De la radio matérielle à la radio logicielle
Evolution de la menace

Chaouki Kasmi,
Arnaud Ebalard
prenom.nom@ssi.gouv.fr

ANSSI
51, bvd de la Tour-Maubourg
75700 Paris 07 SP

Agenda

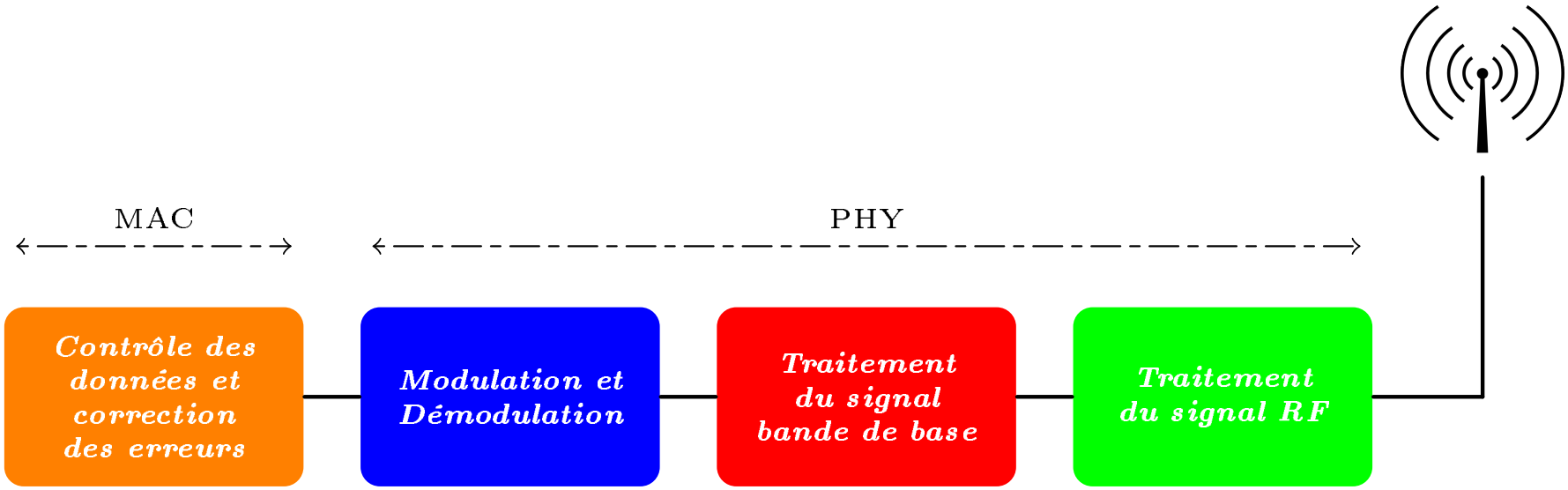
Contexte

Contexte

Sécurité et mobilité

- Multiplication des protocoles sans-fils :
  - Wi-Fi
  - WiMAX/LTE
  - Zigbee
  - 2G/3G
  - RFID/NFC
- Evolution des méthodes de développement de produits radios
- Besoins d'audits sécu
  - Couches basses/hautes
  - Mécanismes sécu

Architecture type d'un émetteur/récepteur



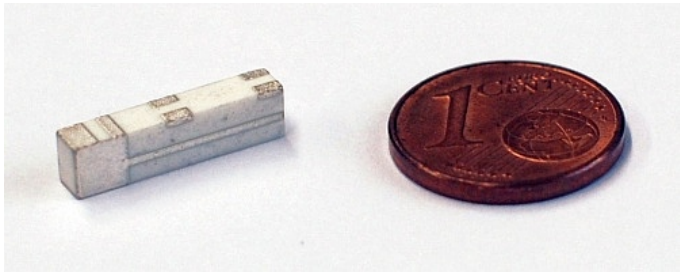
Couche physique (1/3)

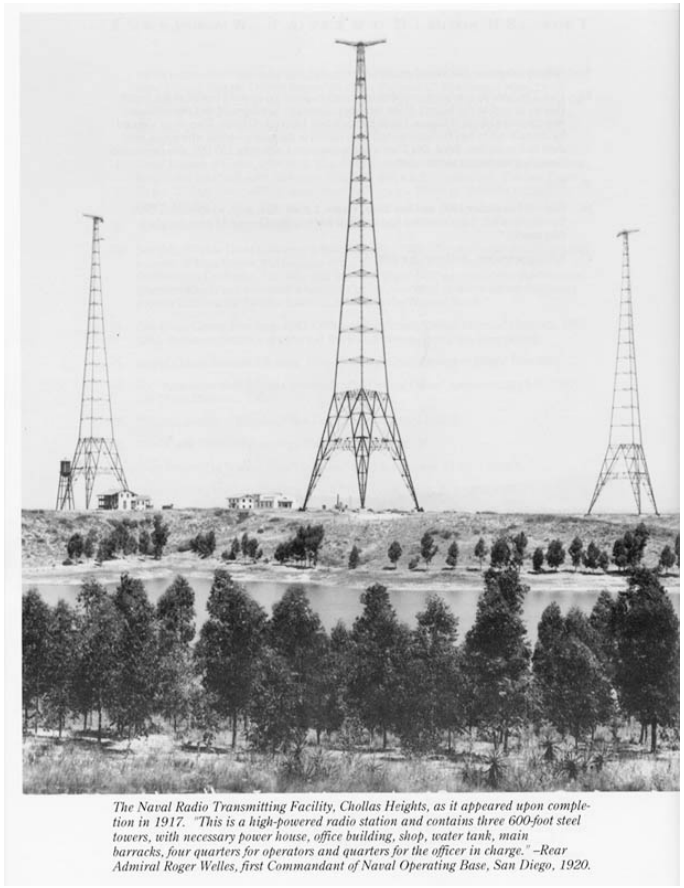
Caractéristiques dimensionnantes

- Fréquence de travail

Impacts

- Architecture du récepteur
- Dimension de l'antenne
- Gain et sélectivité de l'antenne





The Naval Radio Transmitting Facility, Chollas Heights, as it appeared upon completion in 1917. "This is a high-powered radio station and contains three 600-foot steel towers, with necessary power house, office building, shop, water tank, main barracks, four quarters for operators and quarters for the officer in charge." –Rear Admiral Roger Welles, first Commandant of Naval Operating Base, San Diego, 1920.

Couche physique (2/3)

Autres caractéristiques dimensionnantes

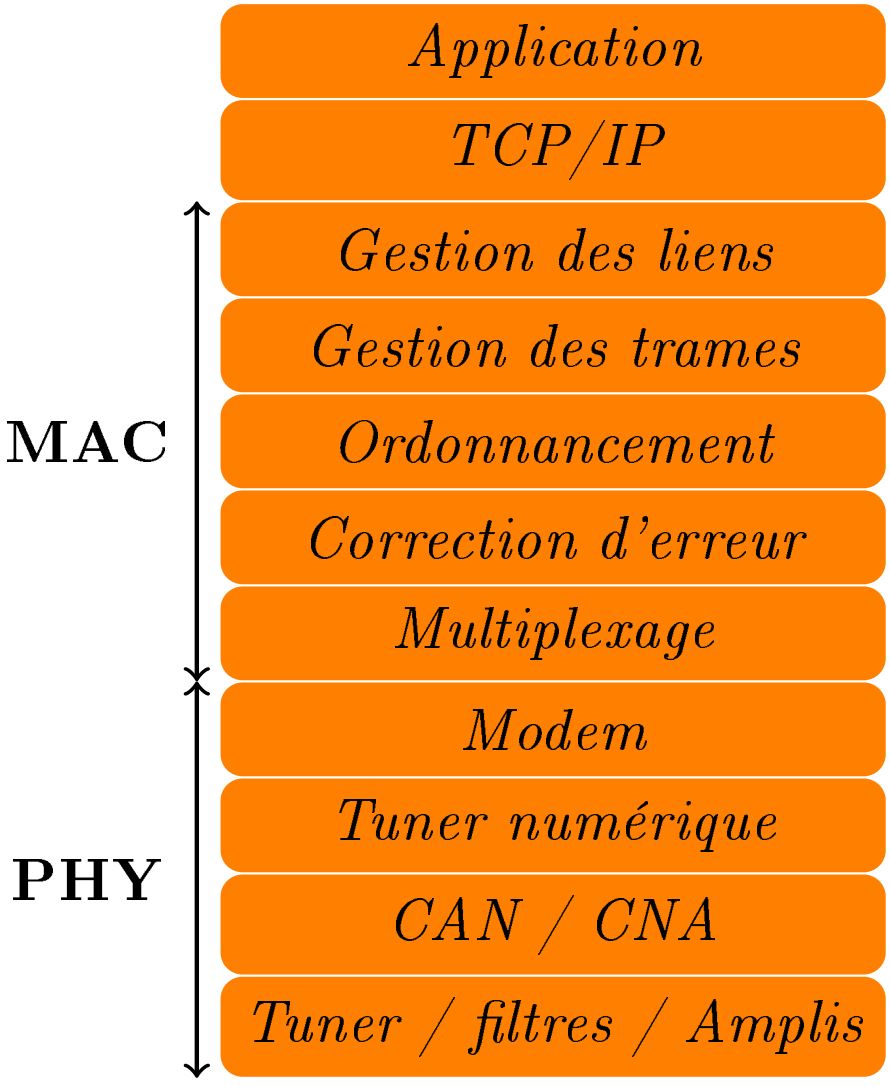
- Bande passante : Conditionne la capacité de traitement de tous les étages, analogiques et numériques (WiFi : 20 MHz, 2G : 200 kHz)
- Utilisation de saut de fréquence : nécessite une agilité du récepteur (Bluetooth : 1600 sauts/seconde)
- Parallélisme des communications
  - Simplex (Pager)
  - Alternat (half duplex) (RFID)
  - Bidirectionnel simultané (full duplex) (3G)
  - MIMO (WiMax, 802.11n)

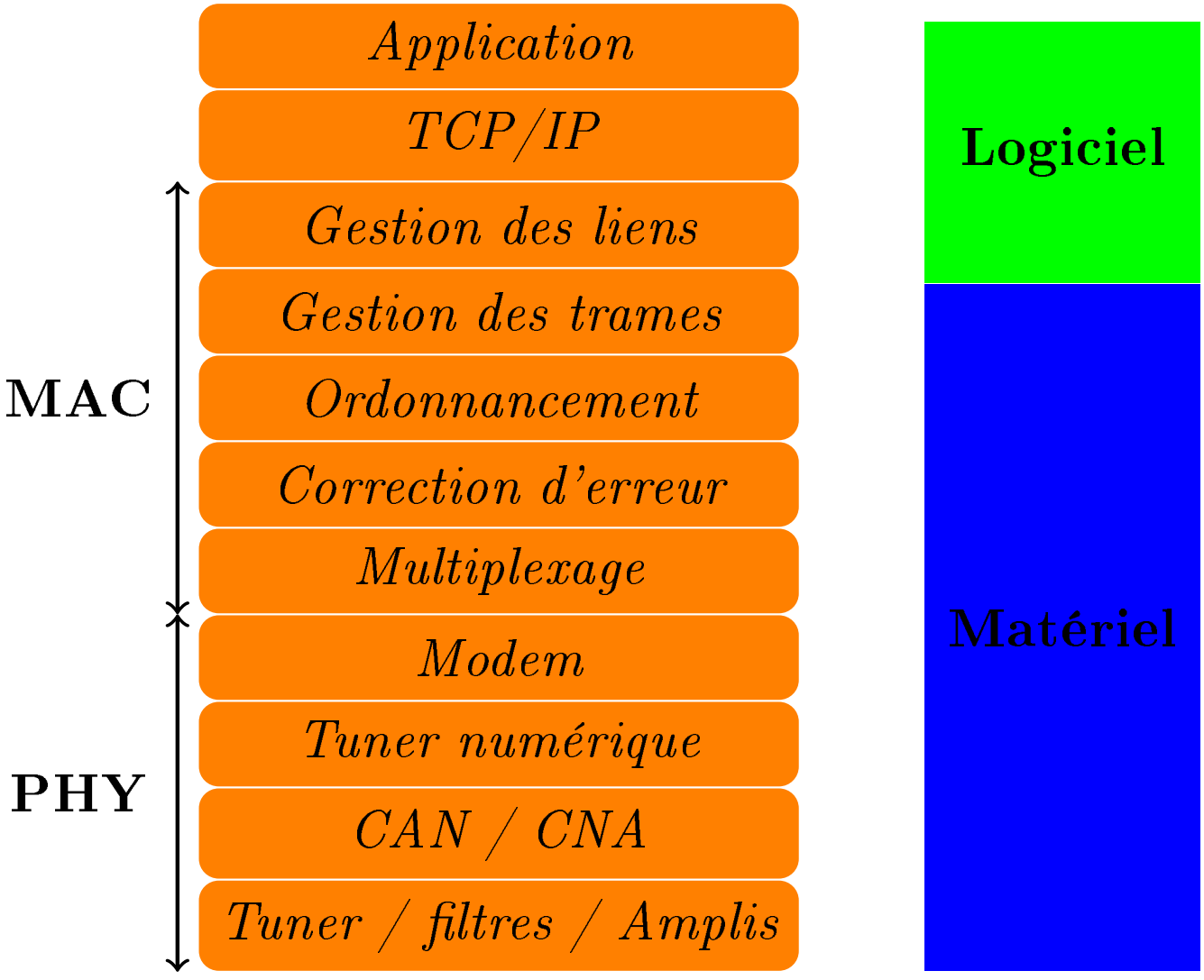
Couche physique (3/3)

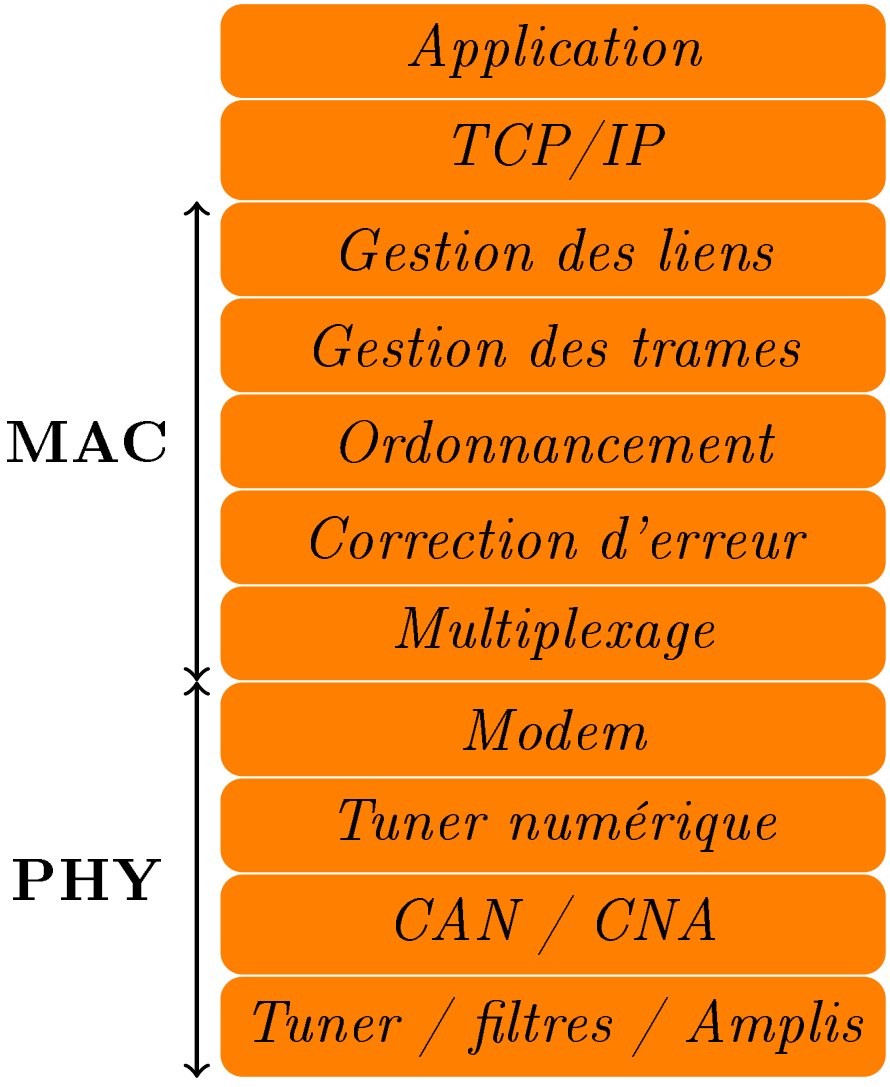
- Modulation
  - Du plus simple (OOK, FSK) (RFID)
  - Au plus complexe (OFDM, n-QAM, DSSS) (DVB, 3G)
- Codage canal
  - Hamming, Manchester, Miller...
- Codes détecteurs et codes correcteurs d'erreurs
  - Du plus simple : CRC (RFID)
  - Au plus complexe : Reed-Solomon (CPL), treillis (GSM), turbo codes (DVB)

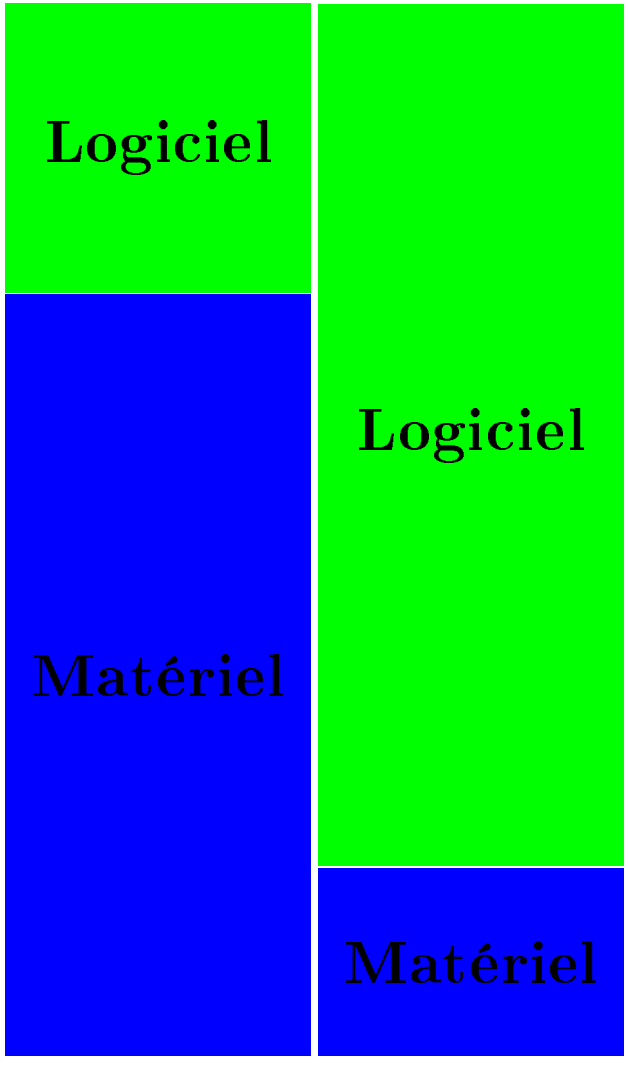
Caractéristiques dimensionnantes

- Détection de porteuse : CSMA
  - Détection de collision : CSMA/CD (ethernet)
  - Évitement de collision : CSMA/CA (WiFi)
- Multiplexage
  - Temporel (TDMA) (GSM)
  - Fréquentiel (FDMA) (GSM)
  - Par code (CDMA) (3G)


Application
TCP/IP
Gestion des liens
Gestion des trames
Ordonnancement
Correction d'erreur
Multiplexage
Modem
Tuner numérique
CAN / CNA
Tuner / filtres / Amplis
MAC
PHY

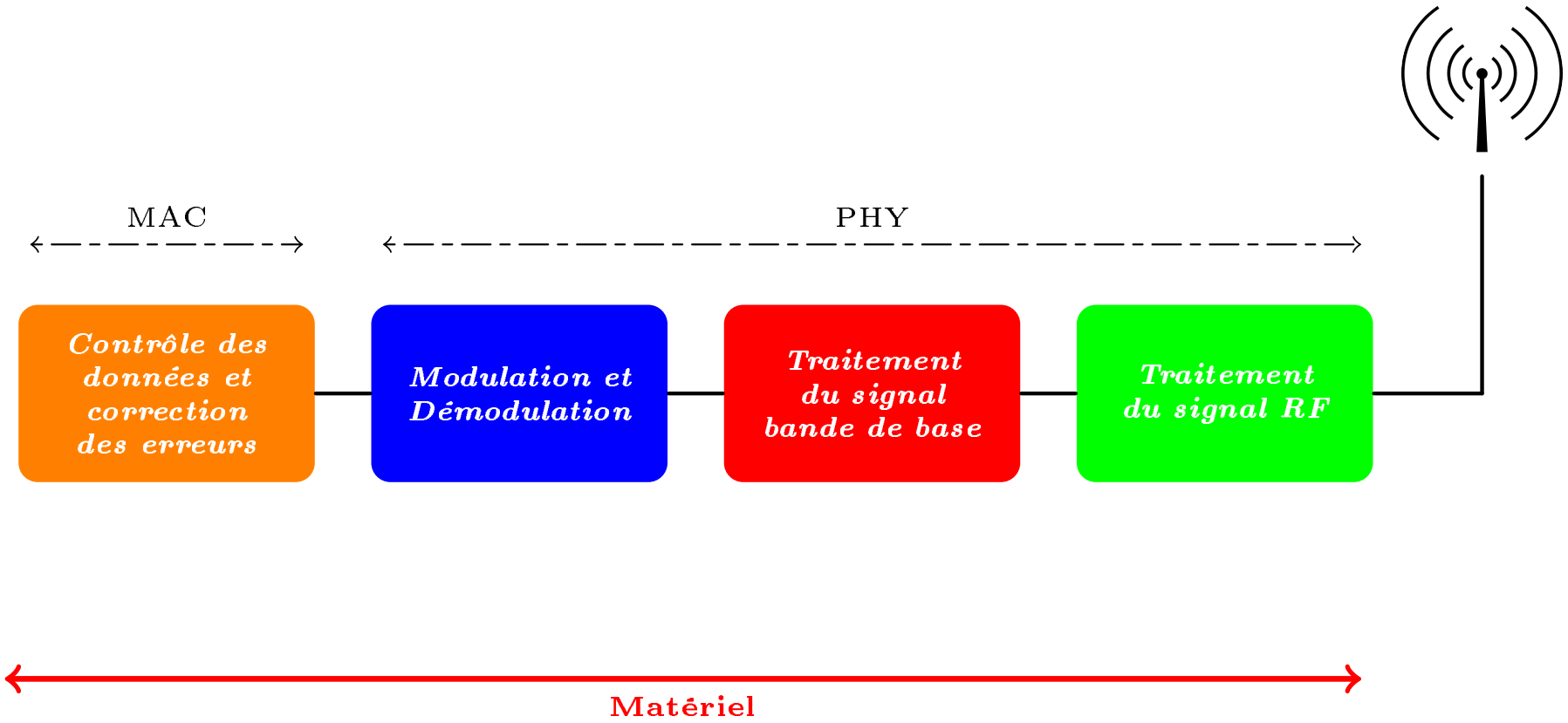

Application
TCP/IP
Gestion des liens
Gestion des trames
Ordonnancement
Correction d'erreur
Multiplexage
Modem
Tuner numérique
CAN / CNA
Tuner / filtres / Amplis
MAC
PHY
Logiciel
Matériel
Radio matérielle


Application
TCP/IP
Gestion des liens
Gestion des trames
Ordonnancement
Correction d'erreur
Multiplexage
Modem
Tuner numérique
CAN / CNA
Tuner / filtres / Amplis
MAC
PHY


Logiciel
Matériel
Logiciel
Matériel
Radio maté-rielle
Radio logicielle

Radio matérielle

Architecture



Objectifs (rappels)

- Interagir avec les couches basses et hautes d'un protocole
- Analyser les mécanismes de sécurité

Radio matérielle

Limitations

Objectifs (rappels)

- Interagir avec les couches basses et hautes d'un protocole
- Analyser les mécanismes de sécurité

Limitations de la radio matérielle

- Unicité protocolaire (antenne, circuit de démodulation)
- Couches basses non modifiables
- Pile protocolaire figée
- Positionnement de la couche sécurité
  - Bas niveau (hard) $\Longrightarrow$ difficile (e.g. Bluetooth, GSM)
  - Haut niveau (driver, applicatif) $\Longrightarrow$ possible (e.g. WiFi ...)

Radio matérielle

Limitations

Objectifs (rappels)

- Interagir avec les couches basses et hautes d'un protocole
- Analyser les mécanismes de sécurité

Limitations de la radio matérielle

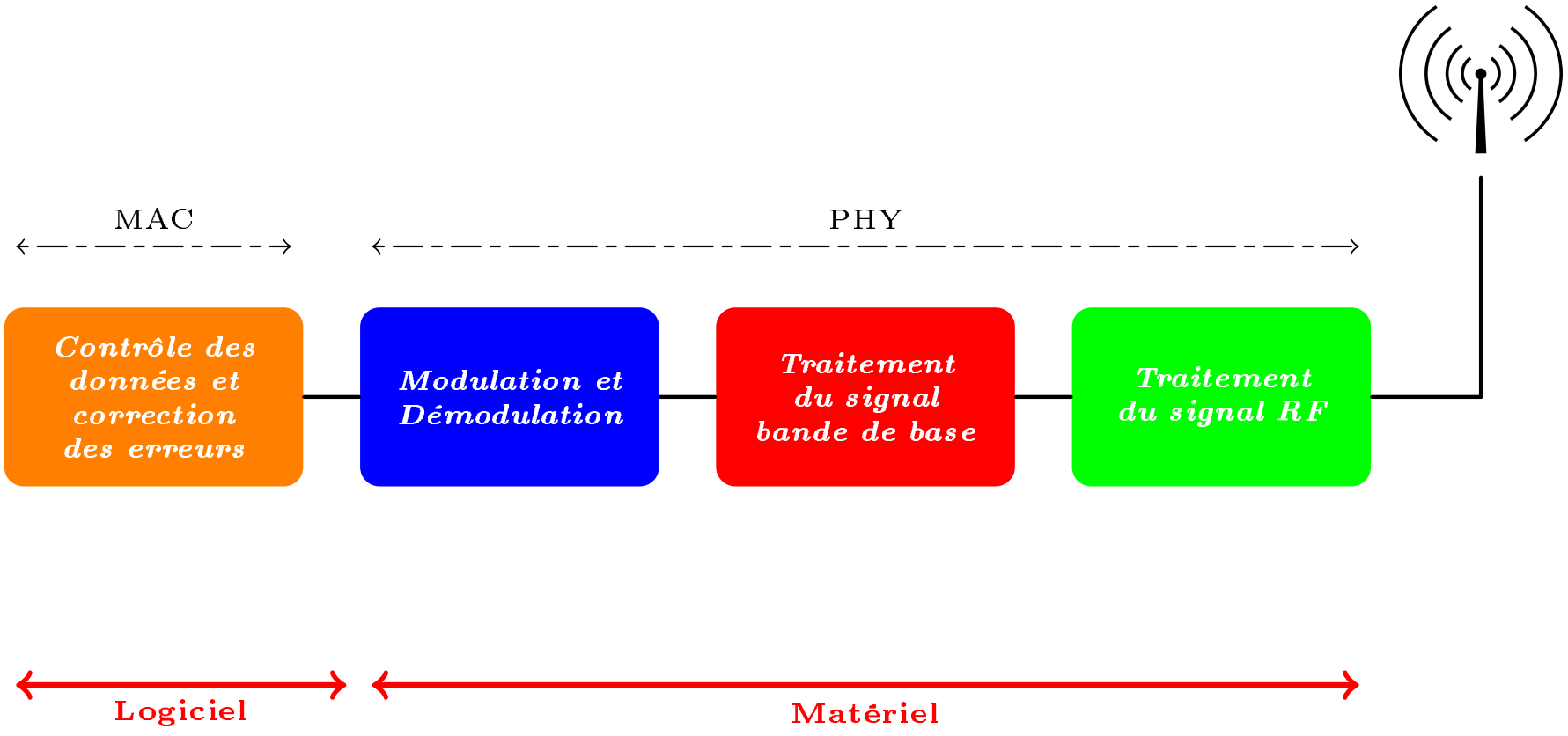
- Unicité protocolaire (antenne, circuit de démodulation)
- Couches basses non modifiables
- Pile protocolaire figée
- Positionnement de la couche sécurité
  - Bas niveau (hard) $\Longrightarrow$ difficile (e.g. Bluetooth, GSM)
  - Haut niveau (driver, applicatif) $\Longrightarrow$ possible (e.g. WiFi ...)

Conclusion

Intérêt limité à des protocoles radios **simples** type contrôle d'accès 125 kHz, 433 MHz

Périphériques reconfigurables

Architecture



Objectifs (rappels)

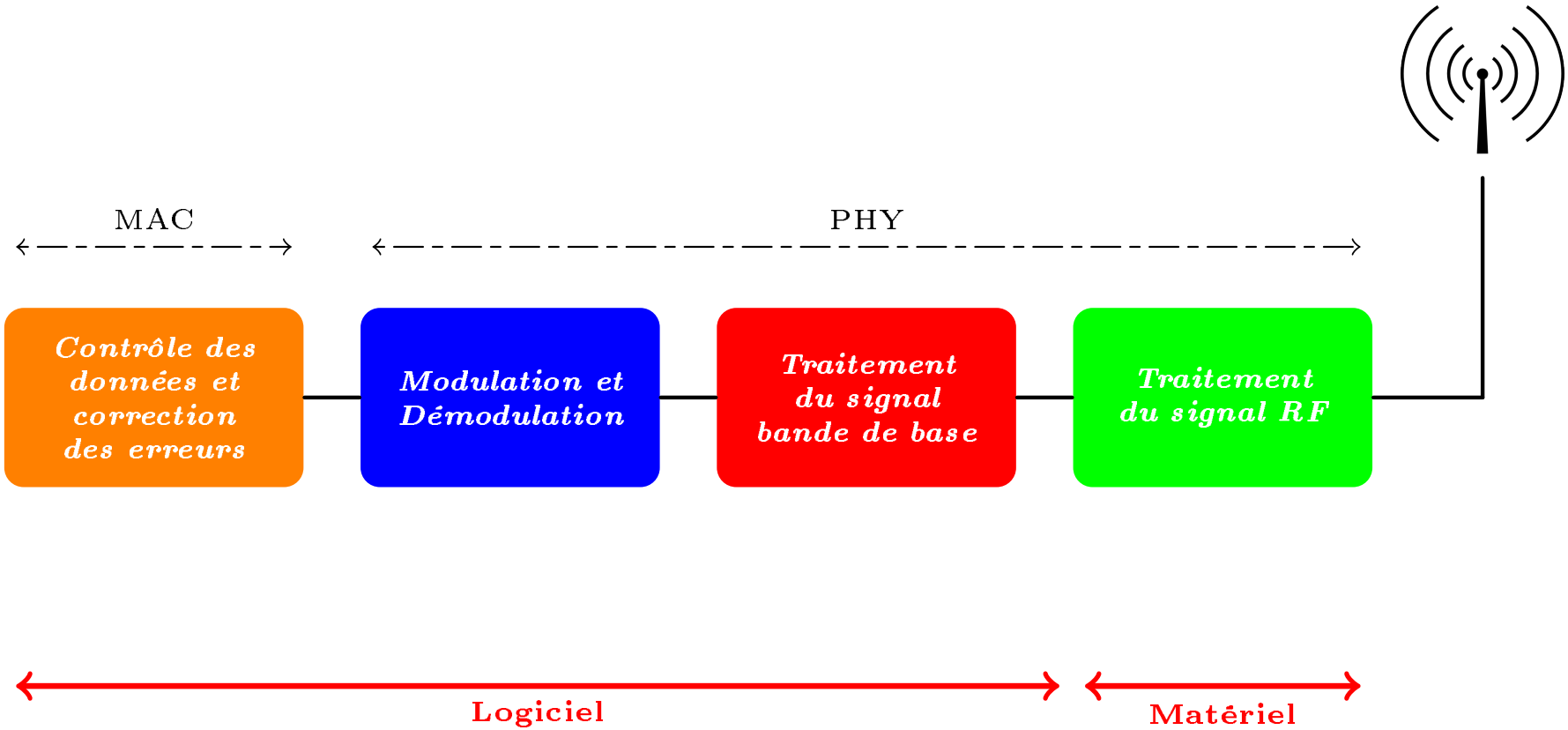
- Interagir avec les couches basses et hautes d'un protocole
- Analyser les mécanismes de sécurité

Limitations des périphériques reconfigurables

- Portée de l'API exposée :
  - Support de l'injection ?
  - Surcharge de champs (CRC en wifi, @MAC sur les premières cartes, UID sur dongles NFC)
  - Automate d'état figé ou non ?
- Couches basses non modifiables
- Ratio entre soft et hard pour la pile protocolaire
- Positionnement de la couche sécurité

Radio logicielle

Architecture



Avantages industriels

- Flexibilité (modification de la couche physique),
- Reprogrammation d'une même plateforme matérielle pour différentes couches physiques (e.g. modulation),
- Coût
  - Réduction des temps de développement,
  - Réduction des qualifications requises

Radio logicielle

Causes des évolutions vers la radio logicielle

Avantages industriels

- Flexibilité (modification de la couche physique),
- Reprogrammation d'une même plateforme matérielle pour différentes couches physiques (e.g. modulation),
- Coût
  - Réduction des temps de développement,
  - Réduction des qualifications requises

$\Longrightarrow$ "Software is the new Hardware"

Radio logicielle

Causes des évolutions vers la radio logicielle

Avantages industriels

- Flexibilité (modification de la couche physique),
- Reprogrammation d'une même plateforme matérielle pour différentes couches physiques (e.g. modulation),
- Coût
  - Réduction des temps de développement,
  - Réduction des qualifications requises

$\Longrightarrow$ "Software is the new Hardware"

Motivation fonctionnelle

- Migration de l'analogique au numérique (DSP, FPGA...)
- Performance des équipements embarqués
- Augmentation de la vitesse des interfaces de communication

Classification des équipements radios

Cat.	**Dénomination**	**Ex. de matériel**
0	Radio matérielle	Récepteur à lampe
I	Radio contrôlée par logiciel	Carte WiFi
II	Radio définie par logiciel	USRP
III	Radio logicielle idéale	N/A
IV	Radio logicielle ultime	N/A

Origine du besoin d'analyse des protocoles radios

Panorama/tendance

- Explosion horizontale : nombre d'équipements connectés
- Explosion verticale : nombre de protocoles radios

Menace

- Dépendance forte aux équipements connectés
- Utilisation pour l'échange de données critiques
  - Wifi, DECT dans les grandes entreprises
  - Zigbee et GPRS pour les applications SCADA
- Résilience supposée des infrastructures de communication

Analyse protocolaire

Contrôle d'accès 125 kHz et 433 MHz

Caractéristiques

- Technologie RFID (basse fréquence)
- Communication bidirectionnelle : faible débit
- Couche physique simple (OOK, FSK)
- Pas ou peu de couche protocolaire

Moyens d'analyse

Réalisation d'un simple circuit analogique ou numérique suffisante

Analyse protocolaire

ISO 14443 (Mifare, NFC)

Caractéristiques

- Fréquence relativement faible
- Faible débit
- Couche physique simple
- **Couche protocolaire complexe**

Moyens d'analyse

- Complexité accrue pour la réalistion d'un circuit analogique ou numérique robuste à ces fréquences
- Nécessité d'implémentation de la pile protocolaire

Conclusion

Intérêt du dongle sur un développement matériel complet

Analyse protocolaire

GSM/3G (900 Mhz, 1.8 GHz, 2.1 GHz)

- Couche PHY et MAC disponibles (standards imbuvables)
- Mécanismes de sécurité fermés [KasmiMorin2011]

Analyses effectuées

- Théorique
  1. A5/1 (après fuite puis rétroconception)
  2. COMP128 (après rétroconception sur carte SIM)
- Pratique
  1. Absence de dongle disponible a mené à
  2. Rétroconception de terminaux (OsmocomBB) puis
  3. Réimplémentation via USRP (OpenBTS) puis
  4. Test des réseaux opérateurs et PoC sécurité (Burning Man)

Analyse protocolaire
DECT (1.8 GHz)

- Couches PHY et MAC documentées (similaires à GSM)
- Mécanismes de sécurité fermés

Analyses effectuées

- Théorique
  - Algorithme de chiffrement (rétroconception de chip DECT)
- Pratique
  1. Tentative de réimplémentation via USRP abandonnée car
  2. Découverte d'une carte DECT reflashable (deDECTed.org)
  3. Démonstration des attaques sur la cryptographie + DoS
  4. Spécification de mécanismes crypto. de substitution

Analyse protocolaire

Bluetooth (2.4 GHz)

- Couche PHY complexe (Modulation GFSK, CR/CC)
- Couche MAC complexe (FHSS 1600 sauts/s, appariement)
- Protocole documenté mais implémentation complexe

Conclusion

- Analyse par dongle possible sur les couches hautes
- Analyse par radio logicielle difficile (bande passante élevée, rapidité de reconfiguration)
  1. ***Partielle*** : en utilisant 1 USRP par passage de la fréq. de réception à 200 μs (< 625 μs)
  2. ***Totale (79 canaux)*** : en couplant 8 USRP !

Analyse protocolaire

Zigbee (868 MHz et 2.4 GHz)

- Couche PHY complexe (Modulation ASK/BPSK, CR/CC)
- Couche MAC complexe
- Protocole documenté, implémentation moins complexe que celle de Bluetooth ($\approx$ 10 fois moins importante)

Conclusion

- ***En théorie***, analyse par dongle sur les couches hautes
- Analyse par radio logicielle possible car
  - Disponibilité d'une implémentation de pile protocolaire
  - Technique de modulation "simple" (DSSS, PSSS)

Analyse protocolaire

WiFi (2.4 GHz, 5 GHz)

Standard totalement disponible

- Couches PHY complexes (différentes modulations)
- Couche MAC complexe mais implémentée
- Sécurité (802.11i)

Evolution historique non négligeable

1. Premières cartes : presque tout en hard, évolutions limitées
2. Explosion en volume du standard
   - Sécurité : WPA, WPA2, mode entreprise, ...
   - Extensions : 802.11s, 802.11f, 802.11p, ...
3. Besoin de modularité au niveau des cartes (MAJ soft)

$\Longrightarrow$ Dématérialisation de la pile protocolaire

Conclusion

Analyse protocolaire

Standards étudiés

- RFID/ISO-14443
- DECT/GSM
- Bluetooth/ZigBee/WiFi

Standards en cours d'analyse

- Réseaux PMR (TETRA/GSM-R)
- Réseaux cellulaires (UMTS/LTE-A/WIMAX)
- Liaisons satellites (IP over Sat/GMR/GPS)

Evolution du matériel vers le logiciel

- Amélioration des équipements (BP, flexibilité...)
- Standardisation des couches physiques
- Intégration de nouvelles interfaces (Ethernet, PCI(e)...)

Conclusion

Prise en compte de la menace

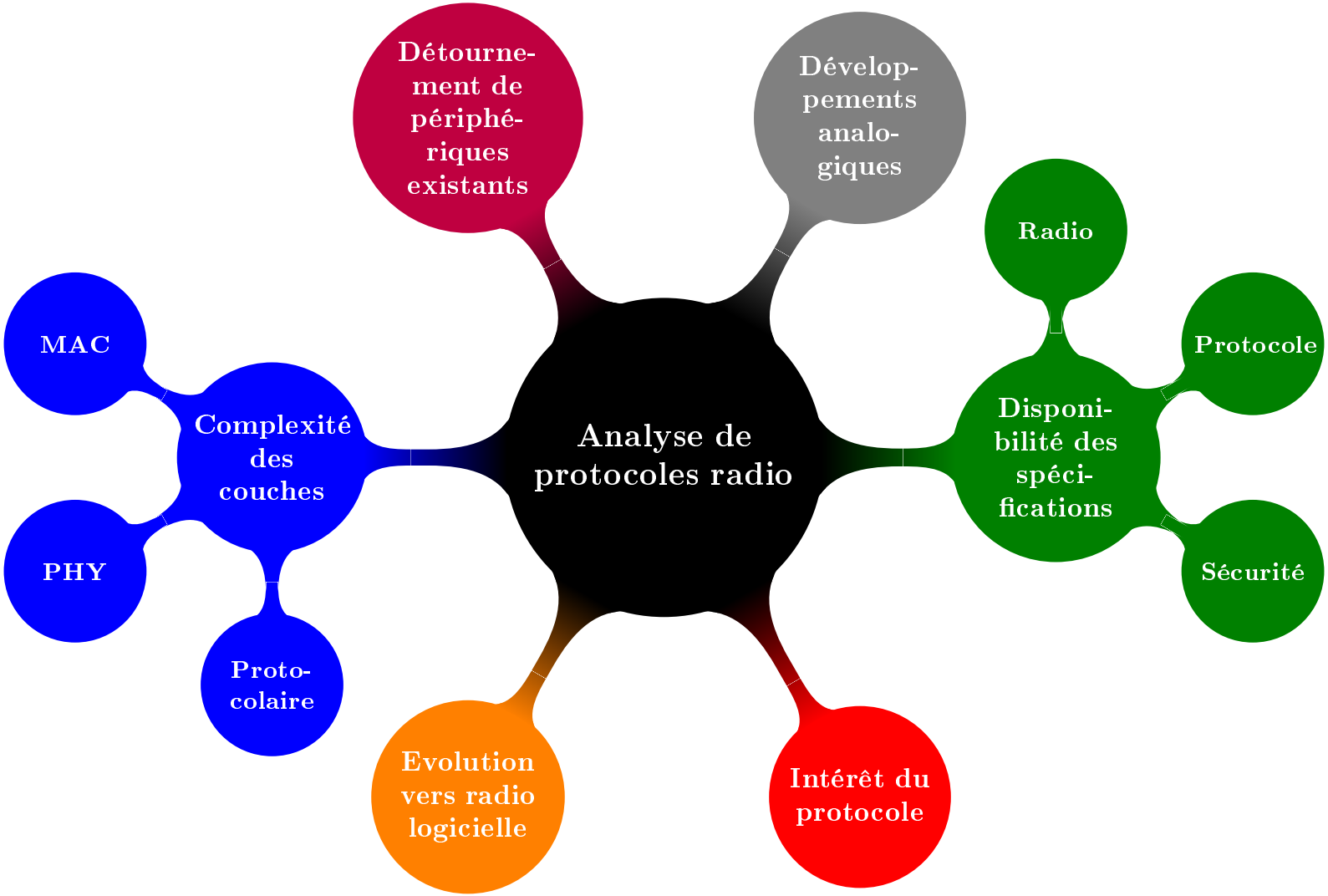
Contexte

- Equipements de plus en plus connectés (SCADA, travail en mobilité, objets du quotidien)

Recommendations

- Sensiblisation des employés
- Formation des employés
- Gestion de risque
- Mise en place d'un plan de continuité d'activité

Critères impactant la méthode d'analyse



Questions ?

Références I

[KasmiMorin2011] C. Kasmi et B. Morin **"Etat des lieux de la sécurité des réseaux de téléphonie mobile"**, Novembre 2011, C&ESAR 2011