT

L'étape suivante a consisté à réaliser un diagramme GRC capable de récupérer en une passe l'intégralité des canaux DECT en se centrant sur la fréquence centrale du canal 4, correspondant grosso modo au milieu du spectre DECT. Cette opération, nécessitant un facteur de décimation de valeur 4 au niveau de l'USRP2, provoque au bout de quelques secondes l'affichage par GNU Radio d'un message d'erreur (succession de 'S') indiquant que le système ne parvient plus à traiter l'afflux de données transmises par l'USRP2[49]. Le diagramme de flux réalisé contient autant de circuits de traitement distincts que de canaux à isoler. Chaque circuit assure un filtrage de canal à l'aide d'un filtre FIR à déplacement de fréquence (pour se centrer sur le canal à récupérer) et pour lequel on fixe un facteur de décimation égal à 10 (soit un échantillonnage à 2,5 Méch/s) afin d'isoler le bon canal. Le reste de chaque circuit est identique à celui utilisé pour la démodulation d'un canal. La

[48] Cf. annexe C §C.2.1.
[49] Un facteur de décimation de 4 implique que l'ordinateur hôte soit capable de traiter un débit de données de 800 Mbit/s, valeur proche du maximum supportable par une interface Gigabit Ethernet.

réalisation d'un tel schéma atteint les limites de ce qu'il est possible de faire avec la fenêtre graphique de GRC, les dimensions maximales de cette dernière étant fixes et non modifiables. La figure suivant présente un des schémas réalisés dans le cadre de ce que l'on peut qualifier, au sens de l'USRP2, de capture « large bande ».

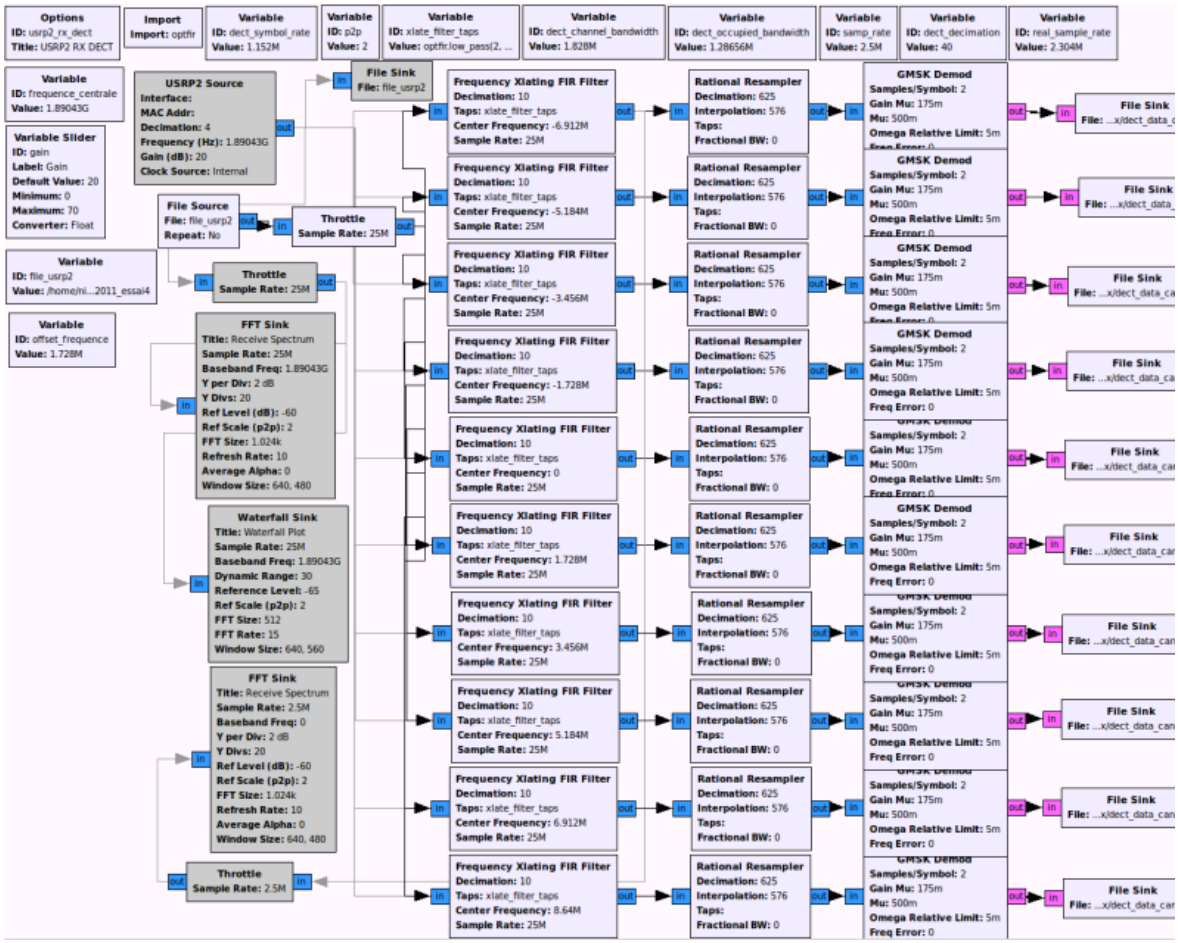

Figure 66 : Diagramme de flux GRC « large bande » d'une démodulation des 10 canaux DECT

Une deuxième configuration, un peu moins rapide à manipuler mais présentant la possibilité d'effectuer des acquisitions sur environ une dizaine de secondes, consiste à réaliser deux acquisition successives, une sur les canaux 0 à 4, l'autre sur les canaux 5 à 9, en se centrant respectivement sur les fréquences centrales des canaux 2 et 7, et en appliquant une décimation de valeur 8. Autre avantage, une disposition judicieuse des blocs de traitement permet de réaliser une architecture de capture « demi bande » plus simple (voir figure suivante) que le diagramme de flux « large bande » vu précédemment.

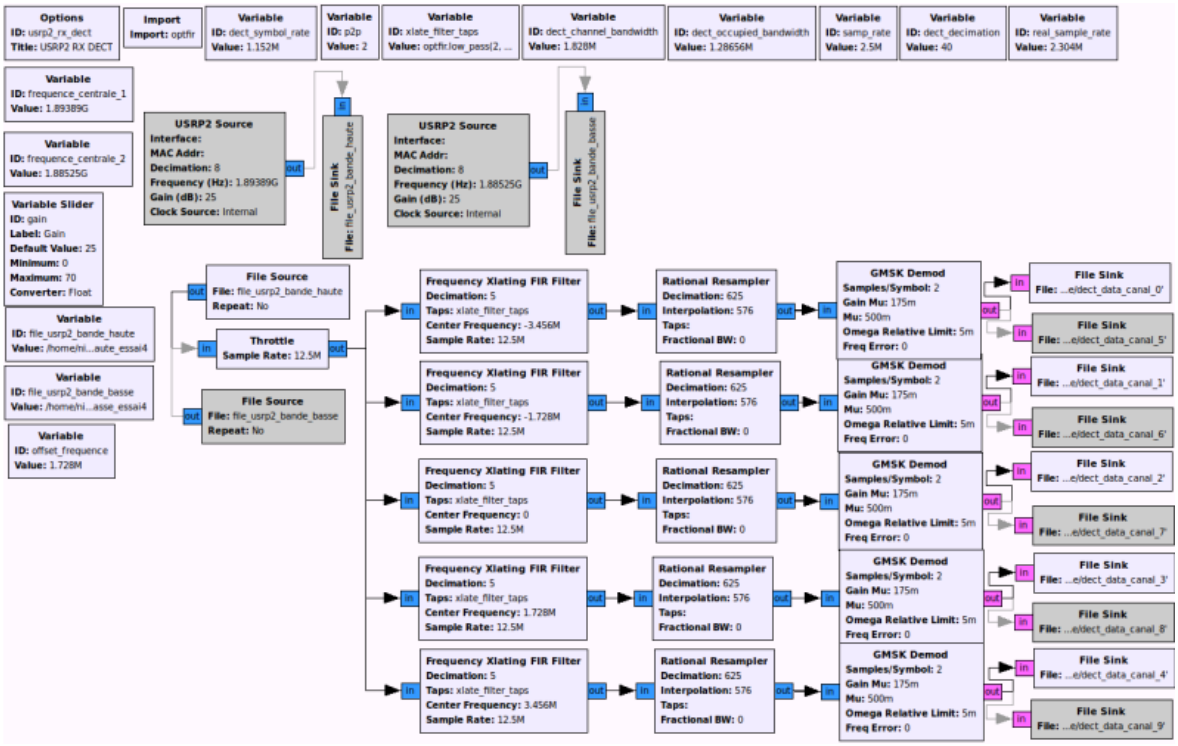

Figure 67 : Diagramme de flux GRC « demi bande » d'une démodulation des 10 canaux DECT en deux passes

L'étape suivante consiste à implémenter un programme en langage C, « dect_scan », afin de traiter des données en sortie de chaque démodulateur GSMK et d'en récupérer les informations relatives aux champs **A** contenant l'identité des RFP avoisinants (RFPI).

Une première approche consiste à récupérer chaque LSB des octets du fichier source à traiter et à les enregistrer dans un fichier texte. Cette méthode permet de manipuler des fichiers de taille huit fois plus petite, ce qui a pour principal avantage d'obtenir rapidement les informations utiles. Pour exemple, il faut moins de deux secondes pour analyser une acquisition d'une dizaine de secondes. Par contre, compte tenu du fait que la plus petite donnée manipulable par le langage C est l'octet, seuls les champs **S** parfaitement alignés avec l'algorithme de détection des motifs hexadécimaux sont détectés (soit dans le pire des cas un sur huit). Cette configuration est envisageable pour récupérer les RFPI contenus dans certains champs **A**. Mais l'analyse et l'affichage des champs composant le RFPI n'est pas triviale (mais toutefois réalisable) étant donné que la longueur de ces champs s'exprime en bits, et non en octets, et sont de longueur variable (cf. annexe C §C.4). De plus, ce code n'est pas pérenne dans le cadre d'une éventuelle réutilisation pour exploiter les champs **B**, c'est-à-dire ceux contenant les données utiles,

comme par exemple la voix. Dans ce cas, en moyenne sept informations sur huit ne seraient pas récupérées, ce qui n'est pas acceptable, surtout si elles sont chiffrées.

Il a donc été décidé de créer un second programme, « dect_scan2 », manipulant directement la représentation spécifique des octets en sortie du démodulateur GMSK, et effectuant une itération sur l'ensemble des dix fichiers correspondant à autant de canaux à analyser. Ces programmes effectuent pour chaque canal une détection et une comptabilisation des champs **S**, des champs N_T dont le CRC est correct, identifie les RFPI et les décomposent dans le cas de RFP de classe A (classe des équipements résidentiels et privés, correspondant à celle des équipements testés). Les figures suivantes présentent des extraits de résultats obtenus avec dect_scan et dect_scan2. Ce dispositif remplit pleinement l'objectif de récupération de l'identifiant (RFPI) des stations de base DECT avoisinantes et démontre la faisabilité d'analyse de ces RFPI.

```
Canal 0
Champ(s) S (RFP) detecte(s)
Champ(s) NT (RFP) detecte(s)
Identifiant de RFP (RFPI) : 01 75 3d 60 d0
Classe de l'équipement : A
Code du fabricant de l'équipement : 17 53
Numéro de FP : 109594
Numéro de RFP : 0 (FP monocellule)

Statistiques:
Nombre de champs S (RFP) detectes : 17
Nombre de champs NT (RFP) detectes (avec CRC correct) : 16
Nombre de RFPI differents detectes (avec CRC correct): 1

Canal 1
Champ(s) S (RFP) detecte(s)

Statistiques:
Nombre de champs S (RFP) detectes : 53
Nombre de champs NT (RFP) detectes (avec CRC correct) : 0
Nombre de RFPI differents detectes (avec CRC correct): 0

Canal 2
Champ(s) S (RFP) detecte(s)
Champ(s) NT (RFP) detecte(s)
Identifiant de RFP (RFPI) : 00 1a 93 e5 c8
Classe de l'équipement : A
Code du fabricant de l'équipement : 01 a9
Numéro de FP : 31929
Numéro de RFP : 0 (FP monocellule)

Statistiques:
Nombre de champs S (RFP) detectes : 62
Nombre de champs NT (RFP) detectes (avec CRC correct) : 55
Nombre de RFPI differents detectes (avec CRC correct): 1

Canal 3
Rien

Canal 4
Champ(s) S (RFP) detecte(s)

Statistiques:
Nombre de champs S (RFP) detectes : 44
Nombre de champs NT (RFP) detectes (avec CRC correct) : 0
Nombre de RFPI differents detectes (avec CRC correct): 0

Canal 5
Rien

Canal 6
Rien

Canal 7
Champ(s) S (RFP) detecte(s)
Champ(s) NT (RFP) detecte(s)
Identifiant de RFP (RFPI) : 00 12 ac d6 98
Classe de l'équipement : A
Code du fabricant de l'équipement : 01 2a
Numéro de FP : 105171
Numéro de RFP : 0 (FP monocellule)

Statistiques:
Nombre de champs S (RFP) detectes : 60
Nombre de champs NT (RFP) detectes (avec CRC correct) : 52
Nombre de RFPI differents detectes (avec CRC correct): 1

Canal 8
Rien

Canal 9
Rien

Process returned 0 (0x0)   execution time : 1.535 s
Press ENTER to continue.
```

Figure 68 : `dect_scan`

```
Canal 0
Champ(s) S (RFP) detecte(s)
Champ(s) NT (RFP) detecte(s)
Identifiant de RFP (RFPI) : 01 75 3d 60 d0
Classe de l'équipement : A
Code du fabricant de l'équipement : 17 53
Numéro de FP : 109594
Numéro de RFP : 0 (FP monocellule)

Statistiques:
Nombre de champs S (RFP) detectes : 128
Nombre de champs NT (RFP) detectes (avec CRC correct) : 112
Nombre de RFPI differents detectes (avec CRC correct): 1

Canal 1
Champ(s) S (RFP) detecte(s)

Statistiques:
Nombre de champs S (RFP) detectes : 399
Nombre de champs NT (RFP) detectes (avec CRC correct) : 0
Nombre de RFPI differents detectes (avec CRC correct): 0

Canal 2
Champ(s) S (RFP) detecte(s)
Champ(s) NT (RFP) detecte(s)
Identifiant de RFP (RFPI) : 00 1a 93 e5 c8
Classe de l'équipement : A
Code du fabricant de l'équipement : 01 a9
Numéro de FP : 31929
Numéro de RFP : 0 (FP monocellule)

Statistiques:
Nombre de champs S (RFP) detectes : 391
Nombre de champs NT (RFP) detectes (avec CRC correct) : 344
Nombre de RFPI differents detectes (avec CRC correct): 1

Canal 3
Rien

Canal 4
Champ(s) S (RFP) detecte(s)

Statistiques:
Nombre de champs S (RFP) detectes : 370
Nombre de champs NT (RFP) detectes (avec CRC correct) : 0
Nombre de RFPI differents detectes (avec CRC correct): 0

Canal 5
Rien

Canal 6
Rien

Canal 7
Champ(s) S (RFP) detecte(s)
Champ(s) NT (RFP) detecte(s)
Identifiant de RFP (RFPI) : 00 12 ac d6 98
Classe de l'équipement : A
Code du fabricant de l'équipement : 01 2a
Numéro de FP : 105171
Numéro de RFP : 0 (FP monocellule)

Statistiques:
Nombre de champs S (RFP) detectes : 422
Nombre de champs NT (RFP) detectes (avec CRC correct) : 372
Nombre de RFPI differents detectes (avec CRC correct): 1

Canal 8
Rien

Canal 9
Rien

Process returned 0 (0x0)   execution time : 36.859 s
Press ENTER to continue.
```

Figure 69 : `dect_scan2`

La figure suivante présente un schéma synoptique du dispositif complet d'acquisition et d'analyse de signaux DECT. Le FPGA de l'USRP2 a été utilisé dans sa configuration standard. Contrairement à certaines implémentations SDR où les traitements

temps réel synchrones sont implémentés dans le FPGA, ici l'essentiel du traitement est mis en œuvre dans le logiciel s'exécutant sur le PC, la problématique temps réel n'étant pas dans le cas présent un prérequis opératoire. Cette plateforme démontre ainsi que pour mettre en œuvre un récepteur DECT avec traitements *a posteriori*, il n'est pas nécessaire d'utiliser des solutions logicielles et matérielles temps réel spécialisées et coûteuses.

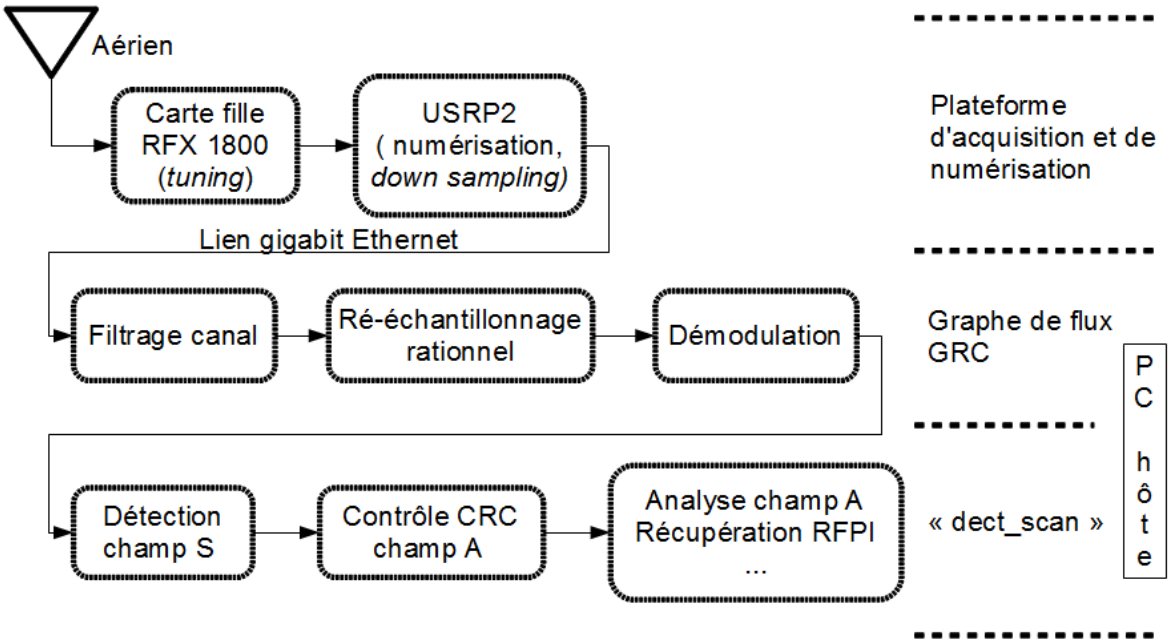

Figure 70 : Dispositif d'acquisition et d'analyse de signaux DECT

Conclusion

Ce stage avait plusieurs objectifs. Il consistait dans une première partie à effectuer une étude complète de la technologie radio logicielle. Une seconde partie était dédiée à la recherche bibliographique des radios logicielles présentes sur le marché ou chez les organismes de recherche. L'étude particulière des systèmes USRP1 et USRP2 et de l'architecture logicielle GNU Radio a conduit à effectuer une recherche sur les tentatives d'implémentation de protocoles de radiocommunication sur ces plateformes, objet de la troisième partie. La mise à disposition d'un USRP2 et de quelques cartes RF a permis de réaliser quelques applications pratiques, décrites en dernière partie.

L'utilité de la radio logicielle s'est imposée au regard de la prolifération des standards de transmission radiofréquence. Elle a investi de nombreux domaines tels que les radios tactiques, la téléphonie mobile, le radioamateurisme et les équipements de test ou de mesure. Nous avons pu constater que la mise en œuvre d'une radio logicielle idéale était bloquée par des contraintes technologiques actuellement non résolues, et que la quasi-intégralité des radios logicielles actuelles implémente un circuit de transposition analogique de fréquence pour rendre le signal radiofréquence exploitable par les circuits de numérisation.

Parmi les diverses architectures logicielles existantes, deux d'entre elles semblent être privilégiées : SCA, principalement utilisée par l'industrie de défense et quelques équipes universitaires (version « libre » OSSIE), et surtout GNU Radio, solution « libre » disposant d'une communauté active (radioamateurs, universitaires, etc.). GNU Radio n'est toutefois pas un produit finalisé et fait régulièrement l'objet d'améliorations et de correctifs, d'où son qualificatif « d'architecture presque mature de développement de radios logicielles ». Les interfaces graphiques GRC et WXGUI *Signal Analysis Tools* ne sont pas des modèles de stabilité et gagneraient à être étoffées de fonctionnalités supplémentaires, notamment pour la prise en compte des couches protocolaires supérieures à la couche physique (PHY). De nombreux outils « libres » de visualisation et d'analyse de signaux captés par des radios logicielles existent mais ne sont pour la plupart qu'adaptés à un usage radioamateur (bande passante étroite).

A l'instar des environnements logiciels, les plateformes matérielles de radio logicielle sont nombreuses mais pour la plupart dédiées à la communauté radioamateur (bande de fréquences limitée, bande passante étroite). Quelques modèles dits « professionnels » sont proposés par des équipementiers. Leurs performances semblent bonnes mais leur prix d'achat, comparable à celui des outils de mesure type oscilloscope ou analyseur de spectre, peut en décourager plus d'un. La famille des USRP constitue un bon compromis. Abordables techniquement et financièrement, ces plateformes d'acquisition et de numérisation de signaux sont particulièrement adaptées pour réaliser des études et expérimentations sur des normes de transmission radiofréquence, moins pour remplacer un équipement spécialisé dans l'implémentation d'un standard de radiocommunication particulier. Certains inconvénients de l'USRP1 (bande passante insuffisante pour certains standards, faible débit de la liaison USB2.0 entre l'USRP1 et le PC hôte) ont été en partie gommés avec l'USRP2, mais on a notamment pu constater que le filtrage de signaux parasites internes n'a pas été pris en compte. La capacité à implémenter des techniques et protocoles de transmission radiofréquence dernière génération nécessiterait également quelques améliorations telles qu'une augmentation de la capacité de traitement en embarqué, pour gagner en rapidité de traitement du signal et par exemple être en mesure de suivre des techniques d'évasion de fréquence ou d'effectuer des traitements applicatifs temps réel.

La conception de systèmes à base de radios logicielles relève dans la pratique plus du défi que du jeu d'enfant. L'emploi d'une radio logicielle « libre » exige généralement de solides compétences en informatique et une connaissance étendue des techniques de radiocommunication et de traitement numérique du signal. Par exemple, l'exploitation de la GNU Radio et des USRP requiert des connaissances approfondies dans de nombreux domaines, dont notamment les systèmes de transmission sans fil, le traitement (numérique et analogique) du signal (transposition, échantillonnage, design des filtres FIR, FFT, conversion I/Q, modulations/démodulations, techniques de détection, de synchronisation, algorithmes, etc.), la conception de circuits et la programmation orientée objet. Il faut notamment bien comprendre comment fonctionnent les différents éléments de traitement du signal utilisés dans les circuits d'émission et de réception (rôle de la carte RF, convertisseurs A/N et N/A, mélangeurs, fonctions des DUC et DDC, amplificateurs avec contrôle de gain, détecteurs, démodulateurs, décodeurs, format des données, etc.) et ensuite savoir comment exploiter les données brutes pour en extraire des données utiles (couches

protocolaires supérieures à la couche PHY). Autre point à prendre en compte : les spécifications techniques des radios logicielles « libres » type USRP sont nettement moins documentées que leurs homologues professionnelles.

GNU Radio fournit un certain nombre de blocs de traitement du signal, mais à l'usage on se rend rapidement compte qu'ils sont loin de prendre en compte tous les cas de figure. Pour réaliser des circuits dits simples (émetteur/récepteur AM ou FM), l'utilisation du GNU Radio Companion (GRC) peut s'avérer suffisante et dans ce cas, seul une connaissance de la programmation en Python peut être nécessaire. Au-delà de ce niveau de complexité, il devient nécessaire de créer ses propres scripts Python, voire dans le cas de configurations plus sophistiquées, de créer ses propres blocs de traitement du signal, voire de modifier la configuration standard du processeur de traitement numérique du signal embarqué sur la carte mère de la plateforme matérielle d'acquisition et de numérisation. Dans ce cas la connaissance d'un langage de description de circuits est nécessaire. D'une manière générale, GRC implémente peu de fonctions de démodulation, encore moins de décodage, et pas grand chose pour le traitement des données. Les traitements de niveau supérieur à la couche PHY, à savoir les couches protocolaires, devront donc systématiquement être programmés, comme ce fut le cas lors de l'étude réalisée sur le DECT.

Le succès commercial des solutions à base de SDR était jusqu'à récemment limité à cause du coût élevé et du peu de flexibilité des équipements programmables disponibles. Comparée au coût nettement supérieur (rapport de dix, voire plus) des SDR propriétaires, la configuration "USRP + GNU Radio" est très attractive, d'autant que les solutions dites professionnelles ne sont pas « libres ». Avec l'arrivée de la GNU Radio une révolution dans les technologies de SDR est en marche et va permettre de réduire considérablement les coûts de développement et de déploiement de plateformes radios logicielles. Ce nouveau paradigme est mis en évidence par le nombre grandissant de projets d'applications radio récemment développées : récepteur RDS FM, solutions RFID, récepteur GPS, applications 802.11a/b/g/p et 802.15.4, etc.

Table des annexes

Annexe A
Architectures de récepteurs de radio logicielle

A.1 Récepteur superhétérodyne

Dans un récepteur superhétérodyne à FI analogique, le signal issu de l'antenne passe par un filtre RF à onde de surface pour isoler la bande de réception, puis est amplifié par un LNA, est ensuite transposé (en une ou plusieurs étapes) autour d'une fréquence intermédiaire (FI) fixe, de nouveau amplifié, puis attaque un démodulateur quadratique effectuant une transposition en bande de base centrée sur la fréquence centrale du canal souhaité, et est ensuite numérisé pour enfin pouvoir faire l'objet d'un traitement numérique. La tête de réception est donc quasi entièrement analogique. La conversion en flux numérique est réalisée en bande de base juste avant exploitation par le processeur de traitement numérique du signal.

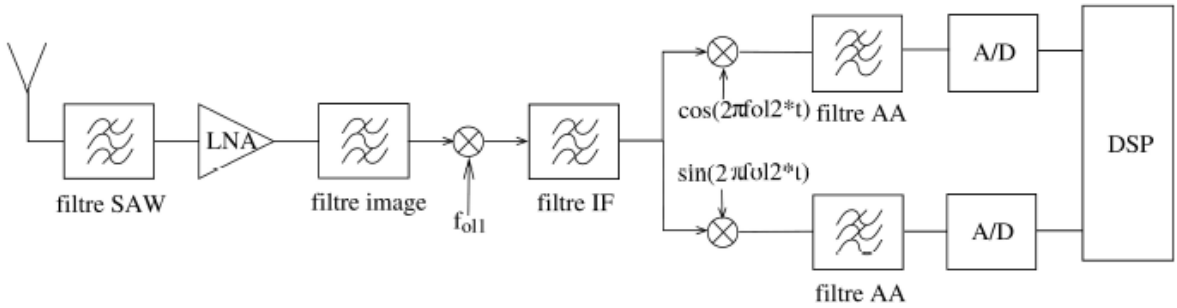

Figure 71 : Architecture d'un récepteur hétérodyne avec FI analogique [perez]

Cette multiple transposition fréquentielle du spectre est assurée par la multiplication du signal RF avec le signal d'un oscillateur local (OL, ou en anglais LO – *Local Oscillator*) de fréquence F_{OL1}, ensuite par la multiplication du signal résultant avec un second OL de fréquence variable F_{OL2}. Un filtre de réjection d'image est placé avant le premier mélangeur car tout signal symétrique au signal RF utile par rapport à F_{OL1} (dit "signal image") se retrouverait après mélange autour de la fréquence intermédiaire et pourrait nuire à la détection du signal utile.

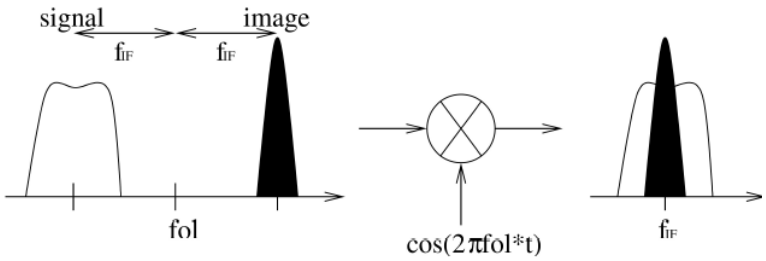

Figure 72 : Effet d'une fréquence image sur le signal utile

Un filtre FI de grande sélectivité réalise un préfiltrage avant le deuxième mélangeur. Le passage de "fréquence intermédiaire" à "bande de base" et la sélection du canal nécessitent de décomposer le signal sur deux voies I et Q à l'aide de deux mélangeurs en quadrature.

Le récepteur superhétérodyne à FI analogique constitue une solution de frontal RF à bon rapport efficacité/coût. Il présente notamment de bonnes performances en termes de sélectivité et de sensibilité. Le filtrage progressif des interférences permet de gérer les contraintes de linéarité du récepteur. Parmi les inconvénients, on peut noter la nécessaire réjection de la fréquence image, la susceptibilité aux fréquences parasites proches de la fréquence intermédiaire et la nécessité d'utiliser des cellules d'adaptation d'impédance. Cette architecture implique également l'utilisation de filtres de grande qualité et n'est pas adapté à un usage multibande (le gabarit des filtres étant lié à la norme choisie). Mais le principal inconvénient est que la plupart des composants analogiques ne sont pas réglables. C'est aussi le concept de radio logicielle le plus éloigné de la règle consistant à exécuter en numérique le plus d'opérations possibles, et hérite donc des inconvénients des circuits analogiques (difficulté de configuration, sensibilité aux perturbations, etc.).

Si différents formats de modulation doivent être gérés, les bandes passantes désirées doivent être soigneusement examinées. Par exemple, si le récepteur gère à la fois du GSM (largeur d'un canal : 200 kHz) et de l'UMTS (largeur d'un canal : 5 MHz), alors les bandes passantes du filtre FI, des filtres antirepliement, et du CAN (et donc le taux d'échantillonnage) doivent être choisies en fonction de la bande la plus large. L'inconvénient est qu'alors en mode GSM, de multiples canaux pourraient apparaître dans la bande FI. Cette difficulté peut être surmontée par un filtrage bande de base réglable, utilisant par exemple des techniques à capacités commutées, toutefois génératrices de bruit. Cette approche classique ne peut être concrètement employée que pour un traitement bande étroite (un seul canal).

L'étage final de démodulation I/Q est un bon candidat pour une implémentation numérique remplaçant l'OL et le réseau de déphasage 90°. Ceci a l'avantage d'éliminer l'erreur de phase et de réduire les fuites de l'OL. Cette solution est communément appelée récepteur à numérisation en fréquence intermédiaire. Cette solution utilise une tête analogique pour la transposition en fréquence intermédiaire, puis un CAN et une démodulation I/Q.

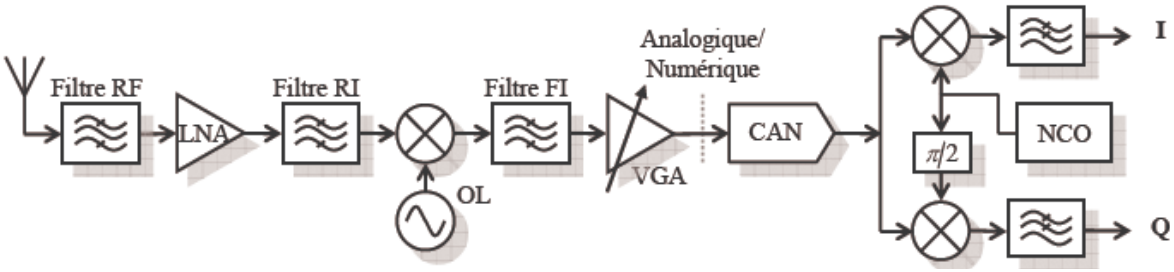

Figure 73 : Récepteur superhétérodyne avec numérisation en FI

La transposition en bande de base est réalisée après le CAN, au sein d'un processeur de traitement numérique du signal. Cette transposition numérique a pour avantage de présenter une quadrature quasi parfaite et exempte de tout offset. De plus, l'emploi d'un processeur de traitement numérique du signal en sortie du CAN permet d'implémenter d'autres fonctionnalités telles que par exemple la détection du format de modulation, le contrôle automatique de gain ou de fréquence, la compression et l'entrelacement des données, et la détection voire la correction d'erreurs.

A.2 Récepteur à conversion directe

La création de récepteurs à conversion directe, dits homodynes ou " Zéro FI ", a été motivée par la problématique de filtrage de la fréquence image. Dans une architecture de réception homodyne le signal RF issu de l'antenne est filtré puis amplifié avec un LNA, puis directement transposé en bande de base à l'aide d'un OL réglé sur la valeur de la porteuse du canal à démoduler (la fréquence intermédiaire FI est donc nulle), et ensuite numérisé. Cette solution nécessite toutefois un bon filtre avant le LNA pour éviter toute interférence de signaux voisins forts. Le filtre antirepliement (AAF, *Anti-Aliasing Filter*) supprime le repliement spectral. Le contrôle automatique de gain (AGC, *Automatic Gain Control*) adapte l'amplitude du signal en sortie du filtre AAF à la dynamique d'entrée du CAN.

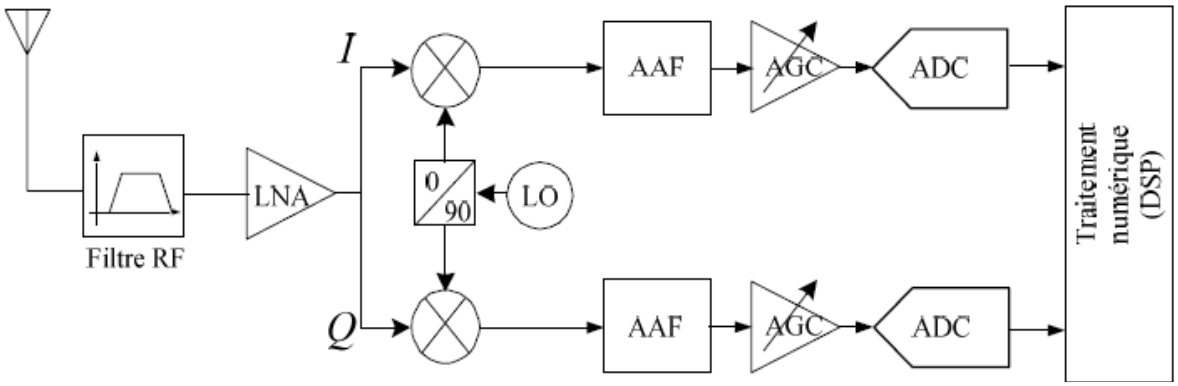

Figure 74 : Architecture de réception à conversion directe (homodyne)

On remarque au passage que le filtre FI n'est plus nécessaire, pas plus que les circuits d'adaptation d'impédance et les étages intermédiaires d'un récepteur hétérodyne. Il est dès lors possible, hormis pour le filtre RF et l'antenne, d'intégrer entièrement la tête RF analogique sur puce. Cette architecture a deux principaux avantages : il n'y a pas de transposition en FI (et donc pas de réjection de la fréquence image) et les CAN/CNA utilisés sont standards et donc peu coûteux. En revanche cette solution présente plusieurs inconvénients. Tout d'abord une contrainte forte pèse sur l'OL. En effet ce dernier doit être capable de s'adapter à tout type de porteuse. Ensuite le mélangeur n'isole pas parfaitement le LNA de l'OL, et inversement. Le signal issu de l'OL est susceptible de remonter jusqu'à l'antenne et de nouveau se mélanger avec lui-même, générant un offset de tension variable et de forte puissance, entraînant une saturation des étages d'amplification et du CAN ainsi qu'une dégradation du rapport signal à bruit en réception (cf. figure suivante). Une solution palliative consiste à employer des algorithmes de compensation d'offset [perez]. De plus l'appariement des voies I et Q à fréquence élevée génère une erreur de phase ou de gain, avec pour conséquence une augmentation du taux d'erreur binaire. Enfin les mélangeurs du circuit de réception sont saturables par des émetteurs dans des canaux adjacents.

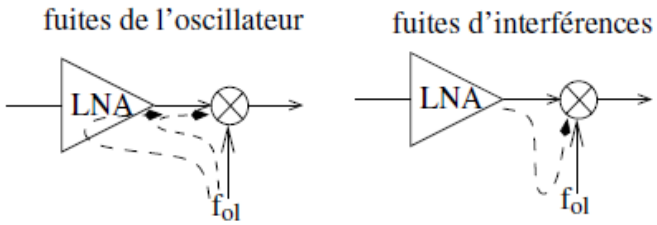

Figure 75 : Fuites du LNA et de l'OL

Malgré tous ses défauts cette architecture est populaire car elle concilie une simplicité du traitement RF, un haut niveau d'intégration et un degré de configuration se

rapprochant du concept défini par la radio logicielle. Selon [desimone] les récepteurs à conversion directe sont particulièrement adaptés aux applications monocanal telles que la téléphonie mobile et sont également les plus recommandés actuellement pour une réception multistandard. Citons pour exemple le récepteur RF à conversion directe CMX994 de CML Microcircuits, intégré sur une seule puce [cml]. Ce circuit, qui fonctionne dans la bande [100 MHz – 1 GHz], intègre la quasi-totalité des étages nécessaires à la réalisation d'un récepteur à conversion directe : un LNA, un convertisseur et un démodulateur I/Q à grande dynamique et un OL commandé en tension ou VCO (*Voltage Controlled Oscillator*) intégré dans une boucle à verrouillage de phase ou PLL (*Phase Locked Loop*).

A.3 Récepteur *Low-IF*

Dans une architecture de récepteur à faible fréquence intermédiaire ou *Low-IF*, le signal RF est transposé en une FI faible mais non nulle, centrée sur des largeurs de bande de ½ à 2 canaux. Cette architecture permet un degré élevé d'intégration, tout en évitant les offsets de tension.

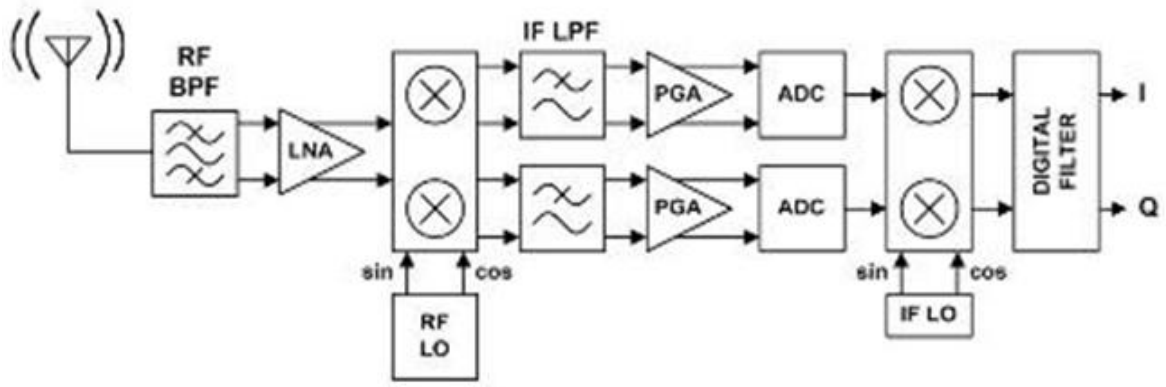

Figure 76 : Diagramme par blocs d'un récepteur *Low-IF* [edom]

A l'instar de la conversion directe, cette architecture impose des contraintes importantes sur les composants en termes de dynamique et de linéarité. Elle est également sensible aux erreurs d'appariement des voies I et Q, et nécessite une réjection des fréquences images. Un compromis est alors à trouver entre une FI suffisamment élevée pour éviter que des canaux adjacents ne perturbent le signal à traiter, et suffisamment basse pour maintenir de bonnes performances lors de l'échantillonnage.

A.4 Numérisation en RF avec sous-échantillonnage

Dans ce cas de figure le signal RF est directement numérisé. L'idée est d'utiliser le CAN (respectivement CNA) comme système de transposition fréquentielle. Cette architecture utilise la transposition directe en bande de base du spectre du signal échantillonné. Les inconvénients majeurs de cette solution sont la dégradation importante du rapport signal à bruit, la nécessaire utilisation d'un filtre très sélectif, et de fortes contraintes (bande passante analogique de plusieurs gigahertz) sur le CAN (respectivement CNA).

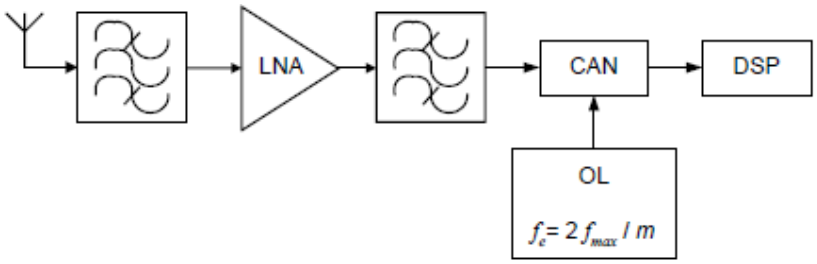

Figure 77 : Architecture d'un récepteur à numérisation en RF

Certains nouveaux appareils peuvent effectivement échantillonner directement le signal RF, mais uniquement pour un usage spécifique. Texas Instrument vend par exemple un composant Bluetooth (le BRF6150) ne nécessitant pas de transposition côté analogique [ti2]. Les contraintes imposées aux CAN sont toutefois telles que la numérisation en RF n'est pour le moment pas généralisable.

Annexe B
Description détaillée d'une SDR

B.1 Introduction

Les récepteurs radio historiques convertissent généralement leurs signaux RF en une fréquence intermédiaire (FI), plus facile à exploiter et indépendante du canal radio écouté. Les SDR modernes font de même ou cherchent à convertir directement le signal radio en numérique, réduisant ainsi la composante de traitement analogique. Cependant la deuxième solution implique des contraintes extrêmes sur la bande passante et la dynamique des CAN et CAN, ramène une grande quantité du bruit thermique de l'antenne dans le circuit de réception et constitue au final une solution assez coûteuse. Par conséquent, la plupart des radios logicielles utilise encore les mêmes techniques de transposition en FI que les radios matérielles. Un contrôle automatique de gain est ajouté pour maximiser la dynamique des signaux qu'un récepteur peut traiter. Les équipements les plus sophistiqués appliquent des opérations de filtrage et de conversion de fréquence minimisant les signaux parasites, images et interférences dans la gamme de fréquences de fonctionnement.

Dans une architecture de réception SDR typique, le frontal RF amplifie puis convertit la fréquence porteuse du signal à récupérer en une fréquence intermédiaire (FI) de sorte que le signal puisse être numérisé par un CAN, puis traité par un processeur de traitement numérique du signal assurant la fonction de modem (détection et correction des symboles reçus). De même, l'émetteur est composé du modem produisant une représentation numérique du signal à transmettre, puis d'un CNA générant une représentation en bande de base ou en FI du signal. Ce signal est alors décalé en fréquence à la fréquence porteuse désirée, amplifié jusqu'à un niveau de puissance approprié et transmis à l'antenne. Si la radio doit transmettre et recevoir simultanément, il y a aussi du filtrage pour limiter les interférences du signal transmis vis à vis du circuit de réception. Le schéma suivant présente l'architecture matérielle typique d'une SDR. L'équipement dispose de ressources logicielles suffisantes pour définir la fréquence porteuse, la bande passante, la modulation, les opérations cryptographiques et le codage de source. Les ressources matérielles peuvent comprendre un mélange de GPP, DSP, FPGA ou autre ressource de calcul, de façon à gérer un large éventail de modulations.

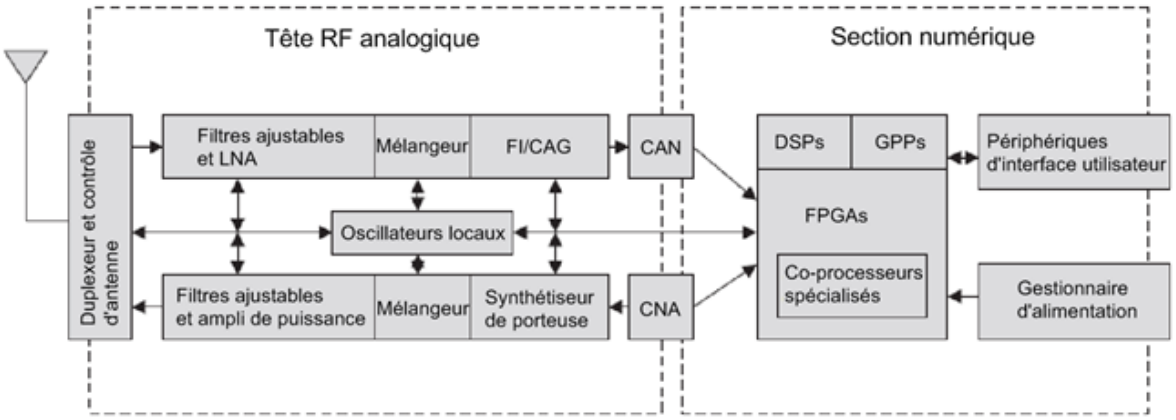

Figure 78 : Architecture matérielle générique d'une SDR

Dans le sens émission un processeur de traitement numérique du signal (DSP – *Digital Signal Processing*) délivre un signal numérique en bande de base. Ce dernier est injecté dans un convertisseur/éleveur numérique ou DUC (*Digital Up-Converter*) transposant le signal bande de base complexe en FI. Le CNA qui suit convertit les échantillons numériques en signal analogique. Le signal est ensuite transposé de FI en RF. Enfin, l'amplificateur de puissance augmente l'énergie du signal pour être rayonnée par l'antenne, l'objectif étant de synthétiser un signal RF avec les caractéristiques attendues, sans introduire de bruit ou de rayonnement risquant d'interférer avec d'autres utilisateurs du spectre radiofréquence.

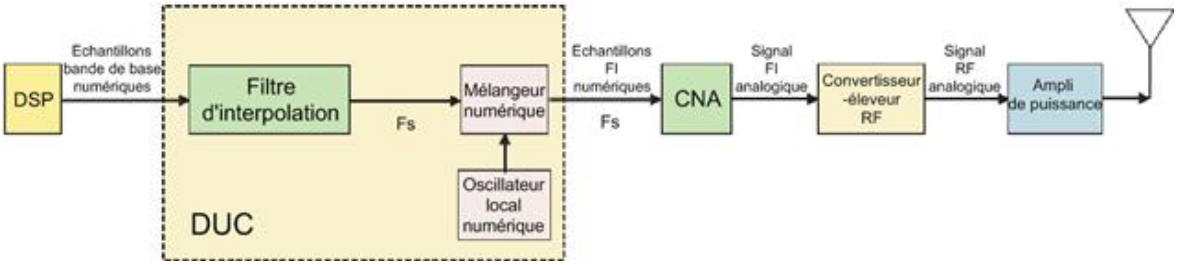

Figure 79 : Émetteur SDR avec DUC

Dans le sens réception le signal est capté par l'antenne, subit quelques traitements analogiques (filtrages, amplification faible bruit, transposition de RF en FI) et est numérisé par un CAN, l'objectif étant de numériser le signal utile et uniquement celui-ci. Les échantillons numériques sont ensuite transmis à une convertisseur/abaisseur numérique ou DDC (*Digital Down-Converter*) généralement réalisé avec une puce monolithique ou un FPGA, pour être convertis en bande de base puis traités par le DSP.

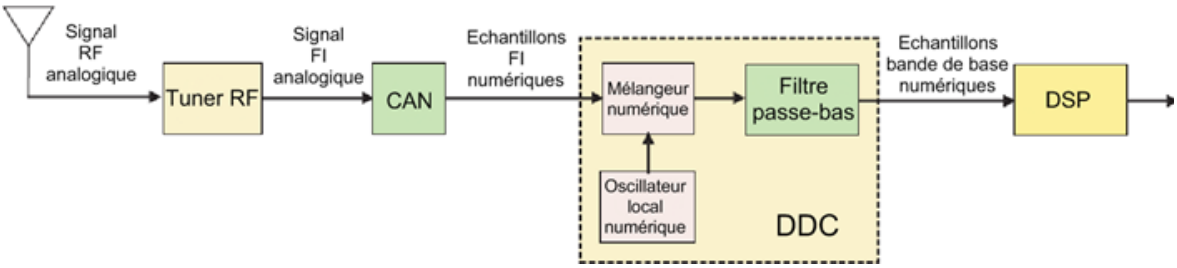

Figure 80 : Récepteur SDR avec DDC

Détaillons maintenant les différents éléments constitutifs d'une SDR, en commençant par l'antenne.

B.2 Circuit d'antenne

La première composante matérielle d'une SDR à considérer est l'antenne[50]. Celle-ci reçoit les signaux utiles et indésirables. Comme il n'existe pas encore d'antenne «universelle» offrant un rendement suffisant dans toutes les bandes de fréquences, les antennes de SDR demeurent spécifiques à un besoin donné. Un autre aspect à prendre en compte lors de la conception d'antennes à large bande, c'est que la puissance de bruit thermique capté par l'antenne augmente linéairement avec la bande passante. Pour toutefois répondre aux performances attendues d'une SDR, il est conseillé de disposer d'antennes multifréquences, multibandes et paramétrables (diagramme de rayonnement, polarisation, bande de fréquences, fréquence porteuse,...). L'utilisation de différents filtres, chacun optimisé pour une bande de fréquences donnée, permet ensuite le traitement de signaux associés à différentes normes. Parmi les diverses antennes existant sur le marché, celles qui se prêtent le mieux à la radio logicielle sont les antennes multibandes, les antennes à résonance réglable et les antennes intelligentes (*smart antenna*).

B.2.1 Antenne multibande

Les radios multibandes RF exigent généralement au moins une antenne par décade. Dans cette configuration, la conception de l'antenne peut ne pas être optimale pour une bande particulière, mais demeure le meilleur choix en terme de coût et de qualité de service. Un exemple d'antenne multibande est l'antenne patch à micro-ruban (*micro-strip patch antenna*).

[50] Une antenne est un composant électronique permettant de rayonner et/ou de capter les ondes électromagnétiques. On utilise différents types d'antennes pour différentes fréquences radio et pour différentes couvertures. Une antenne est principalement caractérisée par son diagramme de rayonnement (directive, omnidirectionnelle, etc.), son gain, sa bande passante, et sa polarisation.

B.2.2 Antennes à résonance réglable

Depuis que la radio logicielle promet des traitements large bande et flexibles, on en attend de même de l'antenne. L'idée de base derrière tous les modèles d'antenne programmable est de gagner en capacité de changer les propriétés de résonance de l'antenne en utilisant uniquement des signaux commandés par logiciel, c'est à dire sans utiliser d'interrupteurs manuels.

Plusieurs concepts d'antenne à résonance réglable ont été testés, mais aucun n'a encore dépassé le stade du laboratoire. Citons par exemple le réseau d'antenne à base de résonateurs électromécaniques (réseau d'antenne patch configurable), où chaque élément résonne à une fréquence différente, ces mêmes éléments étant reliés entre eux par des commutateurs micro-électro-mécaniques ou MEMS (*Micro-Electro-Mechanical Systems*) bi-statiques à commande optique. Grâce à cette technique il est possible de reconfigurer l'antenne pour s'adapter à différentes bandes spectrales. La stabilité de phase de cette antenne est toutefois perfectible, et le diagramme d'antenne trahit les interférences entre les éléments utilisés et non utilisés.

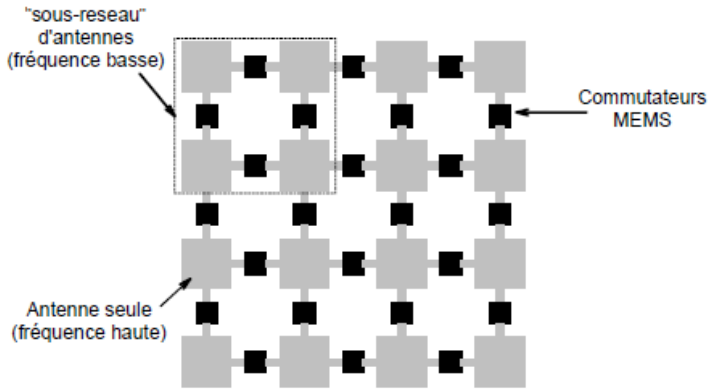

Figure 81 : Réseau d'antenne patch configurable

Figure 82 : Utilisation de commutateurs MEMS dans une antenne configurable

Un autre concept d'antenne utilise des matériaux qui changent leurs propriétés capacitives et inductives en fonction de la tension de polarisation. Ces matériaux sont en mesure de modifier leur fréquence de résonance d'environ 10 %, mais avec d'importantes pertes. Citons également une conception composée de plusieurs segments pouvant être reliés ou non pour modifier la fréquence de résonance. Mais ses performances sont

médiocres en raison des imperfections dans la construction et des interactions avec les éléments inutilisés. Les efforts visant à créer des modèles d'antenne basés sur des exigences plus faibles ont rencontré plus de succès. Le laboratoire scientifique du NXP *Semiconductors* a présenté deux antennes dimensionnées pour le GSM multimode et les téléphones cellulaires 3G. Une utilisait des MEMS pour les segments d'une antenne quart d'onde PIFA (*Planar Inverted-F Antenna*) modifiée, et l'autre utilisait deux PIFA. Les deux configurations offrent de bonnes performances, avec des pertes d'insertion de moins de 6 dB pour les bandes GSM850, GSM900, GSM1800, GSM1900 et UTRA I (UMTS *Terrestrial Radio Access*).

B.2.3 Antennes intelligentes

Les antennes intelligentes sont composées d'une matrice d'antennes différentes dont les signaux subissent un post-traitement ajustable de manière à améliorer leurs performances. Il existe quatre principaux types de traitement d'antenne intelligente : la formation de faisceau (*beam forming*), la combinaison de diversité[51], l'égalisation espace-temps et la technologie MIMO. Le *beam forming* combine les signaux d'antenne afin de modifier la réponse de l'antenne vis-à-vis de l'angle d'incidence, de façon à renforcer le niveau de réception des signaux souhaités, et à atténuer le bruit résiduel. La combinaison de diversité atténue l'évanouissement (*fading*) multitrajet en combinant les signaux de l'antenne. L'égalisation espace-temps corrige les distorsions de fréquence introduites par le canal à l'aide d'un traitement temporel des signaux reçus par les différentes antennes. Enfin, la technologie MIMO (*Multiple-Input Multiple-Output* ou "entrées multiples, sorties multiples" en français) utilise plusieurs antennes, tant au niveau de l'émetteur (2 à 7) que du récepteur (2 ou 3) pour établir plusieurs canaux en simultané et augmenter le débit. La configuration matérielle requise pour supporter les systèmes d'antennes intelligentes sont les mêmes que pour les applications d'émission ou de réception multicanal. Chaque élément d'antenne doit disposer de son propre ensemble de conversion RF/FI et CAN/CNA. Tout le reste du traitement d'antenne intelligente est géré par logiciel.

Les antennes utilisées sur une large gamme de fréquences requièrent un tuner d'antenne asservi aux changements de fréquence, afin d'optimiser le ROS (Rapport d'Ondes Stationnaires). Certaines antennes modernes sont équipées d'un certain nombre de

[51] La diversité est caractérisée en réception par la présence de plusieurs répliques indépendantes d'une même information. Elle peut être spatiale, temporelle, fréquentielle ou mixte (mêlant les techniques précédentes).

composants passifs répartis sur toute la longueur des éléments rayonnants, et sont en mesure de présenter un ROS raisonnable. Les meilleures d'entre elle couvrent une décade (exemple 10-100 MHz). Dans le cas de radios exploitant des bandes plus larges (exemple : 2 MHz à 2 GHz), on s'attend à ce que l'équipement radio dispose d'un moyen de sélection de l'antenne approprié à une bande de fréquences donnée, voire également d'un dispositif de contrôle du pointage de l'antenne.

Les antennes intelligentes font la plupart de leurs traitements en bande de base. Les antennes elles-mêmes, les composants de transposition RF/FI et de numérisation sont les mêmes que pour tout autre système à antennes multiples. Le véritable travail de formation de faisceau, de traitement de la diversité, de codage espace-temps, et/ou de MIMO est réalisé au niveau logiciel.

Le *Wireless Innovation Forum* a défini une API pour gérer les antennes intelligentes [api]. Elle prend en charge le contrôle, la synchronisation, et les fonctions algorithmiques. Les opérations de traitement des antennes intelligentes s'exécutent sur un GPP, et peuvent donc facilement supporter CORBA, tandis que les composants qui traitent réellement les données radio provenant des antennes s'exécutent sur des DSP ou FPGA, composants qui ne supportent pas facilement CORBA, mais y sont interfacés via des adaptateurs logiciels.

B.2.4 Interaction entre antennes

La séparation physique des antennes dans les systèmes multibandes est importante. Par exemple, dans un système avec une antenne HF et une antenne UHF colocalisées, une séparation des antennes de 3 mètres au lieu de 30 centimètres augmente l'affaiblissement du signal hors-bande de 20 dB. Plusieurs radios proches les unes des autres peuvent provoquer des interférences. Normalement, les règles de fonctionnement sont créées afin de limiter le nombre de radios pouvant créer des interférences dans la même zone au même moment, et les SDR intelligentes peuvent également atténuer l'impact de ces interférences en évaluant l'environnement radio afin d'adapter leurs paramètres de transmission.

B.2.5 Autres critères de performance

Le bruit de phase est un critère important pour les modulations sensibles aux variations de phase, comme par exemple les modulations d'amplitude en quadrature (MAQ) à plus de 16 états. Par exemple, les antennes à balayage électronique génèrent un fort bruit de phase lors des commutations.

Dans les applications de SDR portable, l'interaction de l'antenne avec le corps humain doit être prise en considération. En outre, il existe des limites réglementaires sur la quantité de rayonnement auquel le corps humain peut être exposé.

L'étude de l'interaction entre l'émetteur et le récepteur est importante lors de la conception d'une SDR. Un émetteur transmettant n'importe où dans la bande d'un récepteur large bande le surchargera. Certaines radios matérielles utilisent un multiplexeur de fréquence pour séparer les bandes d'émission et de réception, méthode pouvant être reprise dans une SDR. Cependant, une conception de SDR multibande aura besoin d'autres moyens pour se protéger de la surcharge du récepteur, car les multiplexeurs de fréquence n'ont généralement pas assez de bande passante pour gérer ce type de fonctionnement. A défaut, une SDR multibande peut utiliser plusieurs multiplexeurs, par exemple un par bande, mais une telle configuration peut s'avérer coûteuse.

B.3 Tête RF analogique

L'une des plus importantes opérations réalisées par la tête RF analogique d'une SDR est la transposition analogique de fréquence (conversion haute de RF vers FI en réception, et conversion basse de FI vers RF en émission) et la récupération des voies I et Q, dont les divers cas de figure sont présentés en **annexe A** (superhétérodyne, conversion directe, etc.). D'autres constituants sont également importants et font donc ci-après l'objet d'un développement particulier.

B.3.1 Amplificateur de puissance RF

L'amplificateur de puissance (AP), actif en mode émission, fournit généralement sa puissance nominale sur une charge résistive de 50 ohms mais son impédance peut être beaucoup plus faible (5 Ω à 10 Ω, par exemple). Il est en général capable d'indiquer son ROS, le niveau de puissance transmis et sa température de fonctionnement. Les nouveaux systèmes cellulaires, telles que le CDMA et les normes de téléphonie mobile 3G et 4G, exigent un contrôle de puissance sur chaque trame, impliquant de 50 à 100 modifications du niveau de puissance par seconde.

Les AP introduisent des distorsions telles l'ondulation d'amplitude en fonction de la fréquence et la distorsion de phase. L'ondulation d'amplitude dégrade la puissance transmise. Des techniques telles que le *pre-emphasizing* de FI et la compensation de l'amplitude du flux de symboles transmis peuvent compenser cette ondulation. Les non-linéarités de l'AP provoquent des interférences dans les canaux adjacents au canal

d'émission/réception. La prédistorsion est une technique qui peut être utilisée pour rendre linéaire l'amplificateur de puissance. L'idée est de créer une distorsion à l'entrée de l'AP qui annule les distorsions créées par l'AP lui-même. En fonction de la distorsion, ceci peut être effectué en bande de base ou en RF. La prédistorsion dans le domaine RF est réalisée avec des circuits analogiques, et est capable de rendre linéaire l'amplificateur sur la bande passante tout entière en une seule opération. C'est la méthode à retenir lorsque la prédistorsion nécessaire est connue à l'avance. Une autre forme de prédistorsion analogique est la prédistorsion cubique, conçue pour réduire les harmoniques du troisième ordre introduites par le CNA. Théoriquement une prédistorsion peut être réalisée en bande de base, mais il est difficile de la mettre en œuvre car l'on doit tenir compte lors de son calcul de nombreux autres facteurs, tels que le canal choisi et les distorsions du CNA.

Une technique de linéarisation répandue est connue sous le nom d'anticipation ou *feed-forward* (cf. figure suivante). Elle est couramment utilisée pour les stations de base, et bien qu'elle soit difficile et coûteuse à mettre en œuvre, elle peut réduire la distorsion d'intermodulation ou IMD (*Inter-Modulation Distortion*) à moins de -55 dBc sur une largeur de bande instantanée de 30 MHz. Cette technique peut également être utilisée en conjonction avec la prédistorsion RF. L'amplificateur à anticipation consiste en l'appariement d'un amplificateur principal avec un amplificateur d'erreur. La sortie de l'amplificateur principal est combinée avec une image retardée du signal d'entrée, créant un signal d'erreur qui est alors amplifié et soustrait à la sortie de l'amplificateur principal après avoir passé une ligne à retard. Les éléments de temporisation sont réglés de façon à compenser les retards dans les deux amplificateurs. L'inconvénient de cette solution est qu'elle ne facilite pas la mise en œuvre d'un asservissement.

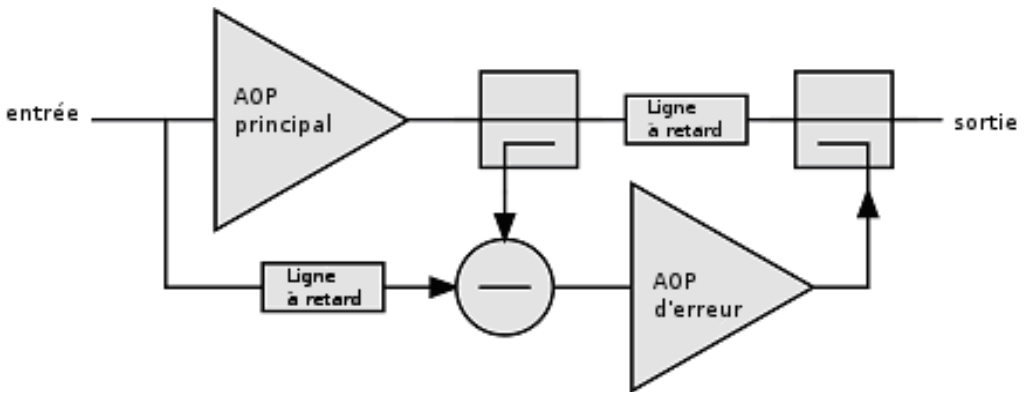

Figure 83 : Amplificateur à anticipation (*feed-forward amplifier*)

La technique du *feed-forward* présente de nombreux avantages, notamment la conservation du gain dans la bande et une stabilité inconditionnelle. De plus l'amplificateur d'erreur n'a pas besoin d'être aussi puissant que l'amplificateur principal. Ses inconvénients sont qu'elle ne permet pas de compensation en température et en dérive due à l'âge, requiert des exigences strictes au niveau des composants, et est plus complexe à réaliser comparé à un amplificateur traditionnel.

B.3.2 Amplificateur faible bruit

Les signaux reçus par l'antenne sont d'un niveau très faible, de l'ordre de -100 dBm (0,1 nW). Pour pouvoir exploiter ces signaux, le circuit de réception doit utiliser un amplificateur RF introduisant le moins de bruit possible, à savoir un LNA. La linéarité des LNA pour traiter des signaux de dynamique élevée constitue leur principal point bloquant.

B.3.3 Composants analogiques programmables

Une radio logicielle restreinte peut contenir au niveau de sa tête RF analogique des composants particuliers appelés composants analogiques programmables ou FPAA (*Field Programmable Analog Array*). Ces circuits intégrés, composés de blocs analogiques et d'interconnexions configurables, constituent en quelque sorte l'équivalent analogique des FPGA et permettent ainsi de concevoir et d'implémenter des fonctions analogiques programmables. Un bloc analogique est généralement composé d'un amplificateur opérationnel et d'un réseau de composants passifs. Certaines dernières générations de FPAA ont été renommées dpASP (*Dynamically Reconfigurable Analog Signal Processor*). Pour exemple, la société Anadigm propose le dpASP AN231E04 [an231].

B.4 Convertisseurs analogique/numérique (CAN)

B.4.1 Caractéristiques techniques

L'élément le plus critique d'un récepteur radio logicielle est l'étage de conversion analogique/numérique. La numérisation de signaux large bande à grande dynamique, nécessaire à la numérisation de diverses formes d'onde, impose la conception de convertisseurs présentant des performances élevées en précision et en fréquence d'échantillonnage. Une conversion correcte du signal est essentielle car les éventuelles distorsions ajoutées à cette étape ont une incidence directe sur le rapport signal à bruit de l'équipement radio. Dans le cas d'un émetteur, des distorsions ajoutées lors de la conversion numérique/analogique risquent également de provoquer une situation de non-conformité réglementaire en raison de signaux indésirables générés hors-bande.

Un CAN comporte principalement quatre éléments : un filtre antirepliement pour supprimer les fréquences indésirables risquant de se mélanger au signal utile, un circuit d'échantillonnage/blocage pour maintenir le signal d'entrée à un niveau constant pour la quantification, un quantificateur pour traduire la tension analogique (maintenant stabilisée) en un mot numérique, et une mémoire tampon (*buffer*).

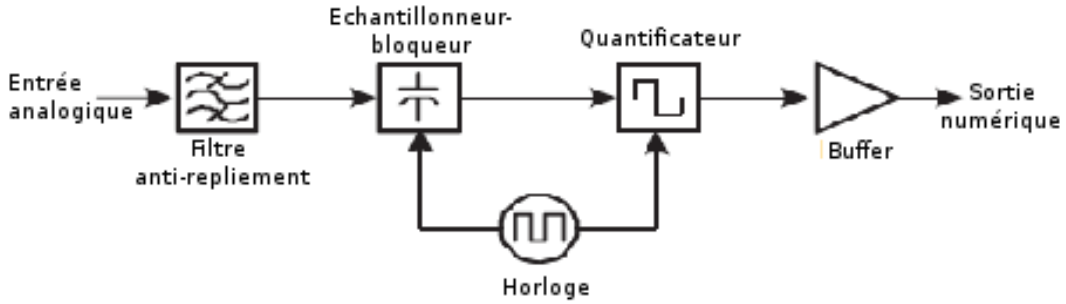

Figure 84 : Schéma fonctionnel d'un CAN

Les performances des CAN sont limitées par trois principaux phénomènes : le *slew rate* des circuits analogiques intégrés, entraînant une réduction de la dynamique de codage ou SFDR (*Spurious Free Dynamic Range*) à mesure que la fréquence augmente, le *jitter* de l'horloge[52] et la dynamique de réception[53]. Le choix du taux d'échantillonnage est aussi important. Plus il est élevé, mieux c'est. Il doit être au moins deux fois supérieur à la bande passante du signal traité (critère de Nyquist). Par exemple, un système traitant un signal de 40 MHz de bande passante doit être conçu pour échantillonner à au moins 80 MHz. Il faut toutefois prendre soin de bien filtrer les harmoniques de niveau 2 et 3 présentes en dehors de la bande d'intérêt, par exemple à l'aide d'un filtre numérique implémenté par un DSP. De même, on veillera à choisir un circuit dont l'IMD est la plus faible possible.

Deux autres caractéristiques importantes d'un CAN sont le niveau de bruit et la SFDR. Dans une infrastructure cellulaire, les récepteurs doivent traiter des signaux très faibles de l'ordre de -100 dBm en présence de signaux dits « bloqueurs », d'où l'importance d'une SFDR et d'un rapport signal à bruit (SNR - *Signal to Noise Ratio*) élevés. Une technique utilisée pour améliorer la SFDR est le *dither*. Le *dither* est un bruit pseudo aléatoire injecté dans l'entrée analogique du CAN. Avec cette technique des technologies

[52] Le *jitter* d'horloge est une variation aléatoire de l'horloge par rapport à sa caractéristique idéale, provoquée par un facteur externe (la source de l'horloge) et des imperfections internes au circuit. Lorsque l'horloge varie légèrement, cela altère la précision d'échantillonnage et dégrade le rapport signal à bruit.

[53] La dynamique de réception est le rapport entre le plus grand signal exploitable et le plus petit signal détectable. Elle est dépendante du niveau de bruit, de la dynamique sans parasites, et du produit d'intermodulation du troisième ordre du récepteur. L'environnement d'exploitation et plusieurs parties du récepteur, notamment les filtres, ont un impact sur la dynamique réellement utilisable.

BiCMOS parviennent à délivrer de hauts niveaux de SFDR sur des centaines de Mégahertz et isoler l'entrée des interférences. Une autre caractéristique importante en réception est le rapport d'interférence sur signal ou NFR (*Near-Far Ratio*), rapport entre le plus haut niveau de puissance reçue, généralement à proximité de l'émetteur, et la puissance reçue la plus faible possible, généralement à partir de l'émetteur le plus éloigné. Par exemple, le NFR est de 90 dB en mode GSM.

B.4.2 Performances

Un CAN générique présente quatre caractéristiques principales : la résolution, le taux d'échantillonnage, la bande passante de l'entrée RF et la SFDR. A titre d'exemple, selon [kenington] un CAN satisfaisant une dynamique de 100 dB avec 12 dB de rapport signal à bruit, et utilisé dans une SDR compatible UMTS WCDMA fonctionnant dans la bande [100 MHz – 2,2 GHz], doit avoir au minimum une résolution de 20 bits, un taux d'échantillonnage de 40 Méch/s et une SFDR de 122 dB. Ces caractéristiques minimales sont bien supérieures à l'état de l'art actuel. La numérisation du signal au plus près de l'antenne, et donc l'emploi de convertisseurs analogique/numérique ayant à la fois une grande dynamique et une haute résolution, est donc un défi important à relever dans les années à venir.

Deux techniques permettent toutefois d’améliorer les performances des CAN : l'entrelacement en temps et en tension (*multistep*) et le *folding*. Le *multistep* consiste en l'intégration sur une même puce de plusieurs convertisseurs rapides travaillant en parallèle. L'entrelacement temporel est assuré par un déphasage de l'horloge d'un convertisseur à l'autre. Un CAN 1 Géch/s, par exemple, est obtenu à partir de quatre CAN 250 Méch/s. Chaque CAN est de plus alimenté par une tension de référence légèrement différente, lui donnant un poids binaire différent. La technique du *folding* met quant à elle en jeu un convertisseur "grossier", assurant le traitement des bits de poids fort, et plusieurs convertisseurs plus précis pour affiner le traitement des bits de poids faible. Les CAN les plus communément utilisés sont "à approximations successives", "flash", "pipeline" et "sigma-delta". Le tableau suivant effectue un comparatif des performances de ces différents types de CAN.

Tableau XV : Comparatif des performances des principaux types de CAN

Type de CAN	Flash	Approximations successives	Rampe(s)	Sigma-delta	Pipeline
Avantages	Très rapide. Excellente bande passante. Très bonne linéarité	Hautes résolution et précision. Très bonne bande passante. Faible consommation	Haute résolution. Faible courant d'alimentation. Excellente réjection du bruit	Haute résolution. Filtrage numérique sur puce. Excellente résolution. Très bonne linéarité	Débit élevé. Faible consommation. Correction d'erreurs et auto-calibration numériques
Inconvénients	Consommation électrique. Taille de la puce. Capacité d'entrée élevée. Cher. Erreurs de code thermométrique (*sparkle codes*). Faible résolution.	Faible taux d'échantillonnage . La tension doit rester constante durant la conversion. Très bonne résolution. Linéarité moyenne.	Lent	Faible taux d'échantillonnage	Nécessite une fréquence d'horloge élevée
Temps de conversion	Indépendant de la résolution.	Croît linéairement avec la résolution.	Double pour chaque bit de résolution supplémentaire	Compromis entre le débit de données en sortie et la résolution hors bruit	Croît linéairement avec la résolution
Surface de silicium, coût et puissance dissipée	Doublés pour chaque bit supplémentaire	Augmente linéairement avec la résolution	La surface n'augmente pas avec la résolution	Augmentent avec la résolution	Augmentent avec la résolution
Usage	Très haute vitesse sans contrainte de consommation.	Une résolution moyenne à élevée (8 à 16 bits). Faibles taux d'échantillonnage , puissance et taille	Contrôle des tensions continues. Haute résolution. Faible consommation. Bonnes performances en bruit	Haute résolution. Vitesse basse à moyenne	Haute vitesse 8 bits à 16 bits. Consomme moins que le flash

La figure suivante présente le positionnement de ces technologies en fonction de la bande passante en entrée et la résolution effective. Selon [kenington] des CAN 20 bits 5 Géch/s devraient être disponibles d'ici à 2030, permettant ainsi une numérisation directe du signal RF sans filtrage analogique.

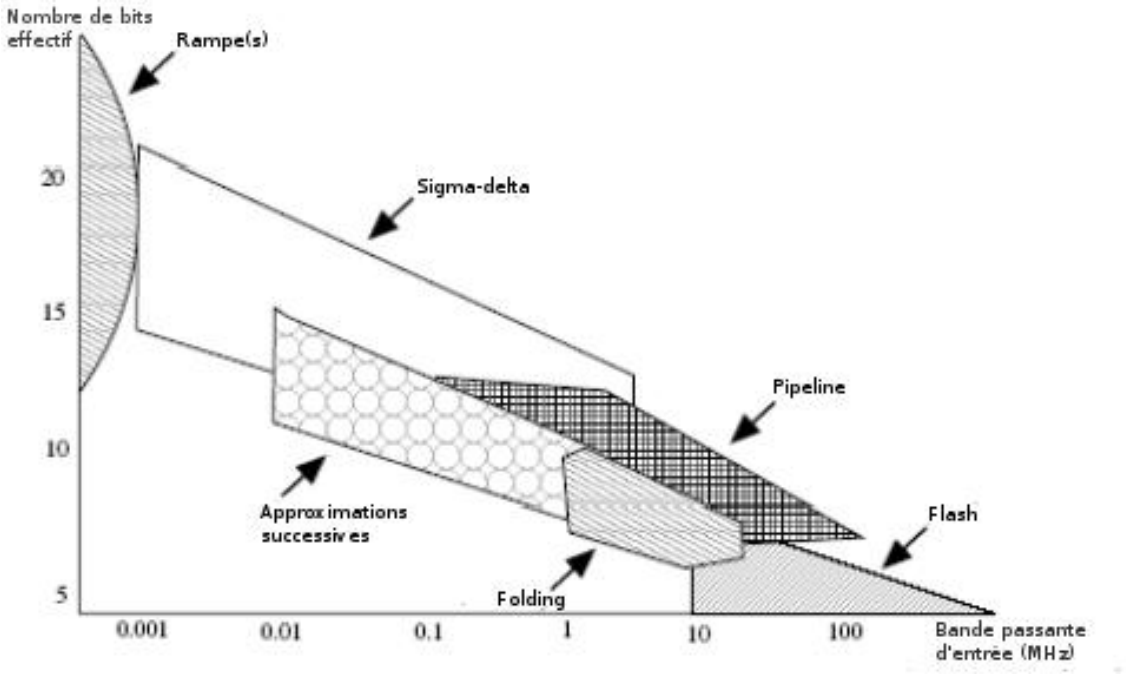

Figure 85 : État de l'art des CAN

B.5 Convertisseurs numérique/analogique (CNA)

Comme le CAN peut être considéré comme le cœur d'un récepteur SDR, de la même manière, le CNA peut être considéré comme ayant une importance équivalente dans la partie émission d'une SDR. Le rôle d'un CNA est de convertir un code binaire en une grandeur analogique. Les entrées d'un convertisseur N bits sont des niveaux logiques 'a_1', 'a_2', ... 'a_N' prenant les états logiques '0' ou '1'.

$$I = I_0[a_N 2^0 + a_{N-1} 2^1 + a_{N-2} 2^2 + ... + a_1 2^{N-1}]$$

, où I_0 est un courant de référence, et les coefficients a_1, a_2, ..., a_N valent 0 ou 1. D'une manière générale le coefficient $a_i = 0$ si le niveau logique 'a_i' = '0', et ai = 1 si 'a_i' = '1'. Les bits 'a_1' et 'a_N' sont respectivement les bits de poids fort et de poids faible.

La précision des convertisseurs réside essentiellement dans la précision des résistances utilisées. Pour caractériser un CNA on utilise généralement la notion de monotonicité (la tension de sortie est fonction croissante du code d'entrée). Si la précision d'un CNA est de ½LSB ou meilleure, la caractéristique du CNA est monotone. En pratique, il s'avère difficile de maintenir une précision de ½LSB pour des convertisseurs à nombre de bits élevés. Les principales techniques de conception des CNA sont la modulation par largeur d'impulsion, le réseau de résistances et le suréchantillonnage sigma-delta.

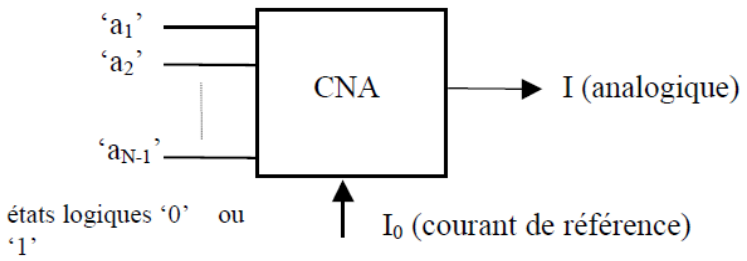

Figure 86 : Synoptique simplifié d'un convertisseur numérique/analogique N bits

Les spécifications-clés à considérer lors du choix d'un CNA sont le SNR, le taux de fuite entre canaux adjacents ou ACLR (*Adjacent Channel Leakage Ratio*) et l'intermodulation. Le SNR est principalement déterminé par le bruit de quantification et le bruit thermique. L'ALCR d'un circuit est essentiellement du à l'intermodulation du troisième ordre (IMD3), aussi doit-elle être la plus faible possible.

Dans le circuit émission d'une SDR, le CNA suit un DUC. Le mélange numérique des signaux I et Q étant injecté dans le CNA, la bande passante de ce dernier doit être élevée, et ce d'autant plus si plusieurs modulateurs I/Q alimentent un même CNA (architecture de transmission multiporteuse large bande).

B.6 Convertisseur/éleveur numérique (DUC)

Un DUC (*Digital Up-Converter*) a pour fonction de transposer en FI un signal numérique bande de base. Il est composé d'un mélangeur numérique et d'un OL qui détermine la fréquence intermédiaire. Le mélangeur génère un échantillon de sortie pour chacun de ses deux échantillons d'entrée (un en phase, un autre en quadrature). La fréquence d'échantillonnage en sortie du mélangeur doit être égale à la fréquence d'échantillonnage du CNA. L'OL fonctionne déjà à la fréquence d'échantillonnage du CNA, mais la fréquence d'échantillonnage en entrée du mélangeur numérique est généralement beaucoup plus faible. Ce problème est résolu avec un filtre à interpolation. Le filtre à interpolation augmente d'un facteur N (facteur d'interpolation) la fréquence d'échantillonnage du signal d'entrée bande de base. Une autre technique que permet cette architecture est la transmission multiporteuse, où la partie numérique est reproduite une fois par porteuse, et les sorties des DUC additionnées avant envoi au CNA. Le schéma suivant présente le principe de fonctionnement d'un DUC.

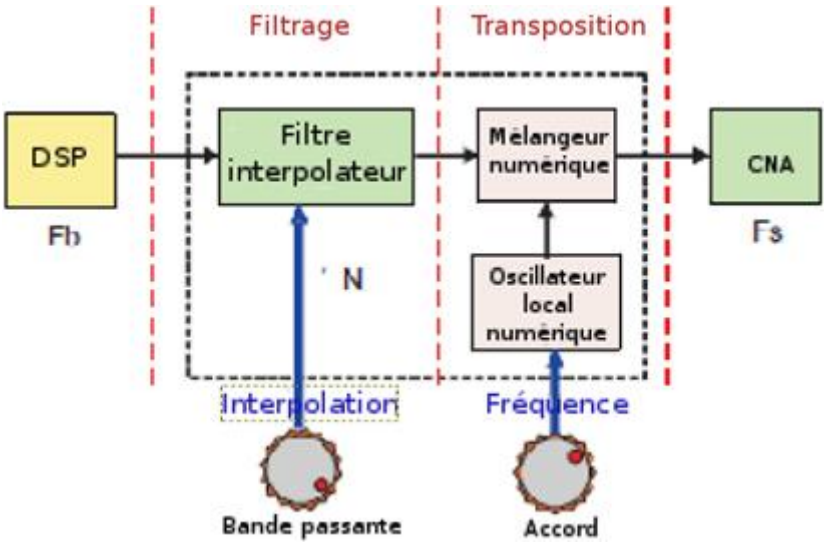

Figure 87 : Convertisseur/éleveur numérique (DUC)

B.7 Convertisseur/abaisseur numérique (DDC)

Un DDC (*Digital Down-Converter*) a pour fonction de transposer en bande de base un signal numérique FI. Le DDC comporte trois fonctions principales : un mélangeur numérique, un OL numérique et un filtre passe-bas à réponse impulsionnelle finie (FIR - *Finite Impulse Response*). Le mélangeur numérique et l'OL effectuent la transposition FI vers bande de base. Le filtre passe-bas FIR limite la bande passante du signal et agit comme un filtre décimateur. Les échantillons numériques en bande de base sont ensuite transmis à un bloc de traitement numérique du signal qui effectue des tâches telles que la démodulation, le décodage et d'autres tâches de traitement.

En sortie du mélangeur, le signal a été transposé en bande de base complexe (signaux I et Q). L'OL utilisant un accumulateur de phase numérique, la commutation entre les fréquences s'effectue en continuité de phase, ce qui est notamment pratique en modulation FSK. Étant donné que la bande passante du filtre FIR est limitée, l'application du critère de Nyquist permet d'abaisser le taux d'échantillonnage. En gardant 1 échantillon sur N, on peut diminuer le taux d'échantillonnage d'un facteur N. C'est ce que l'on appelle la décimation. L'opération de traitement du signal effectuée par le décimateur est exactement l'inverse de celle du filtre d'interpolation du DUC. Si le taux d'échantillonnage de sortie décimé est maintenu supérieur au double de la largeur de bande de sortie, aucune information n'est perdue. L'avantage est que les signaux décimés peuvent être traités plus facilement, peuvent être transmis à un débit plus faible, ou être stockés dans moins de mémoire, ce qui au final revient à une réduction du coût de réalisation. Le schéma suivant présente le principe de fonctionnement d'un DDC.

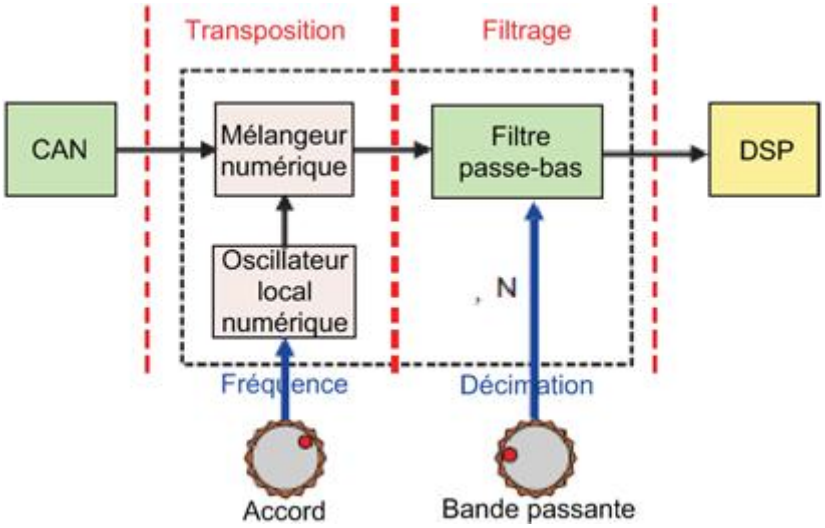

Figure 88 : Convertisseur/abaisseur numérique (DDC)

La complexité des processeurs requis dans un système est directement proportionnelle à la fréquence d'échantillonnage des données d'entrée et de sortie. Par conséquent, en réduisant la fréquence d'échantillonnage, on peut réduire considérablement le coût et la complexité des processeurs de traitement numérique des signaux du système. Non seulement l'utilisation de DDC et de DUC permet de réduire la charge de travail processeur, mais la réduction de la bande passante et du taux d'échantillonnage permettent également de gagner du temps dans le transfert de données vers un autre sous-système. Cela permet de minimiser le temps d'enregistrement et l'espace disque, et de réduire le trafic et la bande passante sur les canaux de communication.

B.8 Traitement numérique bande de base

En réception les échantillons numériques bande de base obtenus en sortie du DDC font l'objet de plusieurs traitements pour en extraire les informations désirées. De même les données à transmettre font l'objet de multiples transformations avant d'alimenter le DUC. Ces transformations sont dépendantes des normes de transmission employées mais intègrent toujours une phase de modulation en émission et de démodulation en réception. Le schéma suivant donne un aperçu des opérations réalisées sur les signaux en émission et réception, et notamment les transformations numériques pouvant être effectuées en bande de base.

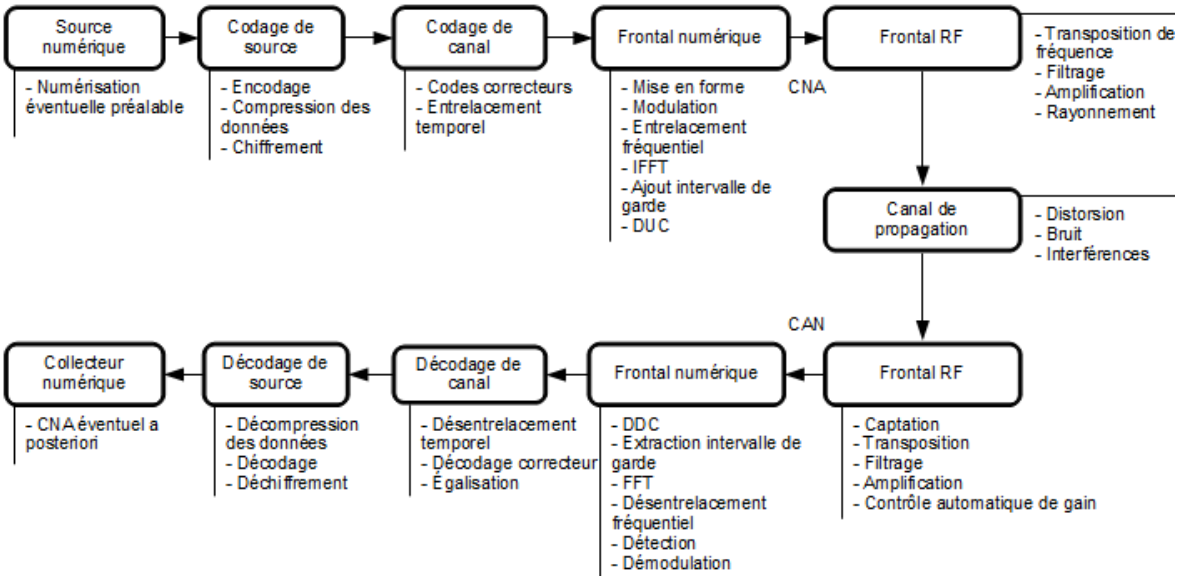

Figure 89 : Traitements du signal en radiocommunication

Parmi les diverses opérations réalisées, on peut citer :

- Le codage/décodage de source : le rôle du codage de source est de représenter le message avec le moins de bits possibles. Pour ce faire, il cherche à éliminer toute redondance contenue dans le message de la source (compression). Si la source est analogique, le codage de source joue également le rôle de numériseur ;

- Le codage/décodage de canal : l'objectif du codage de canal est de protéger le message des perturbations du canal de transmission en ajoutant en émission de la redondance au message compressé afin de détecter ou de corriger à la réception des erreurs induites par le canal de transmission (exemples de techniques : bit de parité, code de redondance cyclique ou CRC, codes convolutifs, etc.) ;

- L'entrelacement des données : lorsque des erreurs surviennent par paquets trop gros, les codes correcteurs d'erreur, de capacité limitée, ne peuvent plus remplir leur office. La technique de l'entrelacement revient à permuter les symboles codés avant leur transmission. L'entrelacement est donc utilisé pour rendre plus aléatoires les positions des erreurs et donc d'en uniformiser la répartition ;

- La modulation : la modulation effectue une conversion de bits en symboles. Elle consiste à effectuer un codage dans l'espace euclidien, espace généralement adapté aux canaux rencontrés en pratique. Pour une modulation M-aire, on associe à chaque mot de g bits un signal $x_i(t)$, i = 1, 2, . . ., M de durée T choisi parmi les $M = 2^g$ signaux ;

- La démodulation : l'objectif de la démodulation est d'extraire les informations binaires tout en maximisant le rapport signal à bruit ;

- La détection : Le rôle de la détection consiste à décider (avec prise en compte d'éventuelles pondérations) en faveur des symboles les plus probablement émis.

Une partie des traitements appliqués ensuite sur le flux de données binaires est assurée par la couche MAC (*Media Access Control*). Le rôle principal de cette couche protocolaire est de reconnaître et de former les trames binaires, détecter les erreurs de transmission, insérer les adresses MAC de source et de destination dans chaque trame transmise, filtrer les trames reçues et contrôler l'accès au média physique lorsque celui-ci est partagé.

B.9 Ressources calculatoires

La conception d'une SDR doit anticiper les ressources de calcul nécessaires à l'exécution de ses applications les plus complexes. Les principaux processeurs susceptibles d'être utilisés dans une SDR sont les ASIC et dérivés, les FPGA, les DSP, les GPP (exemple : PC traditionnel) et les GPU.

B.9.1 Les ASIC

Les circuits intégrés spécialisés, ou ASIC (*Application-Specific Integrated Circuits*) sont des circuits produits pour un seul client et selon les spécifications de ce dernier. Les ASIC ont initialement été utilisés dans les SDR du fait de leur capacité à concilier des performances en large bande, une haute intégration, une petite taille et une faible consommation d'énergie. Le principal handicap des ASIC réside dans leur manque de flexibilité (ou, inversement, le coût de l'ajout de flexibilité). Pour cette raison, l'industrie des SDR s’est reportée vers d'autres architectures plus souples, tels que les FPGA. À noter qu'il existe également des ASSP (*Application Specific Standard Product*), circuits type ASIC légèrement programmables et fabriqués en masse.

B.9.2 Aparté sur les systèmes intégrés sur puce

La complexité des systèmes allant en s'accroissant (en termes de fonctionnalités), les systèmes électroniques font de plus en plus appel aux concepts de modularité matérielle et de programmation logicielle. Au début des années 2000 est apparu le concept de systèmes sur circuits programmables, ou SOPC *(System on a Programmable Chip*), système complet contenant processeur(s), mémoires, périphériques d'interfaces, bus, convertisseurs, blocs analogiques, etc. Un SOPC intègre sur une seule pièce de silicium tous les modules nécessaires à la réalisation d'une opération donnée, pouvant être réutilisés

dans plusieurs conceptions différentes, et garantissant une configuration aisée ainsi qu'une grande puissance de calcul.

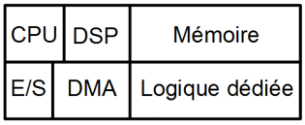

Figure 90 : Exemple de constitution d'un SOPC

Dans un SOPC, le processeur (CPU), de type *softcore*, peut exécuter diverses tâches via l'intégration d'un système d'exploitation. Un *softcore* est une implémentation de CPU disponible sous forme de blocs de propriété intellectuel ou IP[54] (*Intellectual Property*) réalisés à l'aide d'un langage de description de haut niveau type VHDL. Le VHDL (*Very high-speed integrated circuit Hardware Design Language*) est un standard IEEE (référence 1076-1993) dédié à la modélisation, la simulation et la synthèse de systèmes matériels logiques. C'est un langage de description de matériel ayant pour objectif de détailler l'architecture et le comportement de systèmes électroniques numériques. Le principe de conception en VHDL est indiqué dans la figure suivante.

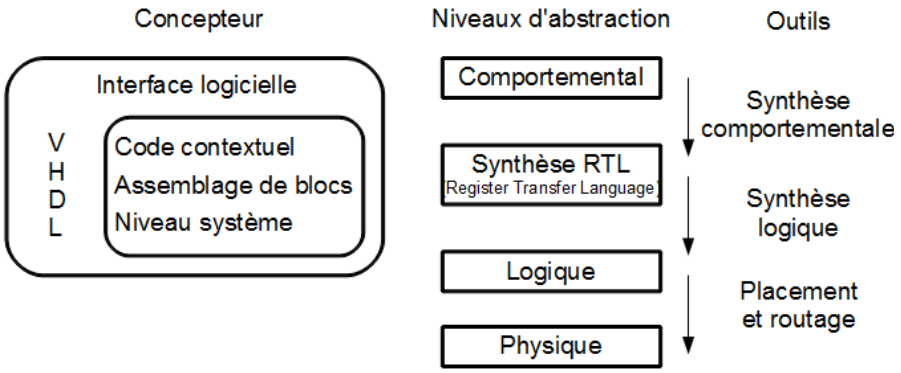

Figure 91 : Principe de développement VHDL

Le langage VHDL-AMS (VHDL *for Analog and Mixed Signal*, [wiki2]) est aussi un standard IEEE (1076.1-1999). C'est une extension du VHDL, qui en reprend la structure (typage fort des données, bibliothèques, objets, description concurrentielle/séquentielle), et qui permet de décrire des modèles à différents niveaux (système, macro modèle, transistor) afin de définir le comportement de systèmes analogiques et mixtes logiques/analogiques. Citons également l'existence d'IP-AMS (IP *Analogue and Mixed Signals*), IP pour circuits analogiques et mixtes.

[54] Les IP sont des fonctions complexes " boîte noire ", disponibles sous forme de bibliothèque et respectant le principe de propriété industrielle.

Souvent utilisé dans un FPGA, le *softcore* peut être reconfiguré pour s'adapter à différents cas d'utilisation (performances, consommation, fonctions, etc.). La contrepartie est qu'un processeur de type *softcore* est plus lent qu'un processeur matériel, mais est toutefois plus facile à maintenir. Citons pour exemple les processeurs *softcore* Nios II pour Altera [nios] et MicroBlaze pour Xilinx [µblaze].

B.9.3 Les FPGA

Les réseaux de portes programmables *in situ* ou FPGA (*Field-Programmable Gate Array*) sont des circuits intégrés VLSI (*Very-Large-Scale Integration*) composés d'un nombre élevé de blocs logiques configurables ou CLB (*Configurable Logic Block*). Un CLB est constitué au minimum d'une table de correspondance (LUT – *Look-Up Table*) et d'une bascule. Une LUT sert à implémenter des équations logiques (de généralement 4 à 6 entrées et une sortie), une petite mémoire, un multiplexeur ou un registre à décalage. Les CLB comportent principalement des réseaux de portes logiques, des registres, des unités de multiplication/accumulation et des fonctions d'horloge. Les CLB sont interconnectés par un système matriciel configurable de liaisons haute vitesse, et sont reliés à des blocs d'E/S programmables ou (IOB – *Input Output Blocks*). Les blocs d'entrées/sortie d'un FPGA se situent en périphérie de la matrice logique et permettent de relier la structure à des signaux externes. Les blocs de mémoire peuvent être des petites mémoires rapides double accès (pour les tampons et les tables de coefficient), ou de grandes mémoires simple accès (pour le stockage de grandes tables de données). Si la mémoire interne est insuffisante, plusieurs blocs d'entrée/sortie sont capables de piloter des mémoires externes rapides. Les blocs de traitement numérique du signal contiennent des multiplicateurs et parfois des accumulateurs fonctionnant à des vitesses élevées. Enfin, il y a souvent quelques blocs contenant des circuits spécialisés tels qu'une PLL, une gestion d'horloge ou un circuit d'aide à la programmation. L'ensemble dispose ainsi d'un haut niveau de flexibilité d'emploi. Les FPGA permettent d'effectuer des traitements logiques personnalisés et offrent généralement un grand nombre d'unités de traitement et de mémoires tampon (*buffers*), ce qui réduit la fréquence de fonctionnement et donc la consommation d'énergie nécessaire à une application donnée par rapport à celle requise pour un DSP. Ces composants logiques programmables *in situ* ont créé un nouveau paradigme de programmation : la programmation câblée configurable. La figure suivante présente un exemple d'architecture de FPGA.

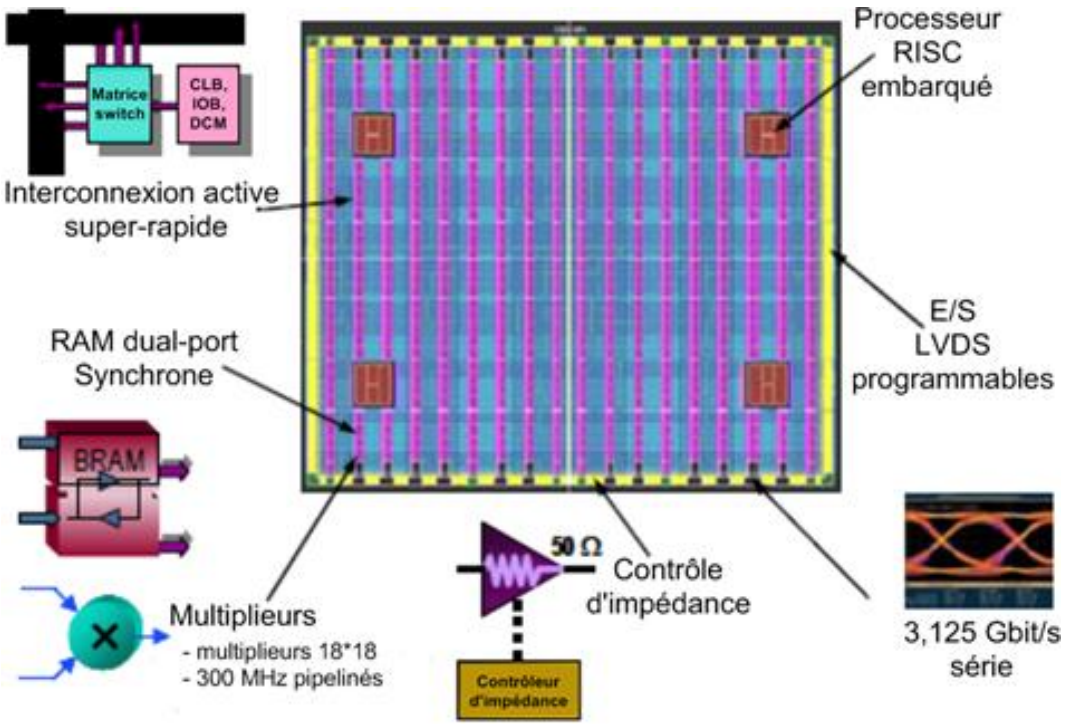

Figure 92 : Exemple d'architecture de FPGA : le Virtex-II Pro

La complexité de programmation d'un FPGA requiert une expertise technique avancée afin d'exploiter la puissance de traitement disponible. En changeant la configuration d'un FPGA, il est possible d'en changer complètement ses fonctionnalités. Toutefois, ce processus de modification nécessite son redémarrage ce qui impose des délais trop longs dans le cas de certaines applications temps réel. En outre, les circuits auxquels le FPGA se connecte peuvent ne pas fonctionner correctement suite à une configuration " à chaud ". Du fait de leur relative complexité, la procédure de débogage des FPGA est assez coûteuse en temps.

En raison du grand nombre de multiplicateurs et de mémoires au sein d'un FPGA, les opérations de convolution, corrélation et filtrage font l'objet d'une implémentation efficiente et présentent des performances déterministes. Les FPGA sont particulièrement performants pour des opérations de traitement vectoriel impliquant de nombreuses opérations mathématiques effectuées en parallèle. Ils sont néanmoins moins efficaces que les DSP et les GPP pour les parties d'algorithme nécessitant une prise de décision et pour des chemins d'exécution non déterministes. Citons quelques exemples de fonctions pouvant être implémentées dans un FPGA : générateur de signaux déterminés par des tables, oscillateur contrôlé numériquement, DDC et DUC.

L'aspect le plus séduisant des FPGA est leur puissance de calcul. Par exemple, la famille des FPGA Virtex-7 de Xilinx [xilinx], composants de dernière génération, contient entre environ 45 000 et 300 000 CLB, pour un total d'environ 300 000 à 2 millions d'éléments logiques. Par exemple, pour implémenter la norme 802.11a, seuls 3000 CLB sont nécessaires. Un autre exemple de FPGA haute performance est l'Altera Stratix V, commercialisé au premier trimestre 2011. Il possède notamment plus d'un million d'éléments logiques en version VE, jusqu'à 50 Mbits de mémoire embarquée et plus de 3500 multiplieurs 18*18 [stratix5]. De tels composants coûtent néanmoins assez cher (plusieurs milliers d'euros). Un exemple de FPGA bon marché (moins de 50 $) est l'Altera Cyclone III EP3C25 [cyclone3a] [cyclone3b]. Il possède environ 25 000 éléments logiques et 600 kbits de mémoire embarquée, 4 PLL, 66 multiplieurs 18*18 à 260 MHz, et embarque un *softcore* Nios II. Il supporte de multiples standards d'entrée-sortie dont notamment PCI Express, et peut s'interfacer à des mémoires externes de type QDR SRAM (*Quad Data Rate Static RAM*) ou DDR SDRAM (*Double Data Rate Synchronous Dynamic RAM*).

Les FPGA ont connu une véritable révolution ces dernières années, tant au niveau de la performance que du coût. Ils approchent désormais le niveau de performance des ASIC, la flexibilité en plus. Il est également possible d'ajouter des *softcores* dans un FPGA, ce qui permet de réaliser des solutions à puce unique (SOPC) dans certaines applications où les critères de taille réduite et de fiabilité sont importants. Les performances des FPGA sont en amélioration permanente compte tenu d'une compétition effrénée des fondeurs, notamment Xilinx et Altera. Il faut toutefois garder à l'esprit que pour réussir une application à base de FPGA, il faut non seulement bien connaître les caractéristiques du (ou des) FPGA employés mais aussi les moyens à mettre en œuvre pour pouvoir les exploiter. Pour programmer un FPGA, le développeur décrit la configuration des blocs logiques et leurs interconnexions. Le principe de développement se rapproche plus de la conception de circuits que de la programmation. Rappelons en effet que la programmation d'un FPGA ne se fait pas à l'aide d'un langage traditionnel tel que C, mais en VHDL. Toutefois des variantes de C permettant de programmer un FPGA existent, tels que SystemC, l'avantage reste cependant faible car le programme résultant demeure une description de circuits logiques. La conception d'un système basé sur l'utilisation de FPGA associe saisies de schémas et spécifications de haut niveau (structurelle et/ou fonctionnelle)

en langage VHDL ou Verilog, et langage C. Le schéma de synthèse suivant correspond au cycle de programmation d'un FPGA.

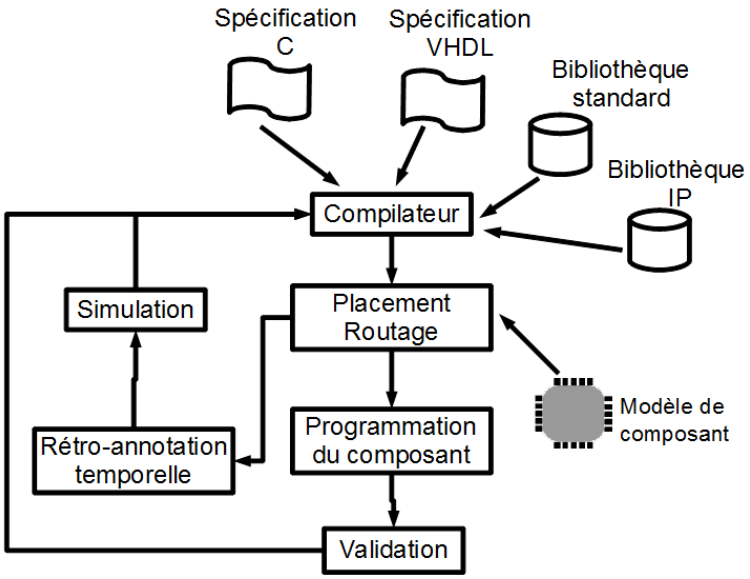

Figure 93 : Cycle de programmation d'un FPGA

La "configurabilité" d'un FPGA est un aspect important à garder à l'esprit lors de son utilisation. Elle consiste à pouvoir reconfigurer à la volée une partie du design, à partir d'un fichier binaire, soit pour adapter le FPGA à de nouvelles conditions d'utilisation, soit pour gérer l'évolution d'une application. La majorité des FPGA ne peut être reconfigurée que dans son intégralité, c'est à dire que pour changer de configuration, un FPGA doit cesser ses activités, entrer dans un état de reconfiguration, se reconfigurer, puis être remis en état opérationnel. Les dispositifs auxquels un FPGA se connecte doivent être capables de gérer ces processus sans entrer dans un état indésirable. La série des FPGA Virtex de Xilinx supporte un mode de configuration partielle permettant une configuration séparée des colonnes de la matrice logique, sans nécessiter l'arrêt du composant. [xilinx]

Les FPGA ont su s'imposer comme une alternative entre les solutions dédiées très performantes (ASIC) et les solutions programmables très flexibles (microprocesseurs et DSP). Ils offrent désormais des performances et des capacités permettant l'implémentation de nombreuses applications courantes. Pour configurer ces "couteaux suisses", de nouveaux outils de conception font leur apparition. Le choix d'un FPGA dépend souvent fortement de la qualité des outils de conception disponibles pour ce composant. Au cours de ces dernières années, une nouvelle industrie de fournisseurs d'IP s'est développée pour offrir des milliers d'algorithmes spécifiques aux applications implémentées sur FPGA.

B.9.4 Les DSP

Les processeurs de traitement numérique du signal ou DSP (*Digital Signal Processor*) sont des processeurs spécialisés en traitement numérique du signal, aussi constituent-ils un choix plausible lors de la conception d'une SDR. Les DSP exécutent efficacement des opérations de traitement vectoriels telles que les multiplications/accumulations (MAC[55]), avec des vitesses de traitement pouvant atteindre plus de 30 milliards de MAC par seconde (TMS320C647x *Multicore* DSP de Texas Instrument [ti]). On distingue les processeurs DSP selon le format de représentation (virgule fixe ou flottante) et la taille des données manipulées (généralement multiple de 16 bits) ainsi que la capacité d'adressage mémoire. À l'origine, les DSP étaient conçus pour exécuter, au sein d'un unique cœur, des MAC aussi vite que possible. Les DSP modernes peuvent utiliser plusieurs noyaux algorithmiques, voire même plusieurs *softcores*. L'état de l'art actuel des DSP met l'accent sur la maximisation de la bande passante entre les unités de traitement et la mémoire, prend généralement en charge plusieurs bus de données et consomme moins d'énergie que la plupart des GPP. Les DSP peuvent être programmés avec un langage de haut niveau, tel que C ou C++, et peuvent même embarquer un système d'exploitation. Les DSP sont les circuits les mieux adaptés aux traitements simples de signaux numériques. De par leur production en masse (les DSP occupent de nombreux secteurs de l'électronique), ils permettent également de faire des économies d'échelle. Un DSP typiquement utilisable dans une SDR est le Blackfin ADSP-BF561 d'Analog Devices [blackfin]. Il s'agit d'un DSP double cœur de fréquence d'horloge maximale 600 MHz pouvant effectuer jusqu'à 2,4 Giga-MAC (milliards de multiplication/accumulation) par seconde, et bon marché (30$).

Du fait de son architecture de conception spécifique, le DSP était jusqu'au début des années 2000 le composant le mieux adapté au traitement du signal. Les FPGA récents sont capables de soutenir la comparaison avec les DSP en termes de performances et de fournir en plus l'ensemble des signaux d'horloge utiles à la réalisation de formes d'onde complexes. De plus, bien que le cahier des charges d'un DSP peut sembler suffisant pour prendre en charge une application donnée, il faut prendre soin d'estimer tous les besoins en traitement des données pour éviter que le DSP ne soit pas sous calibré aux vues de l'application souhaitée. En effet, contrairement aux FPGA, les ressources arithmétiques d'un DSP sont partagées par tous les traitements effectués sur la puce. Pour une application

[55] Une multiplication-accumulation (MAC) correspond à l'opération suivante : A = A + B*C.

nécessitant une faible bande passante, un ou plusieurs DSP peuvent être suffisants pour gérer les traitements d'une SDR, sans avoir besoin d'un FPGA. Pour des applications nécessitant plus de bande passante, un FPGA peut être utilisé comme frontal large bande d'un DSP. Ledit FPGA assure alors la conversion entre le haut débit des CAN/CNA et un débit plus faible, permettant ainsi au DSP de réaliser l'intégralité des traitements. Par exemple, dans un système à sauts de fréquence, l'étage CAN/CNA serait exploité sur une bande passante suffisamment élevée pour couvrir tous les canaux, le DSP exploiterait un canal, et le FPGA mettrait en œuvre des algorithmes de saut de fréquence à l'aide d'oscillateurs à commande numérique et de filtres numériques.

B.9.5 Les processeurs à usage général (GPP)

Les processeurs à usage général ou GPP (*General Purpose Processor*) sont ceux venant les premiers à l'esprit pour quiconque écrit un programme informatique. Les GPP disposent tous d'un jeu d'instructions générique (CISC ou RISC), un séquenceur d'instruction, et une unité de gestion de la mémoire ou MMU (*Memory Management Unit*). Ces instructions effectuent des opérations telles que la multiplication, l'addition ou le stockage, mais ne sont toutefois pas optimisées pour un usage particulier. Or dans le contexte de la radio logicielle, l'application qui nous intéresse le plus est le traitement du signal. Les GPP sont généralement couplés avec un système d'exploitation ayant pour tâche de créer un niveau d'abstraction permettant le développement d'applications avec peu ou aucune connaissance sur le matériel sous-jacent.

En règle générale les processeurs à usage généraux peuvent être utilisés dans les radios logicielles. Cependant, ils manquent généralement de puissance de calcul pour gérer le flux du signal radio lui-même. Ils sont habituellement utilisés dans les opérations finales du récepteur (ou initiales de l'émetteur), lorsque le signal est un message binaire bas débit. Toutefois, les GPP de dernière génération peuvent faire mieux que ça. Par le passé, les GPP n'avaient pas la capacité de traiter de grandes quantités de données issues de signaux radio. Les nouveaux processeurs disposent désormais d'unités de traitement vectoriel haute vitesse pouvant s'avérer utiles dans les applications de SDR. Les GPP récents peuvent effectuer plus d'un milliard d'opérations mathématiques par seconde grâce à des techniques de *super pipeline*. Par exemple un microprocesseur Intel Core i7 est multicœur, *multi-thread*, et a une importante quantité de mémoire et d'unités de traitement vectoriel. Ces caractéristiques sont suffisantes pour une SDR gérant une bande étroite. Les principaux inconvénients des GPP sont une consommation d'énergie élevée, un plus grand

encombrement par rapport à une solution à base de DSP/FPGA, et des options d'entrées-sorties limitées. Il existe toutefois certaines applications, telles que les systèmes de développement et de tests, où ces limitations ne sont pas importantes. La méthode la plus courante pour s'interfacer avec un GPP est d'utiliser des bus périphériques haute vitesse tels que PCI Express (PCIe). Plusieurs FPGA modernes prennent en charge des interfaces PCIe. Combiné avec des dispositifs compatibles PCIe, comme par exemple le FPGA Altera Stratix IIG, un GPP peut être une bonne solution pour exécuter une partie du traitement du signal dans une SDR.

B.9.6 Une aide au GPP : l'accélération matérielle

L'accélération matérielle consiste à confier à un circuit intégré dédié une fonction spécifique anciennement dévolue au processeur central d'un ordinateur (CPU). Ces circuits intégrés accélérateurs, implémentés soit sur la carte mère, soit sur une carte fille, voire même au sein d'un CPU, sont généralement utilisés via des pilotes spécifiques (OpenGL, Direct3D, Glide...).

Il existe différents types d'accélérateurs matériels, pour différents usages telles les cartes d'accélération audio, plus communément appelées cartes son, capables d'effectuer des tâches de numérisation et de traitement du signal audio. Mais les accélérateurs matériels qui retiennent le plus l'attention pour le traitement numérique des données issues d'une radio logicielle sont les cartes d'accélération vidéo, embarquant un ou plusieurs processeurs graphiques, ou GPU (*Graphics Processing Unit*). Un GPU est un microprocesseur à structure hautement parallèle, spécialisé dans le traitement des données d'affichage (traitement du signal vidéo, rendu 3D, gestion de la mémoire vidéo, décompression MPEG, etc.). Il en existe deux types : les processeurs graphiques intégrés sur la carte mère, partageant sa mémoire vive, voire disposant également d'un peu de mémoire dédiée ; et les cartes graphiques dédiées, plus puissantes, disposant de leur propre mémoire vive, et interfacées avec à la carte mère d'un ordinateur via un port PCIe.

Les cartes graphiques embarquent des processeurs de plus en plus puissants. Avec leurs multiples unités de traitement, ces circuits sont parfaitement adaptés aux traitements parallèles. Depuis quelques années les GPU ont trouvé une nouvelle vocation : ils sont en mesure de réaliser des calculs pour des applications non graphiques, et se montrent notamment particulièrement efficaces dans les calculs de transformée de Fourier rapide (FFT – *Fast Fourier Transform*). Jusqu'à présent cette technique était difficile à mettre en œuvre car elle impliquait l'utilisation des API graphiques OpenGL ou Direct3D optimisées

pour le graphisme. Le calcul générique sur processeur graphique (ou en anglais GPGPU, pour *General-Purpose computing on Graphics Processing Units*) permet désormais de réaliser n'importe quel calcul à condition de s'adapter à l'architecture dite " à flots de données " propre au GPU. Il existe plusieurs *frameworks* de type GPGPU :

- OpenCL (*Open Computing Language*) : « libre », multiplateforme et notamment compatible ATI et NVIDIA, langage de programmation dérivé du C ; [khronos1] [khronos2]

- ATI *Stream* SDK : kit de développement utilisant OpenCL, compatible cartes ATI/AMD ; [amd]

- CUDA (*Compute Unified Device Architecture*) : propriétaire, compatible NVIDIA, langage de programmation dérivé du C. [cuda]

Ces *frameworks*, de présentation modulaire (modules de gestion des commandes, des calculs, de la mémoire, etc.) permettent de communiquer directement avec un GPU. La démarche d'emploi d'un GPU dans une SDR est d'autant plus intéressante qu'à prix égal, un GPU est plus puissant qu'un CPU. En effet, un GPU dernière génération atteint le Téraflops (mille milliards d'opérations en virgule flottante par seconde), contre quelques dizaines de Gigaflops (ou Gflops) pour un processeur classique. A titre de comparaison un processeur Intel Core I7-620M offre une puissance de calcul de 21 Gflops tandis qu'une carte Nvidia GeForce GT330M propose 180 Gflops. Afin de faire taire les rumeurs indiquant qu'un GPU serait 100 fois plus rapide qu'un CPU, Intel Corporation a toutefois fait procéder à une série de tests consistant à lancer les mêmes calculs sur une carte graphique Nvidia GeForce GTX 280 et sur un processeur Intel Core i7-960. Le GPU s'est avéré tout de même en moyenne 2,5 fois plus rapide que le CPU, malgré une optimisation logicielle de ce dernier. [lee]

De récents essais de réalisation de SDR à base de GPU en lieu et place de DSP et/ou de FPGA sont particulièrement prometteurs. Dans l'article [gpu] une équipe d'universitaires est parvenue à réaliser un terminal SDR pour le WiMAX à l'aide d'un émetteur-récepteur RF et d'un ordinateur équipé à la fois d'un PC et d'un GPU pour réaliser le traitement des signaux numériques en bande de base. Le code d'exécution du CPU et du GPU a été réalisé en langage de type C à l'aide du kit de développement CUDA SDK *(Software Development Kit*). En comparant les performances d’une carte graphique Nvidia GeForce 9800GTX et d’un DSP Texas Instruments TMS320C6416, la carte graphique s'est révélée 90 fois plus rapide que le DSP lors du décodage d'un code convolutif avec

l'algorithme de Viterbi. Une autre étude a comparé les performances d'un CPU Intel Dual-Core Xeon optimisé avec la bibliothèque FFTW, et d'un GPU Nvidia 8800GTX. La carte graphique s'est révélée entre 2,5 et 10 fois plus rapide que le CPU selon les traitements réalisés [harrison]. Une dernière étude a comparé les performances d'un CPU Intel E6600 et un GPU Nvidia 8800GTX dans le cadre d'une simulation MIMO 2*2. Le GPU s'est révélé de 8 à 9 fois plus rapide que le CPU [akapyev]. Compte tenu de la puissance de calcul des GPU et notamment de leur aptitude aux calculs parallèles, il ne serait pas étonnant de voir leur emploi se démocratiser au sein des radios logicielles, en support des GPP.

B.9.7 Quels processeurs de traitement numérique choisir pour une SDR ?

Il y a plusieurs paramètres à considérer pour évaluer le rendement potentiel d'un dispositif de traitement numérique. Les MIPS (millions d'instructions par seconde), MOPS (millions d'opérations par seconde), MMACS (millions de multiplication - accumulation par seconde) et MFLOPS (millions d'opérations en virgule flottante par seconde) sont toutes des mesures de la vitesse de traitement des instructions dans un matériel. Leur pertinence vis-à-vis de la performance d’un équipement dépend notamment des algorithmes de traitement utilisés. Les besoins en fréquence de fonctionnement d'un FPGA peuvent par exemple être réduits en utilisant plus de multiplicateurs et de RAM. En effet en réalisant des copies multiples d'un même circuit, chaque copie est en mesure de gérer une partie des données manipulées. Un autre facteur important est l'interconnexion entre les unités de traitement numérique. Ces unités peuvent être connectées directement à l’aide d’un matériel dédié, ou au travers d’un bus partagé, et peuvent partager une ressource telle que la mémoire. Le choix d'interconnexion est habituellement dicté par le choix du matériel. Par exemple, dans un FPGA, il est courant et encouragé d’interconnecter les unités de traitement directement entre elles pour éviter les goulets d'étranglement.

La radio logicielle se veut flexible et requiert une importante puissance de calcul. La conséquence est qu'elle combine le plus souvent les différents composants de traitement du signal cités précédemment (DSP, FPGA, GPP, etc.) afin de bénéficier des performances et de la flexibilité spécifiques de chaque élément. Les SDR récentes mixent les trois principaux types de matériel que sont les GPP, DSP et FPGA pour proposer une grande palette d'applications, et implémentent rarement des ASIC car ils ne sont pas reconfigurables. Mais étant donné qu'ils sont optimisés pour une application puis produits en masse, les ASIC présentent néanmoins un rapport (puissance de

`calcul) / (coût*consommation énergétique)` imbattable. Les FPGA sont quant à eux destinés aux applications nécessitant puissance de calcul et souplesse d'emploi. La force des DSP et des GPP réside dans leur grande souplesse d'emploi, leur simplicité de configuration et de réutilisation logicielle. L'emploi de GPU (en renfort de GPP) dans les SDR est encore embryonnaire mais s'avère prometteur. Le tableau suivant synthétise de façon empirique les avantages et inconvénients des différents types de processeurs étudiés.

Tableau XVI : Comparatif des différentes catégories de processeur de traitement du signal[56]

	ASIC	ASSP	DSP	FPGA	GPP	GPP+GPU
Consommation	++	++	O	+	O	-
Coût (petites séries)	--	--	O	-	O	O
Coût (grandes séries)	++	++	O	-	O	O
Puissance de calcul	++	++	O	+	O	+
Réutilisation logicielle	O	O	+	O	++	+
Souplesse	--	-	++	+	++	++

Les caractéristiques techniques d'une SDR sont liées à l'usage qu'il en est fait (téléphonie vocale, transmission de données en réseau, messagerie texte, affichage graphique, vidéo en direct, navigation Web, etc.). La partie numérique peut par exemple mettre en œuvre un codage source. Dans chaque cas, l'objectif est d'utiliser certaines propriétés intrinsèques ou statistiques du type d'information transmise pour réduire le dédit des données à un niveau acceptable pour la transmission. Le codage de la voix, de la vidéo et des données utilise les caractéristiques en redondance du signal source pour comprimer le débit binaire. Des facteurs de compression généralement supérieurs à 10:1 sont obtenus pour le codage de la voix, et jusqu'à 100:1 en codage vidéo. Pour le codage des données, le taux de compression dépend pour beaucoup de la redondance propre des messages et de leur fréquence d'envoi dans le système radio.

Les applications de codage vocal sont généralement implémentées sur un DSP pour lequel les algorithmes de codage nécessitent entre 20 MIPS et 60 MIPS et environ 32 kilo-octets de RAM. C'est également possible sur un GPP, mais au prix d'une capacité de calcul de 100 à 600 MIPS (peu contraignant au regard des performances actuelles des GPP). La transmission de vidéo est presque 100 fois plus exigeante que celle de la voix, et donc moins souvent implémentée sur des GPP ou DSP. L'encodage vidéo est généralement mis

[56] - - : très mauvais ; - : mauvais ; O : neutre ; + : bon ; ++ : très bon

en œuvre sur des processeurs spécialisés implémentant des FPGA, en raison des opérations de corrélation croisée nécessaires au calcul des vecteurs de mouvement des objets sur une image vidéo[57]. Le texte et la navigation sur le Web s'exécutent généralement sur un CPU. Un navigateur Web typique a besoin de stocker les images associées à chaque page Web, afin de rendre le processus de navigation plus efficace, en éliminant la transmission redondante de pages récemment vues. Cela implique des fonctions de cache de données mises en œuvre sur des disques durs ou des mémoires flash type SSD (*Solid-State Drive*).

Afin de se fixer les idées, pour pouvoir s'adapter à une large gamme de formes d'ondes à démoduler et d'applications, une SDR basique doit présenter les performances minimales suivantes : un GPP à 266 MIPS (millions d'instructions par seconde), 32 Mo de mémoire vive (RAM), un DSP à 100 MIPS, et un FPGA équivalent à 500 000 portes logiques configurables. Plus de performances et de ressources sont requises pour des formes d'onde ou des applications complexes. La figure suivante présente à titre indicatif un exemple de cycle de conception de tête de réception mixte de SDR (CAN + tête de réception numérique, exemple sans DSP).

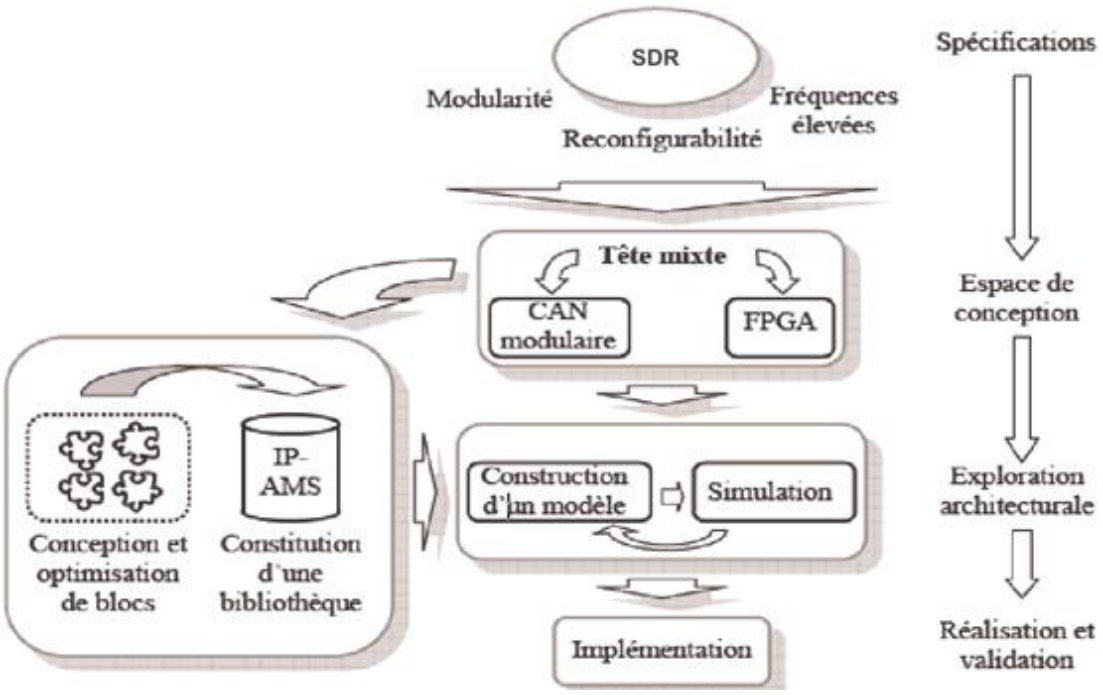

Figure 94: Cycle de conception d'une tête de réception numérique d'une radio logicielle restreinte [barrandon]

[57] Les vecteurs de mouvements ont pour fonction de réduire considérablement le nombre de bits requis pour encoder fidèlement des images.

B.10 Autres caractéristiques importantes d'une SDR

B.10.1 Agilité en fréquence

Au regard de l'agilité en fréquence, on distingue deux types de SDR : celles à modulation flexible dans une bande de fréquences fixe, et celles complètement flexibles (modulation, fréquence). La deuxième option est naturellement à privilégier car elle permet un usage souple du spectre de fréquences et une adaptabilité aux différents réseaux sans fil. En contrepartie, des contraintes sévères pèsent sur le design des éléments passifs de la tête analogique (antenne, réseaux d'adaptation, filtres). En effet un équipement radio multibande produisait jusqu'à présent un jeu fini de signaux à bande étroite, ce qui permettait l'emploi de filtres adaptés aux bandes de fréquences correspondantes et réduisait ainsi le risque d'interférences avec d'autres signaux ou du bruit ; de même pour les antennes, les réseaux d'adaptation, les LNA et les amplificateurs de puissance, optimisés pour obtenir un gain maximum dans une bande de fréquences donnée. Étant donné qu'il n'existe pas à l'heure actuelle de filtres sélectifs agiles et programmables, l'agilité en fréquence d'un équipement radio se fait au détriment des performances, en particulier de la sélectivité, de l'insensibilité aux interférences et de l'efficacité énergétique.

B.10.2 Étalonnage

Les imperfections du frontal radio peuvent être prises en compte dans les étapes numériques à l'aide d'un étalonnage. Cela débute par une caractérisation du système en utilisant des signaux de test connus, et en appliquant ensuite une compensation des erreurs trouvées. Un des avantages des SDR est que les compensations peuvent être stockées bande par bande ou voie par voie, et changées en fonction du besoin.

Annexe C
Étude pratique de la norme DECT

C.1 Remarques sur les spécifications ETSI du DECT

Les spécifications de base du DECT, ou interface commune (CI - *Common Interface*) se composent de 8 parties principales (parties 1 à 8). Le document EN 300 175-1 est une introduction générale contenant notamment les définitions et liste des abréviations utilisées dans la norme. Les documents EN 300 175-2 à EN 300 175-5 spécifient l'interface air à l'aide d'un découpage inspiré des couches 1 (physique) à 3 (réseau) du modèle OSI. Le document EN 300 175-6 décrit les identités et la structure d'adressage, et l'EN 300 175-7 détaille les caractéristiques de sécurité. L'EN 300 175-8 précise la transmission et le codage de la parole. En outre, il existe une spécification de tests de certification, l'EN 300 176.

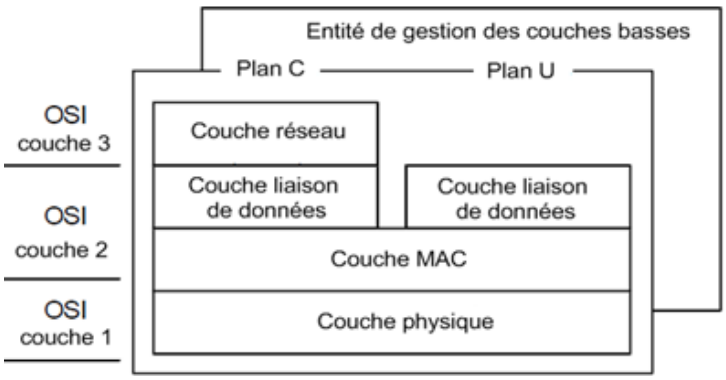

Figure 95 : Structure en couches du DECT[58]

La pile des protocoles de couche basse du DECT est associée à deux interfaces vers les couches de plus haut niveau : une avec l'entité de contrôle de l'application (C-*plane*), l'autre pour le transport des données (U-*plane*).

C.2 Couche physique

La couche physique divise le spectre radio en canaux physiques. Elle a pour principaux rôles de moduler/démoduler les porteuses radio, assurer la synchronisation entre émetteurs et récepteurs, émettre et recevoir un certain nombre de bits dans un certain intervalle de temps et selon une fréquence particulière, et observer l'environnement radio [dect2]. Les canaux physiques DECT sont des voies de communication simplex radio entre

[58] Adapté de [dect1].

deux équipements de terminaison (un RFP ou un PP). Pour établir une connexion téléphonique duplex, deux canaux physiques doivent être établis entre les équipements d'extrémité. L'attribution de un ou plusieurs canaux physiques à une communication relève de la responsabilité des couches supérieures.

La division du spectre en canaux physiques est réalisée en temps et en fréquence (TDMA sur plusieurs porteuses). Sur chaque porteuse la structure TDMA définit 24 *full slots* dans une trame de 10 ms. Chaque *slot* peut être utilisé pour transmettre des paquets de données. Certaines applications DECT utilisent plus d'un *slot* dans chaque direction. Chaque équipement a accès à tous les canaux. Quand une connexion est nécessaire, un canal est sélectionné de façon à créer le moins d'interférence possible avec les canaux déjà utilisés localement. Cela évite toute planification fréquentielle et simplifie les architectures. De plus une utilisation cellulaire du DECT permet de réutiliser les mêmes canaux physiques dans différentes localisations géographiques. Un mécanisme de *handover* permet de relâcher un canal physique et établir un autre sans relâcher la connexion établie.

Dix porteuses sont définies dans la bande de fréquences [1880-1900 MHz]. Leur fréquence centrale vérifie la formule :

`Fc = F0 - (c * 1,728 MHz), où F0 = 1897,344 MHz et c = 0,1, …, 9.`

Le tableau suivant identifie la fréquence centrale associée à chaque numéro de porteuse :

Tableau XVII : Porteuses DECT

Numéro de porteuse	0	1	2	3	4	5	6	7	8	9
Fréquence centrale (MHz)	1897,344	1895,616	1893,888	1892,160	1890,432	1888,704	1886,976	1885,248	1883,520	1881,792

La bande de fréquences entre `Fc - (1,728/2) MHz et Fc + (1,728/2) MHz` correspond au canal RF numéro `c`. On en déduit qu'un canal a pour largeur 1,728 MHz. Dans la pratique la fréquence centrale d'une porteuse d'une RFP ne doit pas s'écarter de plus de 50 kHz de sa valeur théorique. Pour un PP cet écart maximum est le même en fonctionnement *idle* et vaut 100 kHz en fonctionnement actif (les modes de fonctionnement des FP et PP sont décrits aux paragraphes C.3.1 et C.3.2).

La structure TDMA utilisée répète des trames de 11520 bits à un débit de 1152 kbit/s. Dans une trame DECT 24 *full slots* sont créés. Un *full slot* dure environ 0,417 ms. Généralement les *full slots* numérotés de 0 à 11 sont utilisés pour le sens RFP vers PP, et ceux numérotés de 12 à 23 sont utilisés pour le sens PP vers RFP. Les *double slots* sont numérotés de 0 à 10 et de 12 à 22. Les *half slots* sont numérotés 0 ou 1 selon leur position dans le *full slot*.

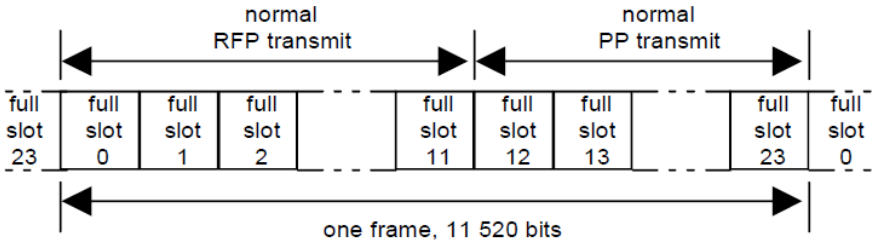

Figure 96 : Principe du TDMA DECT avec *full slots* [dect2]

Un *full slot* contient 480 intervalles symbole (un bit en modulation binaire, deux bits en 4-aire, etc.), un *half slot* en contient 240 et un *double slot* 960.

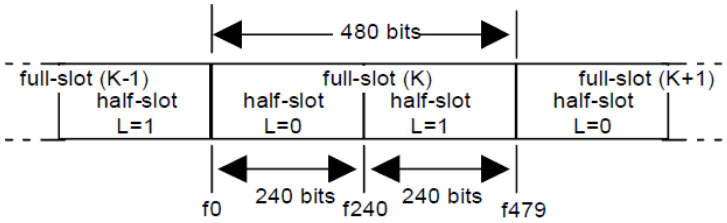

Figure 97 : Format d'un *half slot* [dect2]

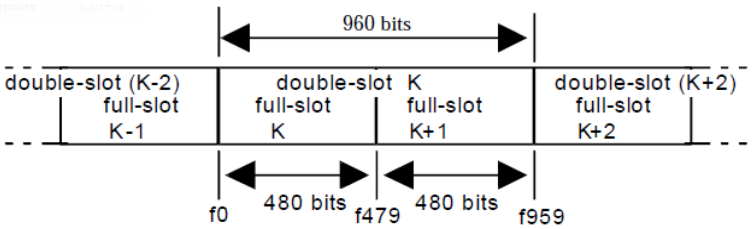

Figure 98 : Format d'un *double slot* [dect2]

Les numéros de *slot* ne sont pas inclus dans chaque transmission de *slot*. Ils sont uniquement définis dans un message spécial (canal Q) transmis à bas débit par toutes les FP.

C.2.1 Paquets physiques

Les données sont transmises dans les dimensions temporelles, fréquentielles et spatiales en utilisant des paquets physiques. Il en existe quatre types :

Tableau XVIII : Paquets physiques DECT

Nom	Type	Nb. de symboles de données	Numérotation
P00	court	96	p0 à p95, p0 = f0
P32	basique	420 ou 424	p0 à p423
P00j	faible capacité	100+j ou 104+j	p0 à p(99+j) ou p(103+j)
P80	haute capacité	900 ou 904	p0 à p899 ou p903

Chaque paquet physique contient un champ de synchronisation **S** et un champ de données **D**. Le champ **S** est utilisé par le récepteur pour stabiliser le lien radio et pour détecter la présence de paquets. Les paquets P80, P32 et P00j peuvent également contenir un champ optionnel **Z** de détection de collision.

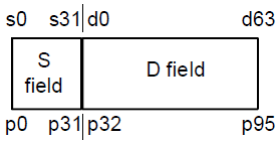

Figure 99 : Paquet P00 [dect2]

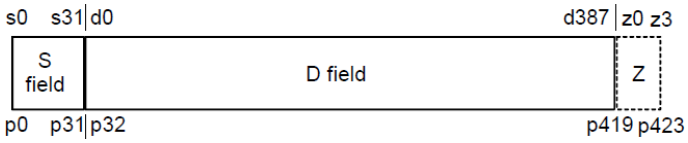

Figure 100 : Paquet P32 [dect2]

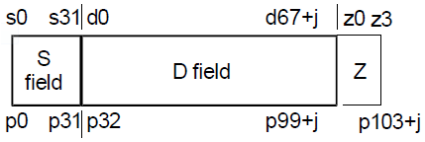

Figure 101 : Paquet P00j [dect2]

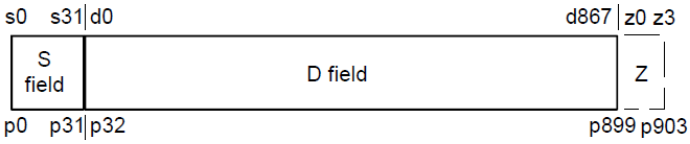

Figure 102 : Paquet P80 [dect2]

Le champ de synchronisation **S**, qui utilise toujours une modulation binaire, comporte 32 bits (s0 à s31) avec 16 bits de préambule et 16 bits de mot de synchronisation paquet. Le champ **S** diffère selon si c'est la RFP ou le PP qui l'émet (les bits sont inversés).

Émission de la RFP :

1010 1010 1010 1010 1110 1001 1000 1010

s0 s15 s16 s31

Émission du PP :

0101 0101 0101 0101 0001 0110 0111 0101

s0 s15 s16 s31

Il existe également un préambule particulier, dit préambule étendu pouvant être utilisé par un récepteur pour la mise en œuvre d'un algorithme de diversité d'antenne. Il correspond au doublement de la séquence binaire du préambule standard [dect2, annexe C].

Les champs de données D sont divisés en trois champs : les champs A, B et X. Un champ **D** est associé à chaque paquet physique et chaque modulation selon le tableau suivant :

Tableau XIX : Les divers champs D [dect2]

	Double slot mode	Full slot mode		Half and long slot mode		
	P80	P32	P00	P00j (j=80)	P00j (j=640)	P00j (j=672)
Configuration	D-field name					
1a	D80a	D32a	D00a	D08a	D64a	D67a
1b	D80b	D32b	D00b	D08b	D64b	D67b
2	D160	D64	D00	D16	D128	D134
3	D240	D96	D00	D24	D192	D201
4a	D160a	D64a	D00a	D16a	D128a	D134a
4b	D240b	D96b	D00b	D24b	D192b	D201b
5	D320	D128	D00	D32	D256	D268
6	D480	D192	D00	D48	D384	D403

Dans tous les cas un champ **D** comporte 68 symboles + la taille du champ **B**. La taille du champ **B** dépend de la taille du paquet physique.

Quatre tailles de champ **D** sont ainsi définies : D00, D08, D32 et D80. Le schéma suivant correspond à la configuration la plus répandue.

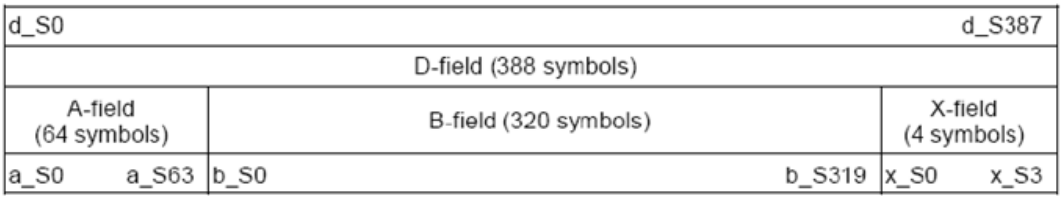

Figure 103: Structure d'un champ D de paquet P32 [dect2]

Le champ **A** est une information de signalisation indiquant les caractéristiques de la trame dont le type de la charge utile et diverses informations réseau. Il est composé d'un en-tête (**H**) de 8 bits (a0 à a7) et d'une queue (**T**) dont la taille varie en fonction du niveau de modulation (64 bits en GFSK). Les 16 derniers bits sont des bits de redondance (RA) pour le contrôle d'erreur des données du champ **A**. Le champ **X** est un code de redondance cyclique (CRC). Il correspond aux quatre derniers symboles du champ **B** (quatre bits en modulation binaire, huit en 4-aire, 12 en 8 aire, etc.).

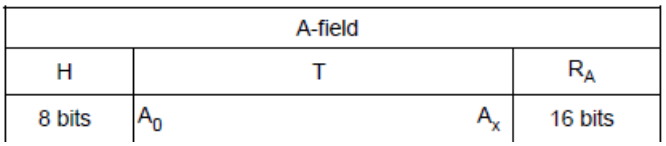

Figure 104 : Structure d'un champ A [dect2]

Le champ **B** contient les données utiles, comme par exemple la voix. Il est toujours sur 320 bits (les donnés sont complétées par une suite de zéros pour atteindre si nécessaire cette longueur).

C.2.2 Canaux physiques

Les canaux physiques sont crées par la transmission entre un PP et une RFP de paquets physiques modulés sur un canal RF particulier, pendant un temps donné en trames successives et pour un emplacement donné. Un canal physique peut servir pour un service simplex sans connexion, tandis qu'une paire de canaux physiques peut fournir un service duplex ou double simplex.

Les canaux physiques sont identifiés par la notation **Ra (K,L,M,N)**, où **a** correspond au type de paquet physique utilisé (sans le P), **K** est le numéro du *full slot* où commence la transmission du paquet, **L** (0 ou 1) indique si la transmission du paquet commence à f0 ou f240, **M** est le numéro du canal RF utilisé pour transmettre le paquet physique, **N** est le numéro du RFP ou RPN (*Radio fixed Part Number*) utilisant le canal physique[59]. A ces paramètres sont rajoutés **s** (= 0 ou 16), indiquant si le préambule du champ de synchronisation **S** est « normal » ou « prolongé », et **z** (= 0 ou 1) pour indiquer la présence ou non d'un champ **Z**. Les différents canaux physiques sont regroupés dans le tableau suivant.

Tableau XX : Canaux physiques DECT

Canal physique	Paquet transporté	K	L	M	N	s	z	Commentaires
R00	P00	{0, ..., 23}	0	{0, …, n}	arbitraire	0/16	0/1	Uniquement transmis dans des *full slots*
R32	P32	{0, ..., 23}	0	{0, …, n}	arbitraire	0/16	0/1	Uniquement transmis dans des *full slots*
R00j	P00j	{0,..., 23}	0/1	{0, …, n}	arbitraire	0/16	0/1	--
R80	P80	{0, …, 10, …, 12, …, 22}	0	{0, …, n}	arbitraire	0/16	0/1	Uniquement transmis dans des *full slots* avec K pair

[59] Attention toutefois : ce numéro dépend du bon vouloir du fabricant et peut être vide de sens dans de nombreux cas.

C.2.3 Modulation de la porteuse RF

La méthode de modulation la plus répandue en DECT est la GFSK (*Gaussian Frequency-Shift Keying*) de BT[60] égal à 0,5. La GFSK est un type de modulation FSK utilisant un filtre Gaussien pour lisser les écarts positif/négatif de fréquence représentant un 0 ou un 1, et limiter ainsi la bande spectrale du signal modulé. Un « 1 » binaire correspond à la transmission d'une porteuse de valeur `Fc+f`, et un « 0 » binaire correspond à la transmission d'une porteuse de valeur `Fc-f`. La valeur nominale de la déviation fréquentielle `f` vaut 288 kHz, mais varie entre environ 200 kHz et 400 kHz selon le motif binaire transmis [dect2]. Comme il a été précisé dans le tableau en page 105, d'autres modulations sont utilisables. Le tableau suivant répertorie les configurations de modulation possibles des champs **S**, **A**, **B**, **X** et **Z** des paquets DECT.

Tableau XXI : Schémas de modulation du DECT [dect2]

Configuration	S–field	A-field	B+X+Z-field
1a	GFSK	GFSK	GFSK
1b	π/2-DBPSK	π/2-DBPSK	π/2-DBPSK
2	π/2-DBPSK	π/2-DBPSK	π/4-DQPSK
3	π/2-DBPSK	π/2-DBPSK	π/8-D8PSK
4a	π/2-DBPSK	π/4-DQPSK	π/4-DQPSK
4b	π/2-DBPSK	π/8-D8PSK	π/8-D8PSK
5	π/2-DBPSK	π/2-DBPSK	16-QAM
6	π/2-DBPSK	π/2-DBPSK	64-QAM

C.2.4 Communication avec la couche MAC

La couche physique communique avec la couche MAC par l'intermédiaire de primitives au travers du D-SAP (*Data field-Service Access Point*). Le D-SAP sert principalement à échanger des champs **D** entre la couche PHY et la couche MAC, à des fins d'ajustement fréquentiel (primitive PL_FREQ_ADJ {req}) ou pour transmettre des informations de collision (PL_TX {req}, PL_RX {req, cfm}).

C.2.5 Communication avec l'entité de gestion de la couche basse

La couche PHY communique avec l'entité de gestion des couches basses (LLME - *Lower Layer Management Entity*) par primitives au travers du PM-SAP (*Physical layer Management entity – Service Access Point*), essentiellement pour invoquer et contrôler les processus de la couche physique :

- recherche d'impulsion de synchronisation (PL_ME_SYNC {req, cfm}),

[60] Cf. page 115 pour une explication du produit BT.

- mesure de force d'un signal sur un canal physique (PL_ME_SIG_STR {req, cfm}) : la force du signal est mesurée sur une bande de 1 MHz centrée sur la fréquence centrale de la porteuse RF concernée,

- agrandissement ou réduction d'une trame (PL_ME_TIME_ADJ {req, cfm}).

A l'aide des mesures de puissance de signaux obtenues via la primitive PL_ME_SIG_STR, la LLME produit deux listes :

- une liste des canaux physiques les plus silencieux, c'est à dire ceux qui subissent le moins d'interférences,

- une liste des canaux dont la force des signaux est la plus forte (effectué uniquement au niveau des PP).

A l'aide de la primitive PL_ME_SYNC et de la détection des numéros de *slot* assuré par la couche supérieure, la LLME doit pouvoir établir le cadencement des trames et *slots*.

C.2.6 Synchronisation entre systèmes adjacents

La synchronisation entre systèmes adjacents permet d'optimiser l'utilisation des ressources radio et améliorer la performance des systèmes synchronisés. Il y a deux classes de synchronisation :

- Classe 1 : augmentation mutuelle de la capacité de trafic de systèmes adjacents par alignement des bandes de garde. Cette classe permet une synchronisation des trames ;

- Classe 2 : utilisée en cas de *handover* entre les deux systèmes. Elle permet une synchronisation de niveau trame et multitrame.

La synchronisation entre FP peut être effectuée de plusieurs manières :

- à l'aide d'un câble entre deux FP,

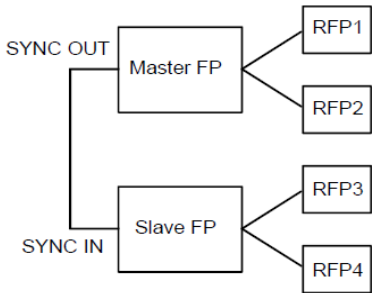

Figure 105 : Synchronisation câblée entre deux FP [dect2]

- à l'aide d'un module GPS (intégré ou externe),

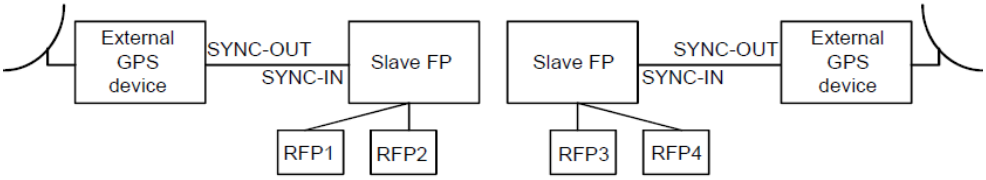

Figure 106 : Synchronisation avec GPS externe [dect2]

- ou un mélange de ces deux configurations.

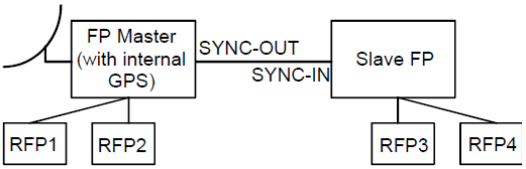

Figure 107 : Synchronisation câblée et avec GPS [dect2]

C.3 Couche MAC

La couche MAC du DECT a deux fonctions principales. Tout d'abord, elle sélectionne les canaux physiques et établit/relâche les connexions à ces canaux. Ensuite elle (dé-)multiplexe des informations de contrôle, ainsi que des informations de couche supérieure et des informations de contrôle d'erreur, en paquets (*bursts*) de la taille d'un *slot*. Ces fonctions sont utilisées pour fournir trois services indépendants : un service de diffusion, un service orienté connexion et un service sans connexion (*connectionless*) [dect3]. Le service de diffusion est une fonction spéciale du DECT : il multiplexe une série d'informations de *broadcast* dans un champ réservé (le champ **A**), et ce champ apparaît dans le cadre de toutes les transmissions actives. Le service de diffusion est toujours transmis dans toutes les cellules (même en l'absence de trafic de l'utilisateur) sur au moins un canal physique. Ces «balises» de transmissions permettent aux PP d'identifier rapidement tous les FP qui sont à sa portée, pour en sélectionner une et s'y verrouiller sans transmission supplémentaire. Dans la norme DECT il y a deux niveaux de multiplexage temporel :

- niveau trame : assuré par la couche PHY (vu précédemment),

- niveau multitrame : assuré par la couche MAC. Une multitrame de 160 ms est composée de 16 trames de 10 ms.

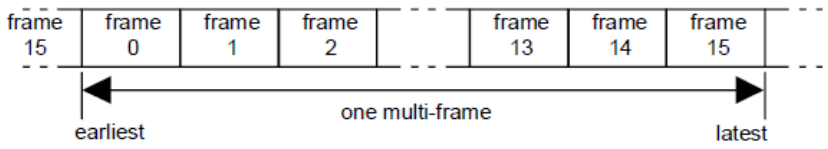

Figure 108 : Multi trame [dect3]

Les numéros de trame ne sont jamais inclus dans une transmission. Les numéros sont déduits du marqueur de multitrame inclus dans toutes les transmissions de FP (ce marqueur est positionné en trame 8 de chaque multitrame). Le schéma suivant détaille la constitution d'une multitrame basique en modulation binaire, c'est-à-dire composée de 16 trames de 10 *full slots*, chaque *full slot* accueillant 480 bits de données (paquet P32 + champ de garde) :

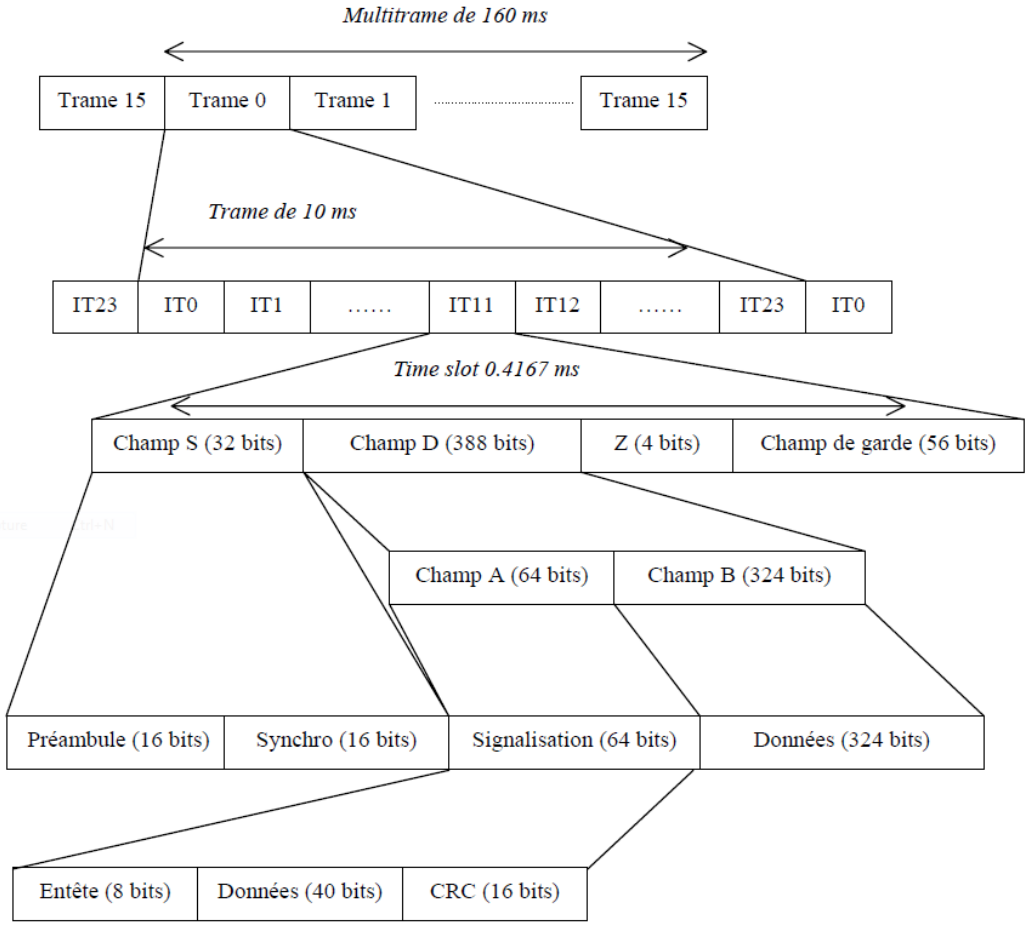

Figure 109 : Structure d'une trame et d'une multitrame [terre]

C.3.1 États de fonctionnement d'un PP

Au niveau de la couche MAC, un PP peut être dans l'un de ces quatre états :

- Actif verrouillé : le PP est synchronisé sur au moins une transmission de RFP et a une ou plusieurs connexions en cours ;

- *Idle* verrouillé : le PP est synchronisé sur au moins une transmission de RFP. Il est capable de créer ou de recevoir des connexions, mais n'en a pas en cours ;

- Actif déverrouillé : le PP n'est synchronisé sur aucune transmission de RFP, et n'est pas capable de créer ou de recevoir des connexions. Le PP tente occasionnellement de détecter une RFP appropriée et de passer en état *idle* verrouillé ;

- *Idle* déverrouillé : le PP n'est synchronisé sur aucune transmission de RFP est n'essaie pas de détecter des RFP.

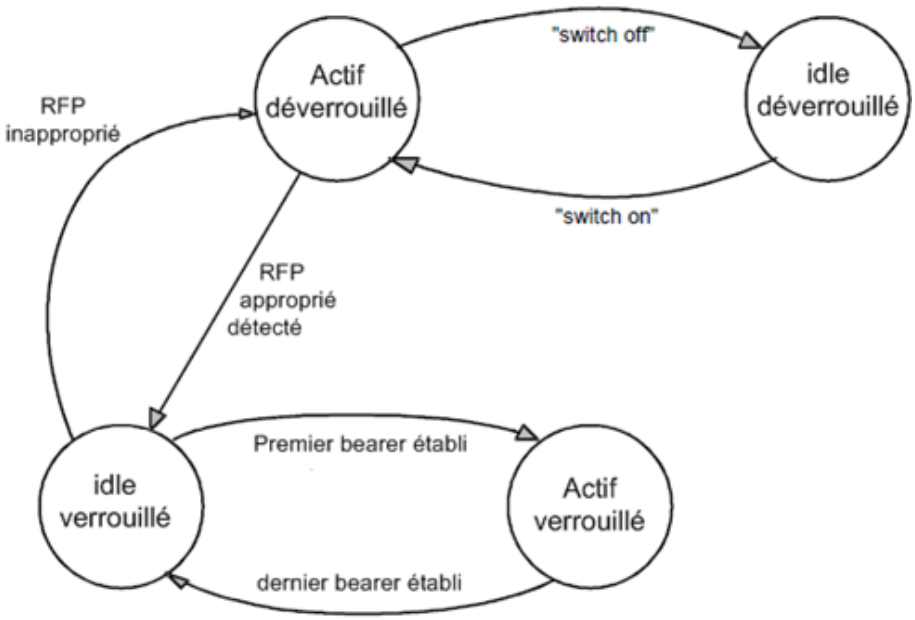

Figure 110 : Diagramme d'état d'un PP (adapté de [dect3])

C.3.2 États de fonctionnement d'un RFP

Au niveau de la couche MAC, un PP peut être dans l'un de ces quatre états :

- inactif : le RFP n'émet ni ne reçoit,

- *idle*-actif ou canal sans connexion : le RFP a au moins un canal de test (*dummy bearer*) ou un canal descendant sans connexion, et le récepteur effectue un sondage des canaux physique selon une séquence donnée,

- actif trafic : le RFP a au moins un canal de trafic, mais n'a pas de canal de test ou de canal descendant sans connexion,

- actif trafic et (canal de test ou sans connexion) : le RFP le RFP a au moins un canal de trafic et maintient un canal de test ou de canal descendant sans connexion.

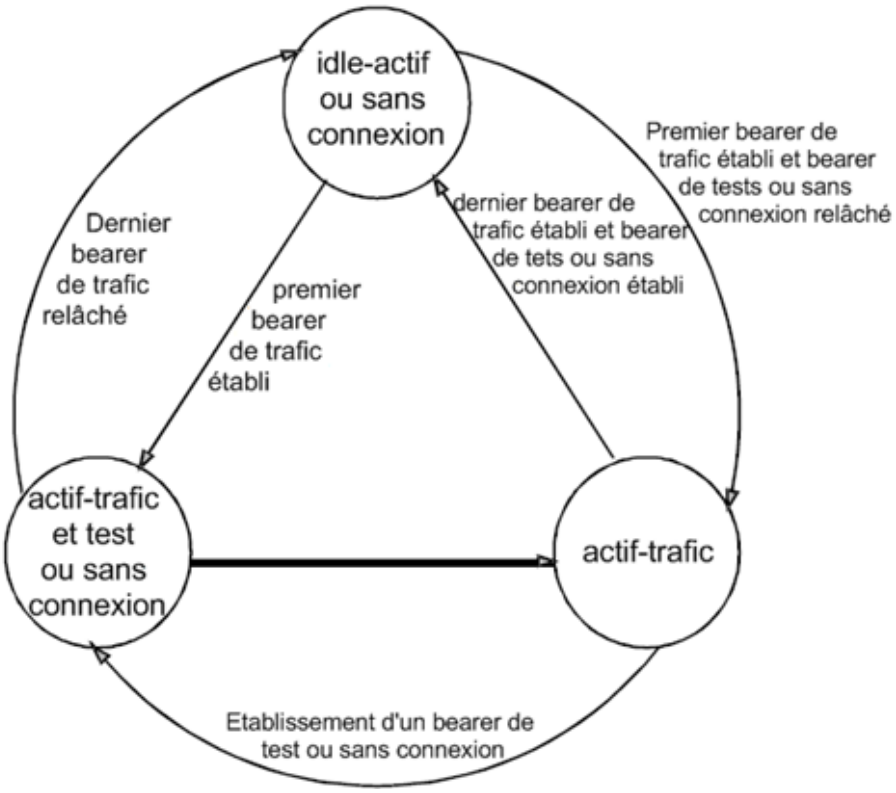

Figure 111 : Diagramme d'état d'un RFP (adapté de [dect3])

Remarque : un *bearer* correspond à une instance de service unique d'une couche physique. C'est globalement l'utilisation d'un canal physique pendant une durée donnée pour fournir un service donné. Il existe quatre types de *bearer* :

- simplex *bearer* : allocation d'un canal physique pour des transmissions monodirectionnelles,

- duplex *bearer* : paire de simplex *bearer* opérant sur deux canaux physiques de sens opposés, utilisant une même porteuse RF et dont les points de départ des *time slots* sont séparés d'une demi-trame,

- double simplex *bearer* : idem duplex *bearer* à la différence près que les canaux physiques des simplex *bearers* opèrent dans le même sens,

- double duplex *bearer* : paire de duplex *bearers* associés à la même connexion MAC.

Un *bearer* peut être dans l'un des trois états opérationnels suivants :

- *dummy bearer* : simplex *bearer* utilisé pour la transmission d'information de *broadcast* entre un RFP et un PP,

- *traffic bearer* : double simplex *bearer* utilisé pour les transmissions point à point,

- *connectionless* (C/L) *bearer* : utilisé pour des transmissions sans connexion.

La couche MAC offre trois groupes de services au profit des couches supérieures et de la LLME :

- *Broadcast Message Control* (BMC) : services continus "point à multipoint" (un RFP vers plusieurs PP) sans connexion,

- *Connectionless Message Control* (CMC) : services (pouvant être bidirectionnels) "point à point" ou "point à multipoint" (un RFP vers plusieurs PP) sans connexion,

- *Multi-Bearer Control* (MBC) : services duplex ou simplex "point à point" orientés connexion entre un RFP et un PP.

A ces groupes de service sont associés divers types de canaux logiques selon la répartition suivante :

- MC-SAP (C_S, C_F, I_N, I_P et G_F) pour le groupe MBC,

- MB-SAP (CL_S, CL_F, SI_N et SI_P) pour le groupe CMC,

- MA-SAP (B_S),

- canaux de contrôle MAC internes (Q, N, M, P).

Deux canaux logiques sont particulièrement intéressants : les canaux Q et N. Le canal Q est le canal « informations du système », canal simplex utilisé pour alimenter les PP avec des informations relatives au RFP. Les canaux Q sont en général transmis de façon répétée en *broadcast* via des *traffic*, *connectionless* et *dummy bearers*, ou bien être transmis à la demande. Certaines informations de canaux Q sont requises par les PP pour passer de l'état actif déverrouillé à l'état *idle* verrouillé. Le canal N est le canal « identités », utilisé pour les transmissions répétées de l'identité d'un système. Les données du canal N sont transmises par les RFP sur des *traffic*, *connectionless* et *dummy bearers*, et par les PP sur des *traffic bearers*. Les canaux N ont deux rôles :

- pour les PP à l'état actif déverrouillé : même rôle que le canal Q. Le canal N aide les PP à trouver un système offrant le service désiré et pour lequel ils ont un droit d'accès,

- pour les PP à l'état actif verrouillé : le canal N est utilisé pour effectuer une « poignée de main » (MAC *layer handshake*) entre RFP et PP.

C.3.3 Messages de la couche d'accès au média

Sauf cas particulier, les valeurs contenues dans les champs **A** et **B** sont codées en binaire naturel et sont arrangées de façon à ce que le MSB est transmis en premier et le LSB en dernier.

	0 MSB	1	1	0	0 LSB	
	a_{13} bn_{13}	a_{14} bn_{14}	a_{15} bn_{15}	a_{16} bn_{16}	a_{17} bn_{17}	

Figure 112 : Exemple de codage de champs A et B [dect3]

Différents messages peuvent être multiplexés dans le champ **T** du champ **A** (algorithme T-MUX). Les contenus d'un champ **T** sont définis pour chaque trame à l'aide des bits a0 à a3 du champ **H**. Parmi les différents messages possibles deux sont intéressant : les messages de canal N (N_T), de canal Q (Q_T) et de canal M (M_T).

Head	Tail	R-CRC
	a_8 ... a_{47}	
	Tail message - 40 bits	

Figure 113 : Champ T [dect3]

C.3.4 Informations d'identités (message NT, a0a1a1 = 011)

La LLME d'un RFP alimente la couche MAC avec un identifiant de droit d'accès primaire ou PARI (*Primary Access Rights Identity*) de 32 bits ou 37 bits (bit E compris). Le RFP ajoute son RPN (*Radio Fixed Part Number*) de 8 bits ou 3 bits au bout de ce SDU pour constituer les 40 bits de la queue (champ **T**) du champ **A**. Le message de 40 bits ainsi constitué forme le RFPI (*Radio Fixed Part Identity*). C'est le seul message de type N_T envoyé par un RFP. Le LSB du RFPI est positionné au bit a47.

E	Primary Access Rights Identifier (PARI)	RPN
a_8		a_{47}
	RFPI Message (N channel)	

Figure 114 : Message RFPI [dect3]

C.3.5 Informations système et marqueur de multitrame (message QT, a0a1a2 = 100)

Le message Q_T est transmis une fois par multitrame.

header Q_H	system information
a_8 - a_{11}	a_{12} ... a_{47}

Figure 115 : Champ T de type Q [dect3]

Le champ Q_H est utilisé pour identifier 16 types d'informations système. Ceux qui nous intéressent sont :

- Q_H = 0, 1 (hexadécimal.) : informations système statiques,

Q_H 0 0 0 N R	SN	SP	esc	Txs	Mc	RF-carriers	spr	CN	spr	PSCN
a_8 a_{11}	a_{12} a_{15}	a_{16} a_{17}	a_{18}	a_{19} a_{20}	a_{21}	a_{22} a_{31}	a_{32} a_{33}	a_{34} a_{39}	a_{40} a_{41}	a_{42} a_{47}

Figure 116 : Informations système statiques [dect3]

, où SN est l'indice de la paire de *slot* de début de transmissions, Txs le nombre de transmetteurs du RFP (1 à 4 et plus) et CN le numéro de la porteuse (0 à 63)

- Q_H = 5 : SARI

Q_H 0 1 0 1	SARI message
a_8 a_{11}	a_{12} a_{47}

Figure 117 : Message SARI [dect3]

C.3.6 Contrôle MAC (message MT, a0a1a2 = 110)

Le message M_T contient une information de contrôle de la couche MAC.

M_T header	command	more headers or information
a_8 a_{11}	a_{12} a_{15}	a_{16} a_{47}

Figure 118 : Message M_T [dect3]

L'en-tête (a8 à a11) indique le type de contrôle. Deux types sont intéressants : le contrôle de chiffrement et le message TARI.

C.3.6.1 Contrôle de chiffrement

Ce message donne une indication du début et de la fin du chiffrement des données

0 1 0 1	command	FMID	PMID
a_8 a_{11}	a_{12} a_{15}	a_{16} a_{27}	a_{28} a_{47}

Figure 119 : Message M_T - contrôle de chiffrement [dect3]

Tableau XXII: Contrôle de chiffrement – champ `command` [dect3]

Command				Message
0	0	x	x	start encryption
0	1	x	x	stop encryption
1	0	x	x	start encryption with cipher key-index (see note)
1	1	x	x	reserved
x	x	0	0	request
x	x	0	1	confirm
x	x	1	0	grant
x	x	1	1	reserved

C.3.6.2 Message TARI

1 0 0 0	TARI field
a_8 a_{11}	a_{12} a_{47}

Figure 120 : Message MT – message TARI [dect3]

C.4 Identification des FP

La structure d'identification commune des équipements DECT fixes (FP) et mobiles (PP) est composée de la classe des droits d'accès ou ARC (*Access Rights Class*) et du détail des droits d'accès ou ARD (*Access Rights Details*). L'ARC et l'ARD constituent pour un FP en une identité de droits d'accès (*Access Rights Identity* - ARI), et pour un PP une clé de droits d'accès (*Portable Access Rights Key* – PARK). La différence entre une PARK et un ARI est qu'à chaque PARK peut être attribué à un groupe d'ARD, d'où la dénomination PARK{y}. Les FP *identities* ou ARI permettent d'informer les PP de l'identité de, et des droits d'accès à un FP. Un FP transmet en *broadcast* cette information sur le canal N (message N_T) par l'intermédiaire de tous ses RFP, au moins une fois par multitrame.

Si une ARI est primaire (PARI), elle forme avec le numéro de RFP *(Radio Fixed Part Number* - RPN), l'identité unique diffusée par un RFP (*Radio Fixed Part Identity* – RFPI) via le canal N_T. Une ARI peut toutefois être diffusée (mais moins fréquemment) en tant qu'ARI secondaire (*Secondary Access Rights Identity* – SARI) sous la forme d'un message distinct transmis sur le canal Q_T. Une ARI tertiaire (*Tertiary Access Rights Identity* – TARI) est également disponible, mais non diffusée (elle est transmise suite à une requête formulée par un PP). La RFPI a trois rôles : porter l'information PARI, identifier de façon unique les RFP environnants et indiquer les domaines de *handover* (interne dans un FP ou externe entre FP) et les zones de localisation. La RFPI est transmise sur les bits a8 à a47 du champ **A** en utilisant le canal N_T.

Le type de PP ou PUT (*Portable User Type*) et le numéro de PP ou PUN (*Portable User Number*) forment l'identité internationale d'un PP *(International Portable User Identity* - IPUI). Un PP est identifié par sa paire PARK{y}-IPUI. Un PP n'est autorisé à accéder à un FP que si l'une de ses PARK contient l'une des ARI du FP, c'est à dire la PARI, la SARI ou la TARI. L'IPUI est utilisé pour identifier le PP dans le domaine défini par son ARI de rattachement. L'IPUI peut être unique localement ou globalement.

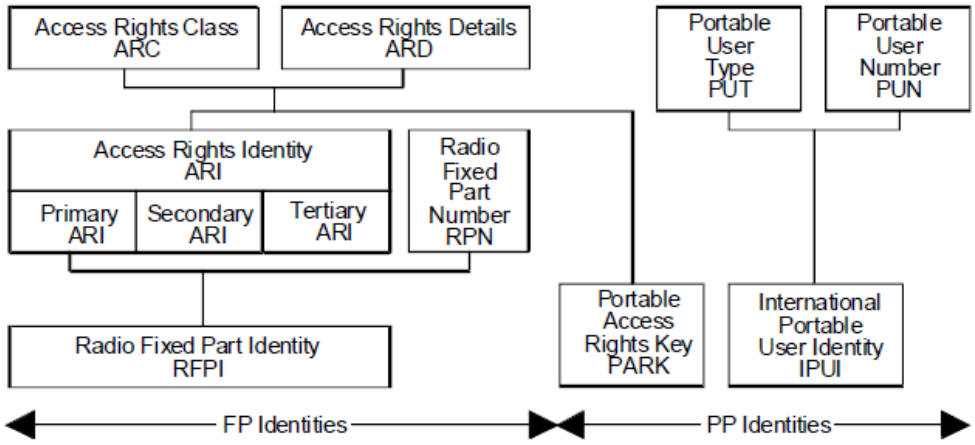

Figure 121 : Structure d'identification générale du DECT [dect6]

Cinq types d'ARI (ARC classes A à E) et différents types d'IPUI ont été définis pour pouvoir identifier les systèmes constituant une installation DECT. Le tableau suivant donne une vue générale des combinaisons des principales identités.

Tableau XXIII: Combinaisons des identités ARI, PARK et IPUI [dect6]

ARI class	Environment	SARI/ TARI	PARK class	IPUI type
A	Residential and private (PBX) single and small multiple cell systems	No	A	N, S
B	Private (PABXs) multiple cell	Yes	B	O, S, T
C	Public single- and multiple cell systems	Yes	C	P, Q, R, S, U
D	Public DECT access to a GSM/UMTS operator network	Yes	D	R
E	PP to PP direct communication (private)	Yes	E	N

Tableau XXIV : Codage des classes de droits d'accès (champ ARC) [dect6]

Binary code	ARC
000	A
001	B
010	C
011	D
100	E
101	F
110	G
111	H

C.4.1 Classe A

La classe A concerne les petits FP monocellules résidentiels ou privés (PBX) et les petits FP multicellules avec un maximum de sept RFP. Une ARI de classe A est globalement unique.

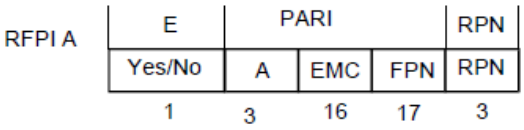

Figure 122 : RFPI classe A [dect6]

Une RFPI de classe A contient notamment les informations suivantes :

- EMC (*Equipment Manufacturer's Code*) : code sur 16 bits (valeur 0 interdite), attribué à chaque fabricant par l'ETSI ou un fournisseur autorisé par l'ETSI. Les gros fabricants peuvent avoir plus d'un EMC ;

- FPN (*Fixed Part Number*) : numéro de FP unique (pour un EMC donné) attribué par le fabricant (valeur maximale 131 071) ;

- RPN (*Radio fixed Part Number*) : numéro de RFP sur 3 bits, attribué par le fabricant ou installateur, et utilisé pour identifier jusqu'à sept RFP au sein d'un FP. Dans le cas d'un FP monocellule, RPN = 0. Cela indique accessoirement que ce FP n'a pas de *handover* intercellule.

Remarque : Le champ E indique si une SARI est disponible.

C.4.2 Classe B

La classe B est réservée aux installations privées plus complexes tels que les LAN et les PABX multicellules. Les RFPI sont attribués soit directement par le fabricant, soit par un revendeur, voire un installateur autorisé par le fabricant. Un ARI de classe B est géographiquement unique.

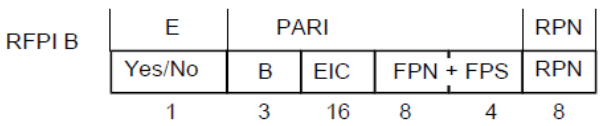

Figure 123 : RFPI classe B [dect6]

Une RFPI de classe B contient notamment les informations suivantes :

- EIC (*Equipment Installer's Code*) : code sur 16 bits (valeur 0 interdite), attribué à chaque fabricant par l'ETSI ou un fournisseur autorisé par l'ETSI. Les gros fabricants

peuvent avoir plus d'un EIC. De grandes compagnies peuvent réutiliser leurs codes EIC sur différents sites ;

- FPN : numéro généralement sur 8 bits (0 interdit), distribué avec l'EIC par le fabricant aux installateurs autorisés ;

- FPS (*Fixed Part Sub-number*) : numéro généralement su 4 bits, attribué par l'opérateur du système ou l'installateur. Dans tous les cas l'ensemble "FPN + FPS" est sur 12 bits et est unique pour chaque UIC ;

RPN : numéro sur 8 bits, attribué par l'opérateur ou l'installateur. La limite de 256 RFP peut toutefois être dépassée par séparation géographique.

C.4.3 Classe C

La classe C est réservée aux accès publics ou à la boucle locale. Un ARI de classe C est géographiquement unique.

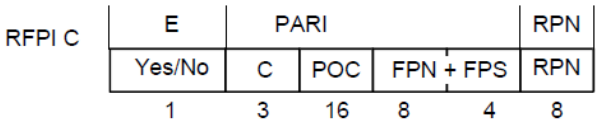

Figure 124 : RFPI classe C [dect6]

Une RFPI de classe C contient notamment les informations suivantes :

- POC (*Public Operator Code*) : code sur 16 bits (valeur 0 interdite) attribué à l'unité ou par bloc à un opérateur par l'ETSI ou un fournisseur de service autorisé par l'ETSI ;

- FPN : attribué par l'opérateur de FP, ce numéro peut être utilisé pour définir différentes zones d'abonnement ;

- FPS : idem classe B ;

- RPN : idem classe B. Les RFPI monocellules ont un LSB égal à 0 pour indiquer l'absence de *handover* dans le FP.

C.4.4 Classe D

Cette classe est réservée à un usage public où le réseau DECT est directement relié à un réseau mobile 2G ou 3G. Cette classe est destinée aux usagers DECT disposant d'abonnement GSM/UMTS. Dans cette classe les PARI ne doivent être utilisés que dans des réseaux DECT appartenant à un opérateur GSM/UMTS. Un ARI de classe D est géographiquement unique.

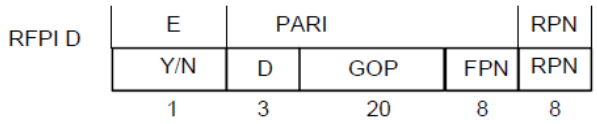

Figure 125 : RFPI classe D [dect6]

Une RFPI de classe D contient notamment les informations suivantes :

- GOP (*GSM OPerator code*) : code d'opérateur GSM/UMTS, connu sous l'appellation PLMN-id (*Public Land Mobile Network Identification*) en terminologie GSM. Ce code est composé du MCC (*Mobile Country Code*) et du MNC (*Mobile Network Code*) ;

- FPN : attribué par l'opérateur GSM/UMTS, ce code sur 8 bits (valeur 0 interdite) est utilisé pour séparer géographiquement les systèmes DECT ;

- RPN : attribué par l'opérateur/installateur GSM/UMTS. Idem classe C.

C.4.5 Classe E

Cette classe est réservée aux communications PP à PP. Les RFPI peuvent être attribués temporairement par l'utilisateur du PP et pour une ou plusieurs applications données en saisissant un code de cinq digits ou TPUI (*Temporary Portable User Identity*).

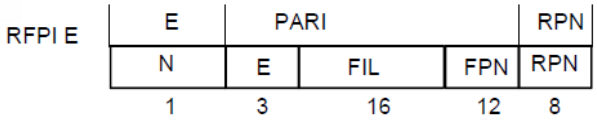

Figure 126 : RFPI classe E [dect6]

Une RFPI de classe E contient notamment les informations suivantes :

- FIL (FILl bits) : motif binaire 0101 sur 16 bits ;

- FPN : numéro aléatoire (valeur décimale entre 001 et 999) commun au groupe de PP appartenant au réseau PP à PP considéré. Saisie au clavier possible ;

- RPN : numéro (valeur décimale entre 01 et 99) utilisé par un PP pour initier un appel PP à PP à l'aide d'un *dummy bearer*.

Annexe D
Composition des cartes Ettus

Remarque : les intitulés type "U…" (ou autre lettre) font référence à l'identification des composants sur les cartes électroniques.

D.1 Composition matérielle de l'USRP1

En détail, la carte mère de l'USRP1 est constituée de :

- Un FPGA (U101) Altera Cyclone EP1C12 240-Pin PQFP [ep1c12], qui implémente en configuration standard quelques opérations de traitement numérique du signal pour la conversion du taux d'échantillonnage et la transposition numérique en (ou de la) bande de base ;

- Un module de conversion A/N et N/A assuré par deux processeurs frontaux de signaux mixtes (*codec*) Analog Devices AD9862 (U601 et U602) comportant chacun deux CAN (64 Méch/s, 12 bits, SFDR 85dB) permettant de gérer au total quatre canaux d'entrée analogique (ou deux paires I/Q), et deux CNA (128 Méch/s, 14 bits, SFDR 83 dB) gérant quatre canaux de sortie analogique (ou deux paires I/Q) ; [ad9862]

- Un contrôleur USB 2.0 (U412) Cypress EZ-USB FX2 CY7C68013−TQ100, qui assure le transport des données entre l'hôte et la carte mère USRP1 ; [cypress]

- Quatre connecteurs d'extension (2 T_X : J667et J669 ; 2 R_X : J666 et J668) afin de relier deux à quatre cartes filles. Remarque : l'USRP1 est compatible MIMO 2x2 ;

- Une EEPROM 2 kbits (U413) Microchip 24LC02B [24lc02b] ;

- Divers connecteurs (J3, J401, J502, J2001 et J2002) ;

- Un peu de glue logique :
    - Régulateurs de tension (U502, U503 et U701) Linear Technology LT1085CM−3.3 [lt1085], Texas Instrument TPS777xx [tps777] et Analog Devices ADP3336 [adp336] ;
    - Circuit intégré de distribution horaire (U702) Analog Devices AD9513 [ad9513] ;

- Oscillateur à quartz 64 MHz contrôlé en tension et compensé en température VCTCXO (X2).

Le circuit AD9862 présente de multiples fonctions. Des amplificateurs programmables ou PGA (*Programmable Gain Amplifier*) précèdent les CAN de manière à ajuster le niveau du signal d'entrée pour maximiser la plage dynamique du CAN. De même les CNA sont suivis d'un PGA. Le circuit d'émission dispose d'un interpolateur et d'un convertisseur/éleveur pour adapter le taux d'échantillonnage de sortie au taux d'échantillonnage du CNA et transposer l'entrée bande de base en sortie basse FI.

D.2 Composition matérielle de l'USRP2

La carte mère de l'USRP2 est composée de :

- Un FPGA (U1) Xilinx Spartan-3 XC3S2000 [spartan3] intégrant un processeur *softcore* AeMB RISC 32 bits 50 MHz et implémentant en configuration standard :
  - deux DDC embarqués assurent le mélange, le filtrage et la décimation jusqu'à 100 Méch/s des signaux entrant dans le FPGA ;
  - deux DUC assurant l'interpolation des signaux bande de base jusqu'à 100 Méch/s avant de les transposer à la fréquence désirée ;

- Un double CAN (U2) 14 Bits, 105Méch/s, SNR 72.4dB et dynamique de codage 85dB Linear Technology LTC2284 [ltc2284] ;

- Un double CNA (U3) 16 bits 400 Méch/s (en sortie, mais 100 Méch/s en entrée) Analog Devices AD9777 [ad9777] ;

- Deux CNA auxiliaires (U4 et U5) 12 bits Analog Devices AD5623 [ad5623] ;

- Deux CAN auxiliaires (U6 et U7) 12 bits Analog Devices AD7922 [ad7922] ;

- Une interface Ethernet 10/100/1000 Mbit/s (U12) National Semiconductor DP83865 [dp83865] ;

- Deux connecteurs d'extension (1 T_X : J401, 1 R_X : J402) afin de relier une à deux cartes filles. Remarque : un seul USRP2 n'est pas compatible MIMO 2x2, mais en en reliant plusieurs il est possible de créer un système compatible MIMO jusqu'à 8x8 ;

- Un lecteur de carte SD ;

- Une SRAM Cypress (U19) 1 Mo CY7C1356C [cy7c] ;

- Une EEPROM (U11) 2 kbits Microchip 24LC024 [24lc024] ;

- Des connecteurs J101 à J108, J201, J204, J203, J301 (MICTOR43−LA), J305, J504, J505, J601 (BEL 0826−1X1T−23−F), J707 (IPASS−SAS−X4−SHLD et IPASS−SAS−X4) ;

- et un peu de glue logique :

  - Oscillateur 100 MHz à bruit de phase ultra faible VCXO CRYSTEK CVHD-950 (U8) [crystek] ;
  - Circuit de distribution d'horloge (U9) 1.2 GHz Analog Devices AD9510 [ad9510] ;
  - CPLD (U10) Xilinx XC9572 VQ44 pour charger le *bitstream* FPGA de la carte SD vers le FPGA [cpld9572] ;
  - "Sérialiseur/désérialiseur" multigigabit Texas Instruments TLK2701 (U13) [tlk2701] ;
  - Deux régulateurs à découpage 2A (U14 et U15) Linear Technology LT 3510 [lt3510] ;
  - Un translateur de niveau logique (U17) : Analog Devices ADG3301 [adg3301] ;
  - Un commutateur 2x2 800 Mbit/s à signalisation différentielle basse tension (LVDS) (U18) National Semiconductor DS90CP22 [ds90cp] ;
  - Un récepteur LVDS différentiel 3V (U20) National Semiconductor DS90LT012AH [ds90lt] ;
  - Un régulateur linéaire CMOS (U22) National Semiconductor LP38692MP [lp38692] ;
  - Un double oscillateur (U23) LTC6908 [ltc6908] ;
  - Un circuit de R.A.Z (U24) Maxim MAX6749KA+T [max6749] ;
  - Trois convertisseurs de tension (U31, U32 et U33) Texas Instruments SN74AUP1T57 [sn74].

D.3 Composition matérielle de certaines cartes RF Ettus

D.3.1 TVRX

La TVRX (version 1) est composée de :

- EEPROM série 2kbits (U1) Microchip 24LC025B [24lc024] ;

- Tuner Microtune MT4937DI5 (U2) [mt4937];

- Régulateur de tension (U3) National Semiconductor LM2940IMP [lm2940] ;

- Dual AGC (U4) ;

- Connecteur 64 pins J2 ; 2 connecteurs 16 pins (J24 et J25).

D.3.2 DBSRX2

La DBSRX2 est composée de :

- EEPROM (U1) 2 kbits Microchip 24LC024 [24lc024] ;

- Régulateur de tension (U2) LM2940IMP [lm2940] ;

- Tuner à conversion directe MAXIM MAX2112ETI+ (U3) [max2112] ;

- Amplificateur faible bruit (U4) Avago MGA62563 [mga62563], gain 22 dB et figure de bruit 0,9 dB ;

- Amplificateurs différentiels (U5 et U6) Analog Devices AD8132 [ad8132] ;

- Connecteur J3, J100 ; connecteur 64 pins J2 ; 2 connecteurs 16 pins (J24 et J25).

D.3.3 RFX900

La RFX900 est composée de :

- Modulateur I/Q Analog Devices AD8349 (U101) [ad8349] ;

- Démodulateur I/Q [800 MHz – 2.7 GHz] (U2) Analog Devices AD8347 [ad8347] ;

- Deux EEPROM (U1 et U102) 2 kbits Microchip 24LC025B [24lc024] ;

- Deux VCO/synthétiseur de fréquence (U3 et U103) Analog Devices ADF4360-3 [adf4360] ;

- Deux amplificateurs faible bruit (U4 et U104) Avago MGA82563 [mga82563], gain 13 dB et figure de bruit 2,2 dB ;

- Amplificateur large bande RF3315 (U105) [rf3315] ;

- Deux commutateurs émission/réception [DC – 3 GHz] (U202 et U209) Hittite HMC174MS8 [hmc174ms8] ;

- Bloc de 6 inverseurs Fairchild Semiconductor 74AC04 (U204) [74ac04] ;

- Filtre à onde de surface (SAW) 915 MHz SAWTEK856327 (FIL1) [856327] ;

- Deux régulateurs de tension (U5 et U6) Analog Devices ADP3336 [adp3336] ;

- Régulateur de tension (U203) Analog Devices ADP3336 [adp3336] ;

- Connecteurs (J3, J100, J202, 16 pins J101, 64 pins J102, 16 pins J24, 64 pins J1) ;

D.3.4 RFX1800

Le schéma de brochage du RFX1800 est quasi-identique à celui du RFX900[61].

D.3.5 WBX

La WBX (révision 2) est composée de :

- Deux commutateurs émission/réception [DC – 3 GHz] (U202 et U209) Hittite HMC174MS8 [hmc174ms8] [62] ;

- Modulateur I/Q [50 MHz – 2 GHz] (U501) Analog Devices ADL5386 [adl5386] ;

- Démodulateur I/Q [50 MHz – 2 GHz] (U307) Analog Devices ADL5387 [adl5387] ;

- EEPROM (U202) 2 kbits Microchip 24LC025B [24lc024] ;

- EEPROM (U403) 2 kbits Microchip 24LC024 [24lc024] ;

- Atténuateur numérique programmable 6 bits par pas de 0,5 dB Hittite HMC472LP4 (U302) [hmc472lp4] ;

- Quatre régulateurs de tension (U306, U308, U503 et U505) Analog Devices ADP3336 [adp3336] ;

- Amplificateur différentiel ADA4937−2 (U304) [ada4937] ;

- Deux synthétiseurs large bande avec VCO (U201 et U401) Analog Devices ADF4350 [adf4350] ;

- Amplificateur faible bruit (U313) Avago MGA82563 [mga82563] ;

- Amplificateur faible bruit Avago MGA62563 [mga62563][63] ;

- Connecteurs J101, J102, J203, J404, J405, 64 pins J201, 64 pins J402, 40 pins J109.

[61] Seule la présence d'un filtre différencie physiquement la RFX900 de la RFX1800.
[62] Le schéma de brochage de la WBX consultable sur le site d'Ettus Research LLC [wbxsch] ne mentionne pas ce composant, probablement parce qu'il s'agit du schéma de la WBX révision 1.
[63] Cf. note de bas de page "62".

Annexe E
Techniques de programmation

E.1 Programmation Linéaire

La programmation linéaire ou LP (*Linear Programming*) est une méthode dans laquelle un développeur suit un processus linéaire de réflexion pour l'élaboration du code. Le processus suivant un cheminement logique, la LP est dominée par des structures conditionnelles, des boucles et des fonctions. Le langage C est l'un des langages de LP les plus populaires.

E.2 Programmation orientée objet

La programmation orientée objet ou OOP (*Object-Oriented Programming*) est radicalement différente de la précédente. Elle s'appuie sur la notion d'objet. Un objet est un assemblage d'attributs (variables, constantes, objet) et de méthodes qui utilisent ces attributs. Une classe est le type d'un objet, et un objet est une instance spécifique d'une classe particulière. Deux langages d'OOP particulièrement populaires sont Java et C++.

E.3 Programmation à base de composants

La programmation à base de composants ou CBP (*Component-base Programming*) est une extension subtile de la précédente. Un composant comprend une ou plusieurs classes, et est complètement défini par ses interfaces et fonctionnalités. L'objectif de cette technique de programmation, qui n'a pas de langage explicitement dédié, est de créer des composants autonomes et facilement interchangeables entre différentes implémentations.

E.4 Programmation Orientée Aspect

La programmation orientée aspect ou AOP (*Aspect-Oriented Programming*) permet la création de relations entre différentes classes. Contrairement à la CBP, l'AOP exige la création de nouvelles constructions de langage pour associer un aspect à une classe particulière. A cette fin, il existe différents langages AOP : AspectJ, AspectC++, Aspect #, entre autres.

E.5 Patrons de conception (Design Patterns)

Un patron de conception est un concept de génie logiciel, indépendant du langage de programmation, décrivant des procédés de conception généraux pour un contexte d'architecture logicielle particulier. Certaines architectures logicielles, telles que le SCA, utilise cette technique, notamment pour le développement des formes d'onde.

Annexe F
Plateformes de recherche

F.1 BEE2

Le *Berkeley Emulation Engine* 2 (BEE2) est une plateforme de radio logicielle utilisée pour des applications nécessitant de grosses capacités calculatoires, notamment en radioastronomie [bee2] [chang] [mishra], mais aussi pour la recherche en radio intelligente et les mesures relatives à l'exploitation de bandes de fréquences larges ou étroites [mellers]. L'architecture matérielle du BEE2 comporte des modules de traitement et des cartes RF modulaires. La carte mère contient cinq FPGA Virtex II Pro 70 disposés en étoile (quatre de calcul interconnectés par des liaisons à 40 Gbit/s et un de contrôle, relié aux quatre autres par des liaisons à 20 Gbit/s) intégrant chacun un PowerPC405. L'ensemble constitue un FPGA virtuel dont la puissance est multiplié par cinq, et peut être relié à au maximum dix-huit cartes RF via des interfaces InfiniBand 4X (IB4X) à 8*1.25 Gbit/s. Chaque FPGA peut être connecté à 4 Go de RAM DDR2. Les cartes filles contiennent des filtres, un CAN 12 bits 64 Méch/s, un CNA 14 bits 128 Méch/s, un FPGA Xilinx Virtex-II Pro et un modem RF séparé de bande passante instantanée 20 MHz ajustable dans les 80 MHz de la bande ISM 2.4 GHz. Ces modules RF peuvent fonctionner en FDD (*Frequency Division Duplexing*) ou en TDD (*Time Division Duplexing*). Avec quatre cartes filles (ou plus) il est ainsi possible de couvrir l'intégralité des 80 MHz de la bande ISM 2.4 GHz. L'ensemble des opérations de traitement du signal étant réalisé sur la plateforme, cette dernière se suffit d'une connexion bas-débit avec le PC. [bwrc]

F.2 CalRadio

CalRadio est un programme de recherche et de développement d'émetteur/récepteur sans-fil mettant en œuvre des plateformes de test. Le domaine de recherche couvre un large spectre de fonctionnalités intégrées dans un équipement de transmission radiofréquence [calradio]. Une plateforme CalRadio dédiée à la norme 802.11b, la CalRadio 1a, est commercialisée par la société Maxentric. Elle est notamment composée d'une carte mère contenant un DSP Texas Instruments TMS320VC5471 intégrant un microprocesseur ARM à noyau uClinux, quatre CAN TLV2541 et quatre CNA TLV5636 Texas Instruments 12 bits utilisés à 100 kéch/s, une interface Ethernet 10/100, 16 Mo de SDRAM, 4 Mo de Flash ROM et 2 Mo de SRAM [maxentric], et d'une carte RF contenant une

émetteur/récepteur [2.4 GHz – 2.5 GHz] à conversion directe Maxim MAX2820. Une seconde plateforme, la CalRadio 1b, est en cours de développement.

F.3 Chameleonic Radio

Chameleonic Radio est un prototype expérimental de radio multibande et multimode, élaboré par l'université d'état et institut polytechnique de Virginie (Virginia Tech), opérant dans les bandes de fréquences de la sécurité publique américaine, à savoir [138 MHz - 174 MHz], [220 MHz - 222 MHz], [406 MHz - 512 MHz] et [764 MHz - 900 MHz], et capable d'opérer dans les bandes 2,4 GHz et 4,9 GHz moyennant quelques extensions dans le design [ellingson]. *Chameleonic Radio* a pour particularité d'utiliser un prototype de circuit intégré RF (RFIC) Motorola capable d'accorder dans la bande [100 MHz – 2,5 GHz] avec une bande passante instantanée de 4,25 kHz à 10 MHz. Il est également constitué d'un FPGA Altera Stratix II, un micro-PC Gumstix fonctionnant sous Linux et un écran tactile LCD utilisés comme interface utilisateur. [gumstix]

F.4 VT-CORNET

Virginia Tech Cognitive Radio Network Testbed (VT-CORNET) est une plateforme de test de radio intelligente basée sur un réseau de 48 USRP2. Sur chaque USRP2 est enfichée une carte RF développée par une équipe de Virginia Tech. Cette carte contient notamment le RFIC Motorola Version 4.0 cité précédemment. Elle fonctionne dans la bande [100 MHz – 4 GHz] avec une bande passante instantanée de 20 MHz, un gain variable jusqu'à 50 dB et une réjection des bandes latérales de 60 dB. L'ensemble est relié par des liaisons Gigabit Ethernet à autant de serveurs Xeon *Quad Core* fonctionnant en *cluster*, et utilise l'API CROSS (*Cognitive Radio Open Source System*) et l'architecture logicielle OSSIE. [vtcornet]

F.5 FPGA4U

FPGA4U est une carte de développement basée sur un FPGA ALTERA Cyclone II EP2C20 et une interface USB 2.0 contrôlée par un Cypress FX2, développée par l'école polytechnique fédérale de Lausanne (EPFL) à des fins pédagogiques. Cette carte est associée à diverses cartes d'extensions dont une carte RF (émission et réception de signaux jusqu'à 30 MHz) développée par un étudiant radioamateur (HB9EGM), Matthias Brändli. Ces projets, compatibles avec la GNU Radio et dont les sources sont disponibles à [fpga4u], s'inspirent grandement de la plateforme USRP.

F.6 HPSDR

HPSDR (*High Performance Software Defined Radio*) est un projet matériel et logiciel « libre » de récepteur SDR composé d'un CAN 16 bits 135 Méch/s et œuvrant dans le bande [0 - 55 MHz]. Le récepteur peut également fonctionner dans les bandes VHF et UHF. La liaison avec le PC est assurée par une interface USB 2.0 ou Ethernet. Le projet est modulaire et comporte un fond de panier (nom de code : Atlas) sur lequel il est possible d'enficher des cartes pour expérimenter de nouvelles techniques ou dispositifs [hpsdr]. Parmi les différentes cartes en développement citons notamment la carte récepteur Mercury. Cette carte assure un échantillonnage direct dans la bande [0 -65 MHz]. Elle est basée sur un CAN 16bits 130 Méch/s et un FPGA ALTERA Cyclone III assurant la fonction de DDC à au maximum 250 kéch/s. Citons également la carte émetteur Penelope comportant un FPGA ALTERA Cyclone II pour assurer la fonction de DUC. Une autre carte importante de l'HPSDR est la carte Ozymandias (ou " Ozy ") qui assure la connexion USB2 avec le PC. Elle contient le même FPGA Cyclone II ALTERA utilisé dans l'USRP1 et effectue une partie des opérations de traitement numérique du signal. L'ensemble des modules du projet est consultable à [hpsdrwiki].

F.7 KNOWS

Le projet KNOWS (*Kognitiv Networking Over White Spaces*) issu de l'alliance de Microsoft et de Dell [bahl] [yuan], est une radio intelligente détectant et exploitant de façon adaptative les bandes libres TV. L'objectif du système KNOWS est de permettre à des équipements sans fil de s'auto organiser, dans un réseau sans contrôleur central, pour maximiser l'utilisation du spectre disponible. La plateforme KNOWS est principalement composée d'un scanner radio, d'une radio configurable, d'un récepteur GPS (pour la synchronisation temporelle) et d'un processeur x86 embarqué.

F.8 KUAR

La plateforme KUAR (*Kansas University Agile Radio*) est une plateforme expérimentale " *low-cost* " dédiée à la bande de fréquences [5.25 GHz - 5.85 GHz] avec bande passante instantanée de 30 MHz. La plateforme embarque un GPP de 1.4 GHz, un FPGA Xilinx Virtex 2 et des connecteurs Gigabit Ethernet et PCI Express pour la relier à un ordinateur. La majeure partie des traitements est réalisable sur la plateforme, réduisant ainsi les contraintes sur les interfaces. La plateforme fonctionne sur batterie et utilise une version modifiée de la GNU Radio. [kuar]

F.9 MARS

Le système MARS *(Maynooth Adaptable Radio System*), finalisé en 2007, est une SDR où toutes les opérations de traitement du signal sont implémentées sur des processeurs à usage généraux [farrell]. Cette plateforme a pour objectif d'être aussi performante qu'une station de base de téléphonie mobile ou BTS (*Base Transceiver Station*), dans la bande de fréquences [1700 MHz - 2450 MHz], avec un objectif à terme de bande passante instantanée de 70 MHz. Les standards étudiés sont le GSM 1800, le 802.11b, le PCS 1900 et l'UMTS (WCDMA). MARS s'appuie sur l'environnement de développement intégré de radio logicielle IRIS, développé par le *Trinity College* de Dublin et fonctionnant sous Windows et Linux. Un fichier de configuration XML spécifie les composants radio, leurs paramètres et les connexions. Une interface de contrôle autorise un comportement cognitif de la plateforme. La plateforme MARS est composée, pour la partie réception d'un CAN 16 bits 105 Méch/s, d'un LNA 12 dB [0.4 GHz - 2.4 GHz], d'un démodulateur I/Q et d'un OL [500 MHz - 2600 MHz], et pour la partie réception, d'un modulateur I/Q, un amplificateur de puissance (20 dB de gain fixe + 60 dB de gain variable) et d'un CNA 16 bits 200 Méch/s. L'ensemble est relié à un PC hôte via une interface USB 2.0 Cypress EZ-USB avec driver optimisé pour obtenir un débit permanent de 256 Mbit/s. A l'instar de la plupart des SDR, le principal goulet d'étranglement de cette plateforme en termes de performances est la connexion USB avec le PC. La plateforme MARS a notamment été testée avec succès en interopérabilité avec un USRP1[64] en DQPSK à 1 Méch/s dans le cadre de la transmission d'une image. Une transmission de signal vidéo a également été réalisée entre un émetteur et un récepteur MARS (bande passante du signal 300 kHz, 2 Méch/s). Une évolution de l'architecture MARS, MARS2 est en cours de développement. Elle contient un composant Xilinx Spartan 3 mais toujours une interface USB. Le concept MARS3 est également à l'étude et offrira une connexion PCI Express à 4 Gbit/s, un ou plusieurs FPGA Virtex-4, une bande passante instantanée de 25 MHz et des liaisons fibre optique CPRI/OBSAI pour le transfert de données à des cartes RF distantes.

F.10 NICT

Le *Japanese National Institute of Information and Communications Technology* (NICT) a réalisé une plateforme SDR pour tester des réseaux mobiles de dernière génération [harada]. La plateforme dispose de deux processeurs embarqués, quatre FPGA

[64] IRIS dispose d'interfaces logicielles pour les deux plateformes.

Xilinx Virtex2 et des modules RF supportant les bandes de [1.9 GHz - 2.4 GHz] et [5.0 GHz - 5.3 GHz]. L'objectif de cette plateforme est de tester des algorithmes de gestion du *handover* entre équipements implémentant différents standards de radiocommunication (802.11a/b/g, *Digital Terrestrial Broadcasting*, WCDMA, et OFDM).

F.11 SORA

La plateforme de radio logicielle SORA, proposée par Microsoft, est dédiée à la recherche académique non commerciale, et a pour vocation d'implémenter et d'expérimenter des transmissions radiofréquence haut débit de type 802.11 à l'aide de configurations CPU multicœurs et de frontaux RF dédiés [sora]. Une carte de contrôle radio ou RCB (*Radio-Controller Board*) est reliée au PC hôte par des liaisons PCIe et DMA autorisant des débits de 16.7 Gbit/s (si PCIe 8x) et un temps de latence inférieur à la microseconde. Elle peut être connectée à diverses cartes RF fonctionnant dans différentes bandes de fréquences [sora3]. Microsoft ne vend pas mais indique les caractéristiques minimales et le coût estimé du matériel à acquérir pour réaliser cette plateforme : PC avec CPU Intel Core i7-9xx et 3 *slots* PCIe x8 ou PCIe x16 (entre 1 000 $ et 2 000 $), RCB avec Xilinx Virtex-5, interface PCIe x8 et 256 Mo de DDR2 SDRAM (1 500 $), frontal RF de type WARP version 1.4 [warp3] (2 000 $ + adaptateur 85 $) ou carte fille Ettus XCVR2450 (400 $ + adaptateur 800 $ [hrht]). L'architecture logicielle SORA implémente les extensions SIMD (*Single Instruction Multiple Data*) des processeurs récents. Avec ces optimisations, SORA est en mesure de gérer du 802.11b avec un microprocesseur monocœur, et du 802.11a/g avec un double cœur. L'environnement de développement est quant à lui fourni par Microsoft, c'est le Sora SDK [sora2]. La plateforme SORA a fait l'objet dune expérimentation dans le cadre de l'implémentation de protocoles 802.11a/b/g (SoftWifi) et est actuellement à l'étude pour implémenter les protocoles LTE, W-CDMA et WiMAX [sora3]. Son architecture logicielle est consultable à [sora4].

F.12 SDR4ALL

SDR4ALL (*Software Defined Radio For All*), projet de recherche né en 2008 de la collaboration entre le CEA et l'école d'ingénieurs SUPELEC, consiste en la mise en œuvre d'outils pour tester en condition réelle des algorithmes et schémas de transmission radio. Réalisé à partir d'équipements prêts à l'emploi, et utilisant un langage haut niveau pour le traitement du signal, SDR4all est un outil logiciel associé à des cartes radio programmables. [sdr4all]

Une première plateforme a été conçue en 2009 autour d'une solution matérielle proche de l'USRP, et de MATLAB. Le matériel radio comporte deux parties : une carte contrôleur (carte mère) et une ou plusieurs cartes RF (cartes filles) en configuration MIMO ou SISO. La carte mère est responsable du contrôle RF, des communications sur le lien USB et des opérations de décimation et d'interpolation. La carte fille est responsable des conversions analogique/numérique et numérique/analogique et des circuits de conversion RF. La carte mère est composée d'un FPGA Xilinx Spartan-3 (comme celui de l'USRP2) et d'un microcontrôleur Cypress EZ-USB (comme celui de l'USRP1). Une carte fille d'émission/réception propriétaire fonctionnant dans la bande ISM [2.4 GHz – 2.5 GHz] est en cours de finalisation. Cette carte est composée d'un double CAN Analog Devices AD9251 (14 bits, dont seuls 12 sont utilisés, 20 Méch/s), un double CNA Maxim MAX5873 (12 bits, 200 Méch/s), un émetteur/récepteur RF [2.4 GHz – 2.5 GHz] avec ampli de puissance et commutateur R_X/T_X d'antenne Maxim MAX2830, un circuit de distribution d'horloge Analog Devices AD9510 et de la glue logique. Une seule antenne est utilisée pour l'émission et la réception (transmission de type *half-duplex*). En insérant jusqu'à quatre cartes filles, le système est compatible MIMO selon plusieurs configurations (un à trois récepteurs, un à trois émetteurs). La configuration de base ne prévoit toutefois que deux emplacements pour cartes RF, pour un total de quatre voies RF. La bande passante instantanée maximale est de 8 MHz. Chaque carte est configurée via un bus de données partagé, et peut être paramétrée par l'API SDR4all, MATLAB ou une application personnalisée utilisant un *toolkit ad hoc*. L'API C/C++ de SDR4all fournit des bibliothèques pour Windows ou Linux permettant de piloter différentes composantes du système, tels le *firmware* et le FPGA. L'API MATLAB permet de piloter le système sans connaissance approfondie du matériel sous-jacent. Un interfaçage est également à l'étude avec Scilab, logiciel « libre » de calcul numérique multiplateforme ayant la particularité de permettre un fonctionnement multitâche.

Un essai de transmission d'image dans la bande ISM 2,4 GHz en OFDM, réalisé avec une configuration SDR4all/USRP [sdr4all2] a été présenté lors du « *6th Karlsruhe Workshop on Software Radio 2010* » [sdr4all3]. L'ensemble cartes mère et fille devrait être disponible à la vente courant 2011 et obtenir la certification CE grâce notamment à une limitation à 10 mW de la puissance rayonnée. Une réflexion est actuellement menée sur la réalisation de deux éventuelles nouvelles cartes RF, une couvrant la bande [50 MHz - 1 GHz], l'autre couvrant la bande [400 MHz – 4 GHz].

F.13 TeraOps

La LANL TeraOps SDR est une plateforme de radio logicielle conçue par le Laboratoire national de Los Alamos (Nouveau Mexique) pour un usage spatial (c.-à-d. pour être embarqué sur un satellite, une navette spatiale, etc.). Elle délivre 40 milliards d'opérations par watt de puissance consommée, échantillonne à 120 Méch/s sur 16 bits et traite 60 MHz de bande passante instantanée. Le processeur de traitement du signal (RTSP – *Real-Time Signal Processor*) est composé de deux FPGA Xilinx Virtex-4 et sept SRAM de 4 Mo. Le GPP embarqué est un microprocesseur SPARC 32 bits. [teraops]

F.14 WARP

WARP (*Wireless Open Access Research Platform*) est une plateforme de radio logicielle communautaire évolutive, extensible et programmable, à vocation académique et de recherche, développée par l'université RICE de Houston (Texas, États-Unis) [warp] et dédiée au prototypage et à la recherche sur les réseaux sans fil de dernière génération. WARP utilise un FPGA avec CPU intégré pour le traitement numérique du signal, ainsi que plusieurs emplacement pour cartes RF, lui permettant de supporter des communications en MIMO 4x4. WARP fournit également des outils de programmation, bibliothèques et codes en libre accès pour gérer le matériel et développer de nouvelles configurations sans fil. La dernière version (version 2) comporte une carte mère [warp2] composée d'un FPGA Xilinx Virtex-4 XC4VFX100 avec PowerPC intégré, 4 Mo de SDRAM, un lecteur de compact Flash, une liaison "WARP-PC" en Ethernet 10/100 Mbit/s, quatre emplacements pour carte fille, un port RS 232 et un port d'entrée/sortie 16 bits ; et une carte RF [warp3] composée d'un double CNA 16 bits 160Méch/s, un double CAN 14 bits 65Méch/s, un CAN 10 bits 20 Méch/s pour voies d'entrée analogiques auxiliaires, un transmetteur RF gérant les bandes [2400-2500MHz] et [4900-5875MHz], une bande passante instantanée de 20 MHz ou 40 MHz et une compatibilité OFDM, SISO et MIMO.

F.15 WIN2CR

Le projet *Winlab Network Centric Cognitive Radio Platform* (WIN2CR), initié par Winlab [winc2r], un centre de recherche américain spécialisé dans les technologies sans fil, et développé à l'université de Rutgers (New Jersey, États-Unis) a débuté en 2004 et était prévu sur quatre ans. Il consistait à réaliser une radio intelligente dotée d'un frontal radio tri-bande agile détectant et supportant un large éventail de formes d'onde dont l'OFDM et le DSSS/QPSK, pour des débits binaires allant de 10 Mbits/s à 50 Mbits/s. Les objectifs de

cette plateforme étaient multiples : opérations multibande, agilité en fréquence et gestion de divers algorithmes de couche MAC. Un prototype a vu le jour en 2008 et a fait l'objet d'une analyse de performance [satarkar]. Cette plateforme utilisait deux cartes radio: une première contenant deux CAN 14 bits 400 Méch/s, deux CNA 16 bits 500 Méch/s, un FPGA Xilinx Virtex-5 SX95T, 1 Go de DRAM DDR2, 4 Mo de SRAM QDR-II, une interface PCI Express huit voies et un circuit RF gérant les bandes ISM/UNII (2,4 GHz et 5 GHz) ; et une seconde composée d'un FPGA Xilinx Virtex-5 LX50, une interface Gigabit Ethernet, 16 Mo de mémoire Flash, 64 Mo de SDRAM DDR2, et une carte fille composée d'un CAN 12 bits 64 Méch/s, un CNA 12 bits 64 Méch/s et circuit RF gérant les bandes ISM/UNII. La plateforme WiNC2R utilise le code de base de la GNU Radio et fournit les API nécessaires à la programmation des couches PHY et MAC. Le logiciel utilisé pour implémenter des capacités de réseau sans fil adaptatif est basé sur le paquet logiciel CogNet [raychaudhuri].

Bibliographie

[24lc024] *Microchip 2K I2C Serial EEPROM 24LC024*. [en ligne]. Disponible sur : http://www.microchip.com/wwwproducts/Devices.aspx?dDocName=en010808

[24lc02b] *Microchip 2K I2C Serial EEPROM 24LC02b*. [en ligne]. Disponible sur : http://ww1.microchip.com/downloads/en/devicedoc/21709c.pdf

[74ac04] *Fairchild Semiconductor 74AC04 Hex Inverter*. [en ligne]. Disponible sur : http://cva.stanford.edu/classes/cs99s/datasheets/74AC04.pdf

[80211n] *IEEE Standard 802.11n-2009*. [en ligne]. Disponible sur : http://standards.ieee.org/getieee802/download/802.11n-2009.pdf

[856327] *SAWTEK 915 MHz SAW Filter*. [en ligne]. Disponible sur : http://www.triquint.com/docs/f/856327/856327.pdf

A

[abgrall] G. ABGRALL, F. LE ROY, J.P. DELAHAYE, J.P. DIGUET et G. GOGNIAT. *A comparative study of two software defined radio platforms* ». SDR 08 Technical Conference and Product Exposition, 26 au 30 octobre 2008, Washington D.C, [en ligne]. Disponible sur : http://data.memberclicks.com/site/sdf/SDR08-4.2-4.pdf

[ad5623] *Analog Devices Dual 12-/14-/16-Bit nanoDAC® with 5 ppm/°C On-Chip Reference AD5623R/AD5643R/AD5663R*. [en ligne]. Disponible sur : http://www.analog.com/static/imported-files/data_sheets/AD5623R_5643R_5663R.pdf

[ad7922] *Analog Devices 2-Channel, 2.35 V to 5.25 V, 1 MSPS, 10-/12-Bit ADCs AD7912/AD7922*. [en ligne]. Disponible sur : http://www.analog.com/static/imported-files/data_sheets/AD7912_7922.pdf

[ad8132] *Analog Devices AD8132. Low cost, high speed Differential Amplifier*. [en ligne]. Disponible sur : http://www.analog.com/static/imported-files/data_sheets/AD8132.pdf

[ad8347] *Analog Devices AD8349. 0.8 GHz to 2.7 GHz Direct Conversion Quadrature Demodulator*, [en ligne]. Disponible sur : http://www.analog.com/static/imported-files/data_sheets/AD8347.pdf

[ad8349] *Analog Devices AD8349. 700 MHz to 2700 MHz Quadrature modulator*, [en ligne]. Disponible sur : http://www.analog.com/static/imported-files/data_sheets/AD8349.pdf

[ada4937] *Analog Devices ADA4937-2, Ultralow Distortion Differential ADC Driver (Dual)*, [en ligne]. Disponible sur : http://www.analog.com/static/imported-files/data_sheets/ADA4937-1_4937-2.pdf

[adl5386] *Analog Devices ADL5386, 50 MHz to 2200 MHz Quadrature Modulator with Integrated Detector and VVA*, [en ligne]. Disponible sur : http://www.analog.com/static/imported-files/data_sheets/ADL5386.pdf

[adl5387] *Analog Devices ADL5387, 50 MHz to 2 GHz Quadrature demodulator*, [en ligne]. Disponible sur : http://www.analog.com/static/imported-files/data_sheets/ADL5387.pdf

[adp336] *Analog Devices ADP3336 High Accuracy Ultralow IQ, 500 mA anyCAP® Adjustable Low Dropout Regulator*, [en ligne]. Disponible sur : http://www.analog.com/static/imported-files/data_sheets/ADP3336.pdf

[ad9510] *Analog Devices 1.2 GHz Clock Distribution IC, PLL Core, Dividers, Delay Adjust, Eight Outputs AD9510*, [en ligne]. Disponible sur : http://www.analog.com/static/imported-files/data_sheets/AD9510.pdf

[ad9513] *800 MHz Clock Distribution IC, Dividers, Delay Adjust, Three Outputs Analog Devices AD9513*, [en ligne]. Disponible sur : http://www.analog.com/static/imported-files/data_sheets/AD9513.pdf

[ad9777] *Analog Devices AD9777 16-Bit, 160 MSPS 2x/4x/8x Interpolating Dual TxDAC+® D/A Converter*, [en ligne]. Disponible sur : http://www.analog.com/static/imported-files/data_sheets/AD9777.pdf

[adf4350] *Analog Devices ADF4350, Wideband Synthesizer with Integrated VCO*, [en ligne]. Disponible sur : http://www.analog.com/static/imported-files/data_sheets/ADF4350.pdf

[adf4360] *Analog Devices ADF4360-3. Integrated Synthesizer and VCO*, [en ligne]. Disponible sur : http://www.analog.com/static/imported-files/data_sheets/ADF4360-3.pdf

[adg3301] *Analog Devices Low Voltage 1.15 V to 5.5 V, Single-Channel Bidirectional Logic Level Translator ADG3301*, [en ligne]. Disponible sur : http://www.analog.com/static/imported-files/data_sheets/ADG3301.pdf

[adroit] *Adroit GNU Radio development*, [en ligne]. Disponible sur : http://acert.ir.bbn.com/projects/adroitgrdevel.

[agullo] J.R. GUTIERREZ-AGULLO, B. COLL-PERALES et J. GOZALVEZ. *An IEEE 802.11 MAC Software Defined Radio Implementation for Experimental Wireless Communications and Networking Research*. IFIP/IEEE Wireless Days 2010 (WD'10). 21 octobre 2010. Venise (Italie), [en ligne]. Disponible sur : http://www.uwicore.umh.es/publications-all.html

[airprobe] *Welcome to AirProbe*, [en ligne]. Disponible sur : https://svn.berlin.ccc.de/projects/airprobe/

[airprobecode] Airprobe source code, [en ligne]. Disponible sur : https://svn.berlin.ccc.de/projects/airprobe/browser

[airprobeht] *A beginners howto*, [en ligne]. Disponible sur : https://svn.berlin.ccc.de/projects/airprobe/wiki/A

[airprobeht2] *Airprobe How-To*, [en ligne]. Disponible sur : http://srlabs.de/uncategorized/airprobe-how-to/

[akapyev] A. AKAPYEV, V. KRYLOV. *Implementation of 802.11n on 128-core processor*. [en ligne]. Disponible sur : http://www.meralabs.com/media/meralabs/publications/files/Implementation_of_802.11n_on_128-core_processor.pdf

[akm] AKM Semiconductor. *ADC AK5394*. [en ligne]. Disponible sur : http://www.akm.com/prodfolder-adc.asp?p=AK5394A

[altera] Altera Inc. *DSP Builder/Simulink*. 2010. [en ligne]. Disponible sur : http://www.altera.com/technology/dsp/dsp-builder/dsp-simulink.html

[amd] *ATI Stream Software Development Kit (SDK) v2.2*, [en ligne]. Disponible sur : http://developer.amd.com/gpu/ATIStreamSDK/pages/Documentation.aspx

[an231] *Anadigm AN231E04 datasheet Rev 1.1 Dynamically Reconfigurable dpASP*, [en ligne]. Disponible sur : http://www.anadigm.com/_doc/DS231000-U001.pdf

[api] S. HYUN, J. KIM, S. CHOI, L. PUCKER et B. FETTE. *Standardizing smart antenna API for SDR networks*. RF Design, septembre 2007, [en ligne]. Disponible sur : http://dsplab.hanyang.ac.kr/sa_api/Standardizing_smart_antenna_API_for_SDR_networks.pdf

[arcepnfc] Autorité de régulation des communications électroniques et des postes. *Étude relative à l'émergence des services mobiles sans contact et leur impact potentiel sur le marché des télécommunications mobiles*. 22 février 2010, [en ligne]. Disponible sur : http://www.arcep.fr/uploads/tx_gspublication/etude-serv-mobiles-sans-contact-220210.pdf

[as37] *AS37 : Action Spécifique 37 Radio Logicielle*, [en ligne]. Disponible sur : http://www-labsticc.univ-ubs.fr/~boutillon/AS_Radio_Logicielle/ArchiPalicot.pdf

[asmi] *Active Serial Memory Interface*. ALTERA. Mai 2003, version 1.2, [en ligne]. Disponible sur : http://www.altera.com.cn/literature/ds/ds_nios_asmi.pdf

[atmel] *AT91SAM ARM-based MCUs and eMPUs*, [en ligne]. Disponible sur : http://www.atmel.com/products/AT91

B

[bahl] P. BAHL, R. CHANDRA, T. MOSCIBRODA, R. MURTY, et M. WELSH. *White space networking with Wi-Fi like connectivity*. SIGCOMM '09, New York, États-Unis 2009, pp. 27–38, [en ligne]. Disponible sur : www.eecs.harvard.edu/~mdw/papers/whitefi-sigcomm09.pdf

[balister] P. J. BALISTER, M. ROBERT, J. REED. *Impact of the use of CORBA for Inter-Component Communication in SCA Based Radio*. SDR Forum Technical Conference, Orlando, novembre 2006, [en ligne]. Disponible sur : http://data.memberclicks.com/site/sdf/sdr06-1.1-4.pdf

[barrandon] L. BARRANDON. *Synthèse architecturale analogique/numérique appliquée aux systèmes sur puce dans un contexte de radio logicielle*. Thèse de doctorat soutenue le 8 décembre 2005, [en ligne]. Disponible sur : http://hal.archives-ouvertes.fr/docs/00/06/50/84/PDF/these.pdf

[baudline] *Baudline*, [en ligne]. Disponible sur : http://www.baudline.com/what_is_baudline.html

[bee2] *Berkeley Emulation Engine 2*, [en ligne]. Disponible sur : http://bee2.eecs.berkeley.edu/

[bwrc] *Berkeley wireless research center – Prototyping platform*, [en ligne]. Disponible sur : http://bwrc.eecs.berkeley.edu/Research/Cognitive/prototyping_platform.htm

[blackfin] *Analog Devices Blackfin Embedded Symmetric Multiprocessor ADSP-BF561*, [en ligne]. Disponible sur : http://www.analog.com/static/imported-files/data_sheets/ADSP-BF561.pdf

[buettner] M. BUETTNER, D. WETHERALL. *A "Gen 2" RFID Monitor Based on the USRP*. [en ligne]. Disponible sur : http://www.cs.washington.edu/homes/buettner/docs/p42-2v40n3k-buettnerA.pdf

[burx] *BitShark USRP RX (BURX) Broadband configurable RF Receiver*, [en ligne]. Disponible sur : http://www.epiq-solutions.com/product_detail.php?line=BitShark&products=BitShark USRP

[businesswire] *The wireless Innovation Forum Announces Annual Award Finalists*, [en ligne]. Disponible sur : http://www.businesswire.com/news/home/20101118007162/en

C

[calradio] *Calit2 Wireless Communications Research and Development Platforms*, [en ligne]. Disponible sur : http://calradio.calit2.net/

[cgran] *The Comprehensive GNU Radio Archive Network (CGRAN)*, [en ligne]. Disponible sur : https://www.cgran.org/

[chang] C. CHANG, J. WAWRZYNEK, et R. BRODERSEN. *BEE2: a high-end reconfigurable computing system*. IEEE Design & Test of Computers, IEEE, vol. 22, no. 2, pp. 114–125, mars-avril 2005, [en ligne]. Disponible sur : http://www.pdfchaser.com/BEE2%3A-A-High-End-Reconfigurable-Computing-System.html

[choong] L. CHOONG. *Multi-Channel IEEE 802.15.4 Packet Capture Using Software Defined Radio*. UCLA Networked & Embedded Sensing Lab. University of California, Los Angeles. Mars 2009, [en ligne]. Disponible sur : http://nesl.ee.ucla.edu/fw/thomas/leslie_choong_multichannel_ieee802154.pdf

[cisco] P. ROSHAN et J. LEARY. *802.11 Wireless LAN Fundamentals*. Cisco Press, 2003, [en ligne]. Disponible sur : http://docstore.mik.ua/cisco/pdf/other/Cisco%20Press,%20802.11%20Wireless%20Lan%20Fundamentals%20%282003%29%20Kb.pdf

[cml] *CMX994 RF Direct Conversion Receiver*, [en ligne]. Disponible sur : http://www.cmlmicro.com/products/index.asp?/Products/RF/CMX994.htm&searchvalue=994&setindex=1

[corgan] *Re: [discuss-gnuradio] Logic utilization of standard USRP2 configuration*. Johnatan Corgan. 21 avril 2009, [en ligne]. Disponible sur : http://www.mail-archive.com/discuss-gnuradio@gnu.org/msg18863.html

[cpld9572] *Xilinx XC9572XL High Performance CPLD*, [en ligne]. Disponible sur : http://www.xilinx.com/support/documentation/data_sheets/ds057.pdf

[cpri] Ericsson AB, Huawei Technologies Co. Ltd, NEC Corporation, Nortel Networks Ltd, Alcatel Lucent, et Nokia Siemens Networks GmbH & Co. KG. *CPRI Specification v4.1*. 2009, [en ligne]. Disponible sur : http://www.cpri.info/downloads/CPRI_v_4_1_2009-02-18.pdf

[crystek] *CVHD-950 VXCO Ultra-low phase noise oscillators*, [en ligne]. Disponible sur : http://www.crystekcrystals.com/crystal/vcxo/vcxo-complete.asp

[csar] General Dynamics. *AN/PRC-112G® CSAR Transceiver*. 2010, [en ligne]. Disponible sur : http://www.gdc4s.com/documents/D-112G-04-0910w.pdf

[cuda] *CUDA toolkit 3.2 RC (September 2010)*, [en ligne]. Disponible sur : http://developer.nvidia.com/object/cuda_3_2_toolkit_rc.html

[cyclone] *Altera Cyclone FPGA Family Data Sheet*, [en ligne]. Disponible sur : http://www.altera.com/literature/hb/cyc/cyc_c5v1_01.pdf

[cyclone3a] *Altera Cyclone III low-cost FPGAs*, [en ligne]. Disponible sur : http://media.digikey.com/pdf/Data%20Sheets/Altera%20PDFs/CycloneIII_Brochure.pdf

[cyclone3b] *Altera Cyclone III products specs*, [en ligne]. Disponible sur : http://www.altera.com/literature/hb/cyc3/cyclone3_handbook.pdf

[cy7c] *Cypress CY7C1354C, CY7C1356C 9-Mbit (256 K × 36/512 K × 18) Pipelined SRAM with NoBL™ Architecture*, [en ligne]. Disponible sur : http://www.cypress.com/?docID=24341

[cypress] *EZ-USB FX2 USB Microcontroller High-Speed USB Peripheral Controller*, [en ligne]. Disponible sur : http://www.keil.com/dd/docs/datashts/cypress/cy7c68xxx_ds.pdf

D

[dboards] *UHD – Daughterboard Application Notes*, [en ligne]. Disponible sur : http://www.ettus.com/uhd_docs/manual/html/dboards.html.

[dect1] European Telecommunication Standard Institute: ETSI EN 300 175-1 V2.3.1 (2010-06): *Digital Enhanced Cordless Telecommunications (DECT); Common Interface (CI); Part 1: Overview.*

Remarque : [dect1] à [dect6] sont en ligne et disponibles à : http://portal.etsi.org/Portal_Pub/APNProcPub.asp?ACTION_TYPE_NB=PU&FROM_DD=14&FROM_MM=Jun&FROM_YYYY=2010&TO_DD=20&TO_MM=Jun&TO_YYYY=2010&REAL_FROM_DD=14&REAL_FROM_MM=Jun&REAL_FROM_YYYY=2010&REAL_TO_DD=20&REAL_TO_MM=Jun&REAL_TO_YYYY=2010

[dect2] European Telecommunication Standard Institute: ETSI EN 300 175-2 V2.3.1 (2010-06): *Digital Enhanced Cordless Telecommunications (DECT); Common Interface (CI); Part 2: Physical Layer (PHL).*

[dect3] European Telecommunication Standard Institute: ETSI EN 300 175-2 V2.3.1 (2010-06): *Digital Enhanced Cordless Telecommunications (DECT); Common Interface (CI); Part 3: Medium Access Control (MAC) layer*.

[dect5] European Telecommunication Standard Institute: ETSI EN 300 175-2 V2.3.1 (2010-06): *Digital Enhanced Cordless Telecommunications (DECT); Common Interface (CI); Part 5: Network (NWK) layer.*

[dect6] European Telecommunication Standard Institute: ETSI EN 300 175-2 V2.3.1 (2010-06): *Digital Enhanced Cordless Telecommunications (DECT); Common Interface (CI); Part 6: Identities and addressing.*

[dectforum] DECT Forum. *The Standard explained*. février 1997, [en ligne]. Disponible sur : htttp://www.dectweb/DECTForum/publicdocs/TechnicalDocument.PDF

[desimone] M. DESIMONE. *Software-Defined Radio - An Overview and Tutorial*. 9 mai 2009, [en ligne]. Disponible sur : https://hostdb.ece.utexas.edu/~wireless/ee381K_spring09/reports/desimone.pdf

[discuss1] *On turning the RFX900 to an RFX1800 and back again*, [en ligne]. Disponible sur : http://lists.gnu.org/archive/html/discuss-gnuradio/2006-09/msg00179.html

[discuss2] *Truth about this work*, [en ligne]. Disponible sur : http://lists.lists.reflextor.com/pipermail/a51/2010-January/000424.html

[dm780] *Digital Master 780*, [en ligne]. Disponible sur : http://www.ham-radio-deluxe.com/Programs/DigitalMaster780.aspx

[doxygen] *GNU Radio 3.2svn C++ API Documentation*, [en ligne]. Disponible sur : http://gnuradio.org/doc/doxygen/index.html

[dp83865] *National Semiconductor DP83865 Gig PHYTER® V 10/100/1000 Ethernet Physical Layer*, [en ligne]. Disponible sur : http://www.national.com/ds/DP/DP83865.pdf

[ds90cp] *National Semiconductor DS90CP22 800 Mbps 2x2 LVDS Crosspoint Switch*, [en ligne]. Disponible sur : http://www.national.com/ds/DS/DS90CP22.pdf

[ds90lt] *DS90LT012AH High Temperature 3V LVDS Differential Line Receiver*, [en ligne]. Disponible sur : http://www.national.com/ds/DS/DS90LT012AH.pdf

E

[edom] L. DER. *An evolution of FM Tuner Architectures*. EDOM Technology Co., Ltd, [en ligne]. Disponible sur : http://www.edom.com.tw/en/index.jsp?lang=en&m=techview&cal=9&id=1383

[ellingson] S.W. ELLINGSON. *A low Cost All-Band All-Mode Radio for Public Safety*. Final Report, 30.12.2008, [en ligne]. Disponible sur : http://www.ece.vt.edu/swe/chamrad/crdocs/CRTM33_Final_Report.pdf

[ep1c12] *Altera Section I. Cyclone FPGA Family Data Sheet*, [en ligne]. Disponible sur : http://www.altera.com/literature/ds/ds_cyc.pdf

[ettus] *Ettus Research LLC*, [en ligne]. Disponible sur : http://www.ettus.com/

[ettus1] Ettus Research LLC. *USRP Family Brochure*. 2010. [en ligne]. Disponible sur : http://www.ettus.com/downloads/ettus_broch_trifold_v7b.pdf

[ettus2] Ettus Research LLC. *TX and RX Daughterboards*. 2010. [en ligne]. Disponible sur : http://www.ettus.com/downloads/ettus_ds_USRP_TXRX_v5b.pdf

[ettus3] Ettus Research LLC. *Transceiver Daughterboards*. 2010. [en ligne]. Disponible sur : http://www.ettus.com/downloads/ettus_ds_transceiver_dbrds_v6c.pdf

F

[f4dan] *F4DAN Software Defined Radio*, [en ligne]. Disponible sur : http://f4dan.free.fr/sdr.html

[farrell] R. FARRELL, M. SANCHEZ ET G. CORLEY. *Software-Defined Radio Demonstrators: An Example and Future Trends*. 30 septembre 2008. [en ligne]. Disponible sur : http://www.hindawi.com/journals/ijdmb/2009/547650.html

[fette] B. FETTE. *Cognitive Radio Technology (Communications Engineering)*. Éditions Newnes, 656 pages, ISBN-10: 0750679522, ISBN-13: 978-0750679527.

[firas] FIRAS ABBAS HAMZA. *The USRP under 1.5X Magnifying Lens!* Révision 1.0. 12 juin 2008. [en ligne]. Disponible sur : http://www.gnuradio.org/redmine/attachments/129

[firooz] H. FIROOZ. *Implementation of Full-Bandwidth 802.11b Receiver*. University of UTAH, [en ligne]. Disponible sur : http://span.ece.utah.edu/pmwiki/pmwiki.php?n=Main.80211bReceiver

[fitzsimons] R. FITZSIMONS. *Find a GSM base station manually using a USRP*. Janvier 2008. [en ligne]. Disponible sur : http://273k.net/gsm/find-a-gsm-base-station-manually-using-a-usrp/

[flexradio] *FlexRadio Systems Product Comparison Matrix*, [en ligne]. Disponible sur : http://www.flex-radio.com/Products.aspx?topic=SDR_Feature_Matrix

[fpga4u] *USB-powered FPGA-based development board*. School of Computer and Communication Sciences of EPF. [en ligne]. Disponible sur : http://fpga4u.epfl.ch/wiki/Main_Page

G

[gap] European Telecommunication Standard Institute: ETSI EN 300 444 V2.1.1 (2008-10): *Digital Enhanced Cordless Telecommunications (DECT); Generic Access Profile (GAP)*, [en ligne]. Disponible sur : http://www.etsi.org/deliver/etsi_en/300400_300499/300444/02.01.01_60/en_300444v020101p.pdf

[geda] *gEDA project's homepage*, [en ligne]. Disponible sur : http://www.gpleda.org/index.html

[gmskcr] Ruby Forum. *Forum: GNU Radio - GMSK and Carrier Recovery*, [en ligne]. Disponible sur : http://www.ruby-forum.com/topic/95894

[gnugen2] The comprehensive GNU Radio Archive Network. *Gen 2 RFID Tools*, [en ligne]. Disponible sur : http://www.cgran.org/wiki/Gen2

[gnuradio1] *GNU Radio*, [en ligne]. Disponible sur : http://gnuradio.org/redmine/wiki/gnuradio

[gnuradio2] *Exploring GNU Radio*, [en ligne]. Disponible sur : http://www.gnu.org/software/gnuradio/doc/exploring-gnuradio.html

[gnuradio3] *How to Write a Signal Processing Block*, [en ligne]. Disponible sur : http://www.gnu.org/software/gnuradio/doc/howto-write-a-block.html

[gnuradio4] *Guide d'installation GNU Radio*, [en ligne]. Disponible sur : http://gnuradio.org/trac/wiki/BuildGuidehttp://gnuradio.org/redmine/wiki/gnuradio/BuildGuide

[gnuradio5] *GNU Radio – the open-source software radio*, [en ligne]. Disponible sur : http://gnuradio.squarespace.com

[godard] L. GODARD. *Modèle de Gestion Hiérarchique Distribuée pour la Reconfiguration et la Prise de Décision dans les équipements de Radio Cognitive*. Thèse de doctorat. 18 décembre 2008, [en ligne]. Disponible sur : http://tel.archives-ouvertes.fr/docs/00/35/53/52/PDF/these_loig_finale.pdf

[gpu] J. KIM, S. HYEON ET S. CHOI. *Implementation of an SDR System Using Graphic Processing Unit*. [en ligne]. Disponible sur : http://staffweb.cms.gre.ac.uk/~gm73/com-mag/COMG_20100301_Mar_2010.PDF

[grc] *GNU Radio Companion*, [en ligne]. Disponible sur : http://gnuradio.org/redmine/wiki/1/GNURadioCompanion

[grc2] J. BLUM. Tutorial "The Gnuradio Companion (GRC) ". 5 octobre 2009. [en ligne]. Disponible sur : http://www.joshknows.com/download/grc_old/grc_gnuradio_hackfest_2009_09_06.pdf

[grdect] *GR_DECT – DECT Receiver*, [en ligne]. Disponible sur : https://www.cgran.org/wiki/GR_DECT

[gsma] *Market Data Summary (Q2 2009)*. GSM Association, [en ligne]. Disponible sur : http://gsmworld.com/newsroom/market-data/market_data_summary.htm

[gumstix] *Gumstix packs*, [en ligne]. Disponible sur : http://www.gumstix.com/store/catalog/packs.php

H

[hamlib] *Ham Radio Control Libraries*, [en ligne]. Disponible sur : http://sourceforge.net/apps/mediawiki/hamlib/index.php?title=Main_Page

[hamlibsr] *Hamlib supported radios*, [en ligne]. Disponible sur : http://sourceforge.net/apps/mediawiki/hamlib/index.php?title=Supported_Radios

[harada] H. HARADA. *Software defined radio prototype for multi-mode and multi-service radio communication systems*. National Institute of Information and Communications Technology (NICT). [en ligne]. Disponible sur : http://www.sdrforum.org/pages/sdr05/4.6%20Special%20Applications%202/4.6-04%20Harada.pdf

[harrison] G. HARRISON, A. SLOAN, W. MYRICK, J. HECKER et D. EASTIN. *Polyphase channelization utilizing general-purpose computing on a GPU*. [en ligne]. Disponible sur : http://www.sdrforum.org/sdr08_papers/5.3/5.3-5.pdf

[heron] *Hunt Engineering HERON RTG003*, [en ligne]. Disponible sur : http://www.hunt-rtg.com/readytogo/rtg003.htm

[hmc174ms8] *Hittite HMC174MS8 GaAs MMIC T/R switch DC – 3GHz*, [en ligne]. Disponible sur : http://www.hittite.com/content/documents/data_sheet/hmc174ms8.pdf.

[hmc472lp4] *0.5dB LSB 6-Bit Digital Attenuator SMT, DC - 3.8 GHz*, [en ligne]. Disponible sur : http://www.hittite.com/products/view.html/view/HMC472LP4

[hpsdr] *High Performance Software Defined Radio*, [en ligne]. Disponible sur : http://openhpsdr.org/

[hpsdrwiki] *HPSDR Wiki: Community Portal*, [en ligne]. Disponible sur : http://openhpsdr.org/wiki/index.php?title=HPSDRwiki:Community_Portal

[hrd] *Ham Radio Deluxe*, [en ligne]. Disponible sur : http://www.ham-radio-deluxe.com

[hrdv5] *HRD v5 Beta*, [en ligne]. Disponible sur : http://www.ww2pt.com/2009/08/hrd-v5-beta.html

[hrht] *Software Sora Digital Foundation Data Transfer Card HR-SRMB-M01*, [en ligne]. Disponible sur : http://www.hrht-hpc.com/en/product_read.asp?id=105

[hydra] K. MANDKE, R. C. DANIELS, R. W. HELATH JR et S. M. NETTLES. *On the challenge of building a multi-antenna software defined packet radio*. Wireless Networking & Communications Group (WNCG). Department of Electrical & Computer Engineering. University of Texas (Austin). 2008, [en ligne]. Disponible sur : http://netlab.ece.utexas.edu/hydra/docs/sdr2008.pdf

I

[ingemarsson] C. INGEMARSSON. *Hardware evaluation platform based on GNU Radio and the USRP*. Department of Electrical Engineering. Université de Linköpings. 21 mai 2009, [en ligne]. Disponible sur : http://liu.diva-portal.org/smash/record.jsf?pid=diva2:218764

[ism] Wikipédia. *Bande industrielle, scientifique et médicale*. [en ligne]. Disponible sur : http://fr.wikipedia.org/wiki/Bandes_ISM

J

[johnston] *(USRP-users) Interface to the expansion port, and connect the USRP2 to a Virtex 5*, [en ligne]. Disponible sur : http://lists.ettus.com/pipermail/usrp-users_lists.ettus.com/2010-December/000213.html

[jpeojtrs] *Joint tactical radio system*. 2010, [en ligne]. Disponible sur : http://www.public.navy.mil/jpeojtrs/Pages/Welcome.aspx

[jtrs] U. S. Government Accountability Office. *Restructured JTRS Program Reduces Risk, but Significant Challenges Remain*. 2006, [en ligne]. Disponible sur : http://www.gao.gov/cgi-bin/getrpt?GAO-06-955

[jtrs2] Boeing, Inc. *Joint Tactical Radio System, Ground Mobile Radios (JTRS GMR)*. 2010, [en ligne]. Disponible sur : http://www.boeing.com/defense-space/ic/jtrs/docs/JTRS_GMR_overview.pdf

[jtrs3] Global Security. *Joint Tactical Radio System - Programmable, Modular Communications System*. 2010, [en ligne]. Disponible sur : http://www.globalsecurity.org/military/systems/ground/jtrs.htm

K

[kenington] P. B. KENINGTON. *RF and Baseband Techniques for Software Defined Radio*. Éditions Artech House, 2005, 340 pages. ISBN: 1580537936.

[khronos1] *OpenCL – The open standard for parallel programming of heterogeneous systems*, [en ligne]. Disponible sur : http://www.khronos.org/opencl

[khronos2] *OpenCL Introduction an Overview*. Juin 2010, [en ligne]. Disponible sur : http://www.khronos.org/developers/library/overview/opencl_overview.pdf

[kit] *Simulink-USRP: Universal Software Radio Peripheral (USRP) Blockset*, [en ligne]. Disponible sur : http://www.cel.kit.edu/downloads.php

[knauth] *Implementation of an IEEE 802.15.4 Transceiver with a Software-defined Radio setup*. Embedded World 2008 (26. - 28. February 2008, Nürnberg, Deutschland), [en ligne]. Disponible sur : http://www.ceesar.ch/fileadmin/Dateien/PDF/NewsEvents/emw2008_paper_Knauth.pdf

[kuar] G. J. MINDEN, J. B. EVANS, L. SEARL, D. DEPARDO, V. R. PETTY, R. RAJBANSHI, T. NEWMAN, Q. CHEN, F. WEIDLING, J. GUFFEY, D. DATLA, B. BARKER, M. PECK, B. CORDILL, A. M. WYGLINSKI et A. AGAH. *KUAR : A Flexible Software-Defined Radio Development*. Platform Information Technology and Telecommunications Center, The University of Kansas. [en ligne]. Disponible sur : http://www.ittc.ku.edu/publications/documents/minden2007_dyspan07.pdf

[kushal] K. Y. SHAH. *Computational complexity of signal processing functions in software radio*. Bachelor of Engineering in Electronics and Communication. Gujarat University. Master of Science in electrical engineering. Université d'État de Cleveland. Décembre 2010, [en ligne]. Disponible sur : http://etd.ohiolink.edu/send-pdf.cgi/Shah%20Kushal%20Yogeshkumar.pdf?csu1292854939

L

[labview] *Qu'est-ce que LabVIEW ?*, [en ligne]. Disponible sur : http://www.ni.com/labview/whatis/f/

[lee] V.W LEE, C. KIM, J. CHHUGANI, M. DEISHER, D. KIM, A.D NGUYEN, N. SATISH, M. SMELYANSKIY, S. CHENNUPATY, P. HAMMARLUND, R. SINGHAL ET P. DUPEY. *Debunking the 100X GPU vs. CPU Myth : An evaluation of Throughput Computing on CPU and GPU*. Intel Corporation. Juin 2010, [en ligne]. Disponible sur : http://www.cpe.virginia.edu/pdf/Debunking.pdf

[linrad] *Linrad home page*, [en ligne]. Disponible sur : http://www.nitehawk.com/sm5bsz/linuxdsp/linrad.htm

[lm2940] *National Semiconductor LM2940/LM2940C 1A Low Dropout Regulator*, [en ligne]. Disponible sur : http://www.national.com/ds/LM/LM2940.pdf.

[lp38692] *National Semiconductor 1A Low Dropout CMOS Linear Regulators Stable with Ceramic Output Capacitors* [en ligne]. Disponible sur : http://www.national.com/ds/LP/LP38690.pdf

[lt1085] *Linear Technology LT1085-Fixed - 3A, 5A, 7.5A Low Dropout Positive Fixed Regulators*, [en ligne]. Disponible sur : http://www.linear.com/pc/productDetail.jsp?navId=H0,C1,C1003,C1040,C1055,P1280

[ltc2284] *LTC2284 - Dual 14-Bit, 105Msps Low Power 3V ADC*, [en ligne]. Disponible sur : http://www.linear.com/pc/productDetail.jsp?navId=H0,C1,C1155,C1001,C1150,P15833

[lt3510] *Linear Technology LT 3510 Monolithic Dual Tracking 2A Step-Down Switching Regulator*, [en ligne]. Disponible sur : http://cds.linear.com/docs/Datasheet/3510fd.pdf

[ltc6908] *LTC6908 - Dual Output Oscillator with Spread Spectrum Modulation*, [en ligne]. Disponible sur : http://www.linear.com/pc/productDetail.jsp?navId=H0,C1,C1010,C1096,P20292

[lyrtech] *Lyrtech Small Form Factor development platforms*, [en ligne]. Disponible sur : http://www.lyrtech.com/Products/SFF_SDR_development_platforms.php

M

[mari] M. DE MARI. Évaluation des dispositifs de Software Defined Radio. Rapport de stage de 2ième année au sein de la Chaire de radio flexible (SUPELEC), été 2010.

[massiani] A. MASSIANI. *Prototypage de Systèmes Haut Débit combinant étalement de spectre, multi-porteuses et multi-antennes*. Thèse de doctorat, 25 novembre 2005, Institut national des sciences appliquées de Rennes, [en ligne]. Disponible sur : http://tel.archives-ouvertes.fr/docs/00/05/70/76/PDF/these_finale_Plan.pdf

[mathworks] Mathworks. *Recorded Webinar: Developing Software Defined Radio Systems Using MATLAB and Simulink*. 16 mars 2006, [en ligne]. Disponible sur : http://www.mathworks.com/company/events/webinars/wbnr30307.html

[mathworks2] *Version 5.0 (R2010b) Communications Blockset Software*, [en ligne]. Disponible sur : http://www.mathworks.com/help/toolbox/commblks/rn/bsjl8d4.html#bsjrdu7

[max2112] *Maxim complete, Direct-Conversion Tuner for DVB-S2 Applications*, [en ligne]. Disponible sur : http://datasheets.maxim-ic.com/en/ds/MAX2112.pdf

[max6749] *Maxim µP Reset Circuits with Capacitor-Adjustable Reset/Watchdog Timeout Delay*, [en ligne]. Disponible sur : http://datasheets.maxim-ic.com/en/ds/MAX6746-MAX6753.pdf

[maxentric] *Maxentric Calradio*, [en ligne]. Disponible sur : http://www.maxentric.com/MaxentricSite/CalRadio.html

[mellers] S. MELLERS, B. RICHARDS, H. H. SO, S. MISHRA, K. CAMERA, P. SUBRAHMANYAM et R. BRODERSEN. *Radio testbeds using BEE2*. Signals, Systems and Computers, 2007, [en ligne]. Disponible sur : http://www.eee.hku.hk/~hso/Publications/RadioTestbedsBEE2-v10-br.pdf

[mga62563] *Avago MGA-62563 Current-Adjustable, Low Noise Amplifier*, [en ligne]. Disponible sur : http://www.avagotech.com/pages/en/rf_ics_discretes/rf_ics/gaas_amplifiers_mixers_switches/mga-62563/.

[mga82563] *Avago MGA-82563 0.1– 6 GHz 3 V, 17 dBm Amplifier*, [en ligne]. Disponible sur : http://www.avagotech.com/docs/AV02-1985EN

[mishra] S. MISHRA, D. CABRIC, C. CHANG, D. WILLKOMM, B. VAN SCHEWICK, S. WOLISZ et B. BRODERSEN. *A real time cognitive radio testbed for physical and link layer experiments*. IEEE International Symposium Dynamic Spectrum Access Networks (DySPAN), novembre 2005, [en ligne]. Disponible sur : http://www.tkn.tu-berlin.de/publications/papers/dyspan05_cr-testbed2.pdf

[mitola] J.MITOLA. *Software Radio Architecture: Object-Oriented Approaches to Wireless Systems Engineering*. Editions Wiley, 2000. 543 pages. ISBN 0471384925.

[mitola2] J. MITOLA. *Cognitive Radio: An Integrated Agent Architecture for Software Defined Radio*. Ph.D. dissertation, Royal Institute of Technology (KTH), Sweden, 2000, [en ligne]. Disponible sur : http://web.it.kth.se/~maguire/jmitola/Mitola_Dissertation8_Integrated.pdf

[mitola3] J. MITOLA. *Software Radios: Survey, Critical Evaluation and future directions*. IEEE National Telesystems Conference. Mai 1992.

[mobicom10] J. IL CHOI, M. JAIN, K. SRINIVASAN, P. LEVIS et S. KATTI. *Achieving single channel, full duplex wireless communication*. MOBICOM 2010, Chicago, Illinois, États-Unis. 20 au 24 septembre 2010, [en ligne]. Disponible sur : http://sing.stanford.edu/pubs/mobicom10-duplex.pdf

[msg14933] *Re: [Discuss-gnuradio] Problem with rx_voice.py*, [en ligne]. Disponible sur : http://www.mail-archive.com/discuss-gnuradio@gnu.org/msg14933.html.

[mt4937] *Microtune 4937 DI15 RF Tuner Module*, [en ligne]. Disponible sur : http://comsec.com/usrp/microtune/4937-DI5-3x8899-2.pdf

[mueller] K.H MUELLER et M. MÜLLER. *Timing recovery in digital synchronous data receivers*. IEEE Transactions on Communications, vol.24, pages 516 à 531, mai 1976.

[µblaze] *MicroBlaze Soft Processor Core*, [en ligne]. Disponible sur : http://www.xilinx.com/tools/microblaze.htm

[µwsdr] *µWSDR Project*, [en ligne]. Disponible sur : http://uwsdr.berlios.de/

N

[nasa] J.C. BRIONES, L.M. HANDLER, S.C. HALL, R.C. REINHART et T.J. KACPURA. *Case Study: Using the OMG SWRADIO Profile and SDR Forum Input for NASA's Space Telecommunications Radio System*. Janvier 2009, [en ligne]. Disponible sur : http://gltrs.grc.nasa.gov/reports/2009/TM-2009-215478.pdf

[ni1] National Instruments. *Logiciels pour les RF et les communications*, [en ligne]. Disponible sur : http://www.ni.com/rf/f/software.htm

[ni2] National Instruments. *Voir au-delà de l'instrument autonome : une approche du test RF définie par logiciel*, [en ligne]. Disponible sur : http://zone.ni.com/devzone/cda/pub/p/id/943

[ni3] National Instruments. *Plate-forme logicielle pour systèmes de communication présents et futurs*, [en ligne]. Disponible sur : http://zone.ni.com/devzone/cda/tut/p/id/5402

[ni4] National Instruments. *Test RF et sans fil*, [en ligne]. Disponible sur : http://sine.ni.com/np/app/main/p/ap/mi/lang/fr/pg/1/sn/n17:mi,n21:1914/

[ni5] National Instruments. *Système de radio définie par logiciel (SDR) basé sur l'émetteur-récepteur IF RIO NI PXIe-5641R*, [en ligne]. Disponible sur : http://sine.ni.com/nips/cds/view/p/lang/fr/nid/207092

[nios] *Nios II Processor: The World's most Versatile Embedded Processor*, [en ligne]. Disponible sur : http://www.altera.com/products/ip/processors/nios2/ni2-index.html

[nisdr] *National Instruments Software-Defined Radio*, [en ligne]. Disponible sur : http://zone.ni.com/devzone/cda/tut/p/id/8787

[north] DR R. NORTH, N. BROWNE et L. SCHIAVONE. *Joint tactical radio system - connecting the GIG to the tactical*. Military Communications Conference, Washington DC, 23 au 25 octobre 2006, [en ligne]. Disponible sur : http://enterprise.spawar.navy.mil/UploadedFiles/JTRS_OVERVVIEW_MILCOM06_v12.pdf

O

[ofdmtx*] FTW IEEE802.11a/g/p OFDM Frame Encoder*, [en ligne]. Disponible sur : https://www.cgran.org/wiki/ftw80211ofdmtx

[omg] *Catalog of OMG Specifications*, [en ligne]. Disponible sur : http://www.omg.org/technology/documents/domain_spec_catalog.htm

[orfidee] *oRFIDGeoloc. Solution de géo-localisation à bord de la frégate Lafayette de la Marine nationale*, [en ligne]. Disponible sur : http://www.orfidee.com/downloads/orfidgeolocfinal.pdf

[ossie] *SCA-Based Open Source Defined Radio*, [en ligne]. Disponible sur : http://ossie.wireless.vt.edu

[oz9aec] *USRP Reference*, [en ligne]. Disponible sur : http://wiki.oz9aec.net/index.php/USRP_Reference

P

[pcm] *Texas instruments PCM1740 105 dB SNR Stereo DAC with Programmable PLL&VCO*, [en ligne]. Disponible sur : http://focus.ti.com/docs/prod/folders/print/pcm1740.html

[pentek] R. H. HOSKING. *Software Defined Radio Handbook Eighth Edition*. Janvier 2010, [en ligne]. Disponible sur : http://www.sdradio.eu/doc/DgtlRcvrHbk43.pdf

[pentek2] *Pentek Software Radio Products*, [en ligne]. Disponible sur : http://www.pentek.com/products/ProductsBy.cfm?Searchtype=Fcn&Category=Software%20Radio

[perez] J. C. NUNEZ PEREZ. *Contribution à la conception de systèmes de radiocommunications : de la modélisation de Transistors Bipolaires à l'évaluation des performances des systèmes d'émission-réception*. Thèse de doctorat présentée à l'INSA de Lyon, 2007, [en ligne]. Disponible sur : http://docinsa.insa-lyon.fr/these/pont.php?id=nunez_perez

[perseus] *Microtelecom Perseus*, [en ligne]. Disponible sur : http://www.microtelecom.it/perseus/index.html

[perseusoft] *Perseus control software V3.0beta1*, [en ligne]. Disponible sur : http://www.microtelecom.it/perseus/software.html

[plötz] *RFID Hacking*. 23rd Chaos Communication Congress « Who can you trust? ». 28 décembre 2008, [en ligne]. Disponible sur : http://events.ccc.de/congress/2006/Fahrplan/attachments/1232-23C3-RFID_Hacking-3.pdf

[pmsdr] *PM-SDR*, [en ligne]. Disponible sur : http://www.iw3aut.altervista.org/index.htm

[powersdr] *FlexRadio PowerSDR™ Features and Capabilities*, [en ligne]. Disponible sur : http://www.flex-radio.com/Products.aspx?topic=powersdr1x

[presdect] *ETSI TR 101 178 V1.5.1 (2005-02). Digital Enhanced Cordless Telecommunications (DECT); A High Level Guide to the DECT Standardization*, [en ligne]. Disponible sur : http://www.etsi.org/deliver/etsi_tr/101100_101199/101178/01.05.01_60/tr_101178v010501p.pdf

[pxi5641r] *NI PXIe-5641 Product In-Depth*, [en ligne]. Disponible sur : http://zone.ni.com/devzone/cda/tut/p/id/8786

[python] *Tutoriel Python pour GNU Radio*, [en ligne]. Disponible sur : http://gnuradio.org/redmine/wiki/1/TutorialsWritePythonApplications

Q

[quisk] *Quisk*, [en ligne]. Disponible sur : http://james.ahlstrom.name/

[qs1r] *SRL QuickSilver QS1R Receiver*, [en ligne]. Disponible sur : http://www.srl-llc.com/

R

[raychaudhuri] D. RAYCHAUDHURI, N. B. MANDAYAM, J. B. EVANS, B. J. EWY, S. SESHAN, et P. STEENKISTE. *Cognet: an architectural foundation for experimental cognitive radio networks within the future internet*. 2006, [en ligne]. Disponible sur : http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.125.7365

[reynwar] *Class gmsk_demod*, [en ligne]. Disponible sur : http://www.reynwar.net/gnuradio/epydoc/gnuradio.blks2impl.gmsk.gmsk_demod-class.html

[rf3315] *RF micro devices RF3315 Broadband high linearity amplifier*, [en ligne]. Disponible sur : http://www.datasheetcatalog.org/datasheet2/a/0ally80539kszo707lsxxjezz5yy.pdf

[rfidhandbook] *Frequencies for RFID-systems*, [en ligne]. Disponible sur : http://www.rfid-handbook.de/rfid/frequencies.html

[rohde] *Rohde & Schwarz*, [en ligne]. Disponible sur : http://www.rohde-schwarz.fr/fr/Produits/Test_Mesure

[rocky] *Rocky 3.7 - SDR software for the SoftRock radio*, [en ligne]. Disponible sur : http://www.dxatlas.com/rocky

S

[sasp] F. RIVET, Y. DEVAL, D. DALLET, D. BELOT et J.B. BÉGUERET. *Un Processeur de Traitement du Signal Analogique destiné à la Radio Logicielle*. 15èmes Journées Nationales Microondes, 23-24-25 Mai 2007, Toulouse, [en ligne]. Disponible sur : http://hal.archives-ouvertes.fr/hal-00161534

[satarkar] S. SATARKAR. *Performance analysis of the WiNC2R platform*. Master of Science, Graduate Program in Electrical and Computer Engineering, [en ligne]. Disponible sur : http://mss3.libraries.rutgers.edu/dlr/TMP/rutgers-lib_26397-PDF-1.pdf

[sca] *JPEO JTRS Standards : Software Communications Architecture (SCA)*, [en ligne]. Disponible sur : http://sca.jpeojtrs.mil/scanext.asp

[scari] *SCARI OPEN : Software Communications Architecture - Reference Implementation*. Communications Research Centre Canada, [en ligne]. Disponible sur : http://www.crc.gc.ca/en/html/crc/home/research/satcom/rars/sdr/products/scari_open/scari_open

[scc41] IEEE SCC41. *IEEE Standards Coordinating Committee 41 (Dynamic Spectrum Access Networks*. 2010, [en ligne]. Disponible sur : http://www.scc41.org/crinfo

[schmid1] T. SCHMID, T. DREIER et M. B. SRIVASTAVA. *Software Implementation of Short-range Wireless Standards for Sensor Networking*. SenSys 2006, novembre 2006, [en ligne]. Disponible sur : http://www.inf.ufsc.br/~tiagorm/Thomas_Schmid_PAPER.pdf

[schmid2] T. SCHMID, O. SEKKAT et M. B. SRIVASTAVA. *An experimental study of network performance impact of increased latency in software defined radios*. Mobicom Wintech Workshop, Montréal (Canada), septembre 2007, [en ligne]. Disponible sur : http://tschmid.webfactional.com/media/media/documents/pdf/2010/01/23/wintech401-schmid.pdf

[sdr4all] *Software Defined Radio For All*, [en ligne]. Disponible sur : http://sdr4all.org/index.html

[sdr4all2] L. S. CARDOSO, R. DE LACERDA, P. JALLON et M.DEBBAH. *SDR4all: A tool for Making Flexible Radio a Reality*. COGIS'09, Paris, France, [en ligne]. Disponible sur : http://hal-supelec.archives-ouvertes.fr/docs/00/44/69/67/PDF/C0947.pdf

[sdr4all3] L. S. CARDOSO, S. AZARIAN, P. JALLON et M.DEBBAH. *SDR4all: Software Defined Radio Made Easy*. 6ième *Workshop* sur la radio logicielle 2010, Karlsruhe, Allemagne, [en ligne]. Disponible sur : http://www.supelec.fr/offres/file_inline_src/342/342_P_11867_70.pdf

[sdrforum] *Wireless Innovation Forum, ou SDR Forum 2.0*, [en ligne]. Disponible sur : http://www.sdrforum.org/

[sdrip] *RFspace SDR-IP*, [en ligne]. Disponible sur : http://www.rfspace.com/RFSPACE/SDR-IP.html?uhfsatbanner

[sdriq] *RFspace SDR-IQ Receiver*, [en ligne]. Disponible sur : http://www.rfspace.com/RFSPACE/SDR-IQ.html

[sdrmax] *SDRMAXII Version 2.0.0.3 Release Notes*, [en ligne]. Disponible sur : http://www.philcovington.com/qs1r_latest/LatestStableRelease/SDRMAXII_Release_Notes_04232010.pdf

[sdrmax3] Kingsqueak.org & kc2rgw.com. *SDR Software Defined Radio*, [en ligne]. Disponible sur : http://www.kingsqueak.org/about/amateur-radio/sdr-software-defined-radio

[sdrshell] Edson Pereira. *SDR-Shell. Amateur Radio Homepage*, [en ligne]. Disponible sur : http://www.ewpereira.info/sdr-shell

[seskar] I. SESKAR. *Support for Physical Layer Experimentation Universal Software Radio Peripheral (USRP/USRP2) and GnuRadio*. Hands-on-Tutorial - Future Internet Summer School 2009 Part 2. Rutgers, The State University of New Jersey, [en ligne]. Disponible sur : http://www.comnets.uni-bremen.de/typo3site/uploads/media/FISS_2009_Part_2.pdf

[sn74] *Single-supply voltage-level translator with nine configurable gate logic functions*, [en ligne]. Disponible sur : http://focus.ti.com/lit/ds/symlink/sn74aup1t57.pdf

[softrock] *WB5RVZ Software Defined Radio Homepage*, [en ligne]. Disponible sur : http://www.wb5rvz.com/sdr/

[sora] *Microsoft Research Software Radio Platform for Academic Use*, [en ligne]. Disponible sur : http://research.microsoft.com/en-us/projects/sora/academickit.aspx

[sora2] *Microsoft Research Software Radio Academic Kit*, [en ligne]. Disponible sur : http://research.microsoft.com/en-us/downloads/35a929d6-0cb0-4318-968a-69d05c9bbc65/default.aspx

[sora3] K. TAN, J. ZHANG, J. FANG, H. LIU, Y. YE, S. WANG, Y. ZHANG, H. WU, W. WANG, et G. M. VOELKER. " Sora: High performance software radio using general purpose multi-core processors ", NSDI 2009, [en ligne]. Disponible sur : http://research.microsoft.com/pubs/79927/Sora-camera-ready.pdf

[sora4] J. ZHANG, K. TAN, S. XIANG, Q. YIN, Q. LUO, Y. HE, J. FANG et Y. ZHANG. *Experimenting Software Radio with the Sora Platform*. SIGCOMM 2010, [en ligne]. Disponible sur : http://conferences.sigcomm.org/sigcomm/2010/papers/sigcomm/p469.pdf

[spartan3] *Xilinx Spartan-3 FPGA Family Data Sheet*, [en ligne]. Disponible sur : http://www.xilinx.com/support/documentation/data_sheets/ds099.pdf

[spectra] PrismTech. *Spectra*. 2010, [en ligne]. Disponible sur : http://www.prismtech.com/section-item.asp?sid4=&sid3=&sid2=54&sid=18&id=305

[spectravue] *SpectraVue*, [en ligne]. Disponible sur : http://www.moetronix.com/spectravue.htm

[spectrum] *Audio Spectrum Analyzer ("Spectrum Lab")*, [en ligne]. Disponible sur : http://www.qsl.net/dl4yhf/spectra1.html

[spectrum2] *Spectrum Lab – Un vrai logiciel laboratoire*, [en ligne]. Disponible sur : http://www.itsrainingelephants.com/2010/07/14/spectrum-lab-un-vrai-logiciel-laboratoire/

[std80211] *IEEE Std 802.11TM-2007*, [en ligne]. Disponible sur : http://www.cs.jhu.edu/~cliang4/public/datasheets/802.11-2007.pdf

[stratix5] *Stratix V FPGAs 2010*, [en ligne]. Disponible sur : http://www.altera.com/literature/br/br-stratix-v-hardcopy-v.pdf

[swig] *SWIG*, [en ligne]. Disponible sur : http://www.swig.org/index.php

[systemvue1] *SystemVue Electronic System-Level (ESL) Design Software*, [en ligne]. Disponible sur : http://www.home.agilent.com/agilent/product.jspx?nid=-34264.0.00&lc=eng&cc=US

[systemvue2] *SystemVue 2010.01, related products*, [en ligne]. Disponible sur : http://www.home.agilent.com/agilent/product.jspx?cc=FR&lc=fre&nid=-34264.925868&pageMode=RL

T

[tektronix] *Worldwide Spectrum Allocations Courtesy of Tektronix*, [en ligne]. Disponible sur : http://www2.tek.com/cmsreplive/tirep/16042/37W_19885_1_2009.09.10.05.04.04_16042_EN.pdf

[teraops] Los Alamos National Laboratory. *High Efficiency Space-Based Software Radio Architectures*, [en ligne]. Disponible sur : http://www.lanl.gov/roadrunner/pdfs/TeraOpsSDRReconpaper.pdf

[terre] M. TERRÉ. *Electronique C4 DECT (v4.1)*. Conservatoire national des arts et métiers, [en ligne]. Disponible sur : http://www1.cnam.fr/elau/publi/terre/images/C4_DECT.pdf

[ti] Site officiel de Texas Instruments, [en ligne]. Disponible sur : http://www.ti.com/

[ti2] *Bluetooth® Technology*: BRF6150, [en ligne]. Disponible sur : http://focus.ti.com/general/docs/wtbu/wtbuproductcontent.tsp?templateId=6123&navigationId=12020&contentId=4653

[tlk2701] *Texas Instruments TLK2701, 1.6 to 2.7 GBPS TRANSCEIVER*, [en ligne]. Disponible sur : http://focus.ti.com/lit/ds/symlink/tlk2701.pdf

[tps777] *Texas Instruments TPS777XX Fast-transient-response 750-mA low dropout linear regulators*, [en ligne]. Disponible sur : http://focus.ti.com/lit/ds/symlink/tps77701.pdf

U

[uclazigbee] The Comprehensive GNU Radio Archive Network. *UCLA Zigbee*, [en ligne]. Disponible sur : https://www.cgran.org/wiki/UCLAZigBee

[uhd] *UHD Start*, [en ligne]. Disponible sur : http://code.ettus.com//redmine/ettus/projects/uhd/wiki

[usrpe100] *Ettus Research™ USRP ™ E100 Embedded Software Defined Radio*, [en ligne]. Disponible sur : http://www.ettus.com/downloads/USRP_E100_Series_temporary_datasheet.pdf

[usrpn200] *USRP N200 Series*, [en ligne]. Disponible sur : http://www.ettus.com/downloads/ettus_ds_usrp_n200series_v3.pdf

V

[valerio] D. Valerio. *Open Source Software-Defined Radio: A survey on GNUradio and its application*. FTW Technical Report. Août 2008, [en ligne]. Disponible sur : http://userver.ftw.at/~valerio/files/SDRreport.pdf

[vtcornet] *Cognitive Radios and Networks*. Bradley Department of electrical & Computer Engineering. Virginia Tech, [en ligne]. Disponible sur : http://wireless.vt.edu/research/Cognitive_Radios_Networks/

W

[warp] *Wireless open-Access Research Platform*, [en ligne]. Disponible sur : http://warp.rice.edu/index.php

[warp2] Mango communications. *WARP FPGA board, hardware version 2.2*, [en ligne]. Disponible sur : http://www.mangocomm.com/products/boards/warp-fpga-board-v2

[warp3] Mango communications. *WARP Radio Board*, [en ligne]. Disponible sur : http://www.mangocomm.com/products/boards/warp-radio-board-v1

[wbxrpp] *WBX Receiver Performance Plots*, [en ligne]. Disponible sur : http://code.ettus.com/redmine/ettus/documents/show/16.

[wbxrs] *WBX receiver sensitivity in CW*, [en ligne]. Disponible sur : http://www.oz9aec.net/index.php/gnu-radio/gnu-radio-blog/319-wbx-receiver-sensitivity-in-cw.

[wbxsch] *WBX Schematics*, [en ligne]. Disponible sur : http://code.ettus.com/redmine/ettus/documents/17.

[webpack] *ISE WebPACK Design Software*, [en ligne]. Disponible sur : http://www.xilinx.com/tools/webpack.htm

[wgpt80211] *Official IEEE 802.11 Working Group Project Timelines*, [en ligne]. Disponible sur : http://grouper.ieee.org/groups/802/11/Reports/802.11_Timelines.htm

[wiki1] Wikipedia. *Cognitive radio*, [en ligne]. Disponible sur : http://en.wikipedia.org/wiki/Cognitive_radio

[wiki2] Wikipédia. *VHDL-AMS*, [en ligne]. Disponible sur : http://fr.wikipedia.org/wiki/VHDL-AMS

[wiki3] Wiktionnaire. *Fond de panier*, [en ligne]. Disponible sur : http://fr.wiktionary.org/wiki/fond_de_panier

[wiley] W. TUTTLEBEE. *Software defined radio: Origins, Drivers and International Perspective*. Éditions John Wiley & Sons Ltd. 25 janvier 2002. 350 pages. ISBN-10: 0470844647. ISBN-13: 978- 0470844649.

[winc2r] *Network Centric Cognitive Radio (WiNC2R)*, [en ligne]. Disponible sur : http://www.winlab.rutgers.edu/docs/focus/WiNC2R.html

[winrad] *Winrad.org*, [en ligne]. Disponible sur : http://www.winrad.org/

[wxgui] *GNU Radio WXGUI Signal Analysis Tools*, [en ligne]. Disponible sur : http://www.joshknows.com/wxgui

X

[xilinx] *VIRTEX-7 FPGAS*, [en ligne]. Disponible sur : http://www.xilinx.com/publications/prod_mktg/Virtex7-Product-Table.pdf

[xilinx2] Xilinx, Inc. *System Generator for DSP*. 2010, [en ligne]. Disponible sur : http://www.xilinx.com/tools/sysgen.htm

[xilinx3] *Xilinx ISE Design Suite 12*, [en ligne]. Disponible sur : http://www.xilinx.com/support/download/index.htm

Z

[zahwe] O. ZAHWE. *Conception et Réalisation d'un Circulateur Coplanaire à Couche Magnétique de YIG en Bande X pour des Applications en Télécommunications*. Thèse de doctorat. 17 juin 2009, [en ligne]. Disponible sur : http://tel.archives-ouvertes.fr/tel-00419725_v1/

[zeligsoft] Zeligsoft. *Zeligsoft SDR/SCA*. 2010, [en ligne]. Disponible sur : http://www.zeligsoft.com/solutions/sdr-sca

Liste des figures

Liste des tableaux

Radio logicielle : analyse d'architectures matérielles et outils informatiques.

Mémoire d'Ingénieur C.N.A.M., Versailles 2011

RÉSUMÉ

Les progrès réalisés en électronique numérique et en informatique ont permis de remplacer une partie de la technologie analogique des systèmes de radiocommunication par une composante numérique et logicielle, et donc une capacité à la configuration et la synthèse de différentes formes d'onde. Depuis quelques années des radios logicielles « libres » apparaissent. Ces équipements offrent la possibilité au plus grand nombre d'étudier le spectre radio, et notamment les protocoles de transmission radiofréquence. Après une étude détaillée de la technologie radio logicielle, un panorama des équipements plus ou moins « libres » est réalisé, en se concentrant principalement sur les architectures matérielles USRP associées au projet logiciel GNU Radio ainsi que sur l'emploi de ces équipements pour étudier et mettre en œuvre quelques protocoles de radiocommunication.

Mots clés : radio logicielle, électronique numérique, informatique, USRP, GNU Radio, protocoles.

SUMMARY

Advances in digital electronics and computing have helped in replacing some of the analog modules of radio communication systems with digital and software components, and thus the ability to configure and to synthesize various waveforms. In recent years, "open-source" software-defined radios emerge. These devices provide the opportunity for many people to study the radio spectrum, including wireless protocols. After a detailed study of the software radio technology, an overview of more or less "open-source" products has been performed, focusing mainly on USRP hardware architecture associated with the GNU Radio project. Finally wireless standards have been explored through implementations based on these tools.

Key words: software radio, digital electronics, computer, USRP, GNU Radio, protocols.