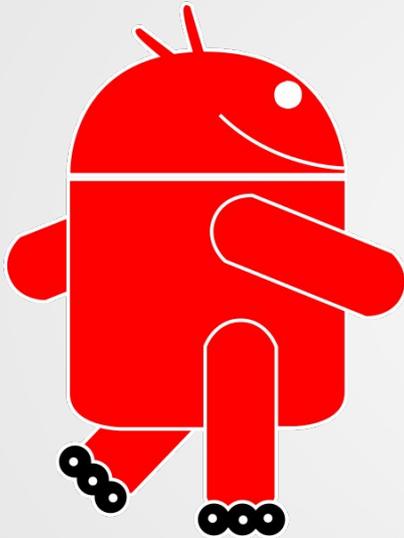


# Replicant: appareils mobiles et logiciel libre



**Replicant**

Paul Kocialkowski  
paulk@replicant.us

Samedi 15 novembre 2014

# Appareils mobiles

Les appareils mobiles sont **partout** : téléphones, tablettes...

Ces appareils sont de vrais ordinateurs :

- Matériel puissant
- Systèmes d'exploitation, mises à jour
- Applications

Appareils de communication et logiciels :

- Premiers téléphones: matériel
- Téléphones fixes actuels : micro-codes
- *Téléphones mobiles* : micro-codes
- *Smartphones* : systèmes d'exploitation

Le logiciel libre arrive à la portée de ces appareils !

# Appareils mobiles : introduction

Pourquoi se soucier de notre **liberté** ? Parce-que nous pouvons !

Raisons éthiques :

- Garder le contrôle plutôt qu'être contrôlé  
4 **libertés** fondamentales du logiciel libre
- Aider sa **communauté**
- **Confiance** et **sécurité** pour les **données** et **communications**
- Contrôler les informations qu'il **collecte**

# Appareils mobiles : introduction

Pourquoi se soucier de notre **liberté** ? Parce-que nous pouvons !

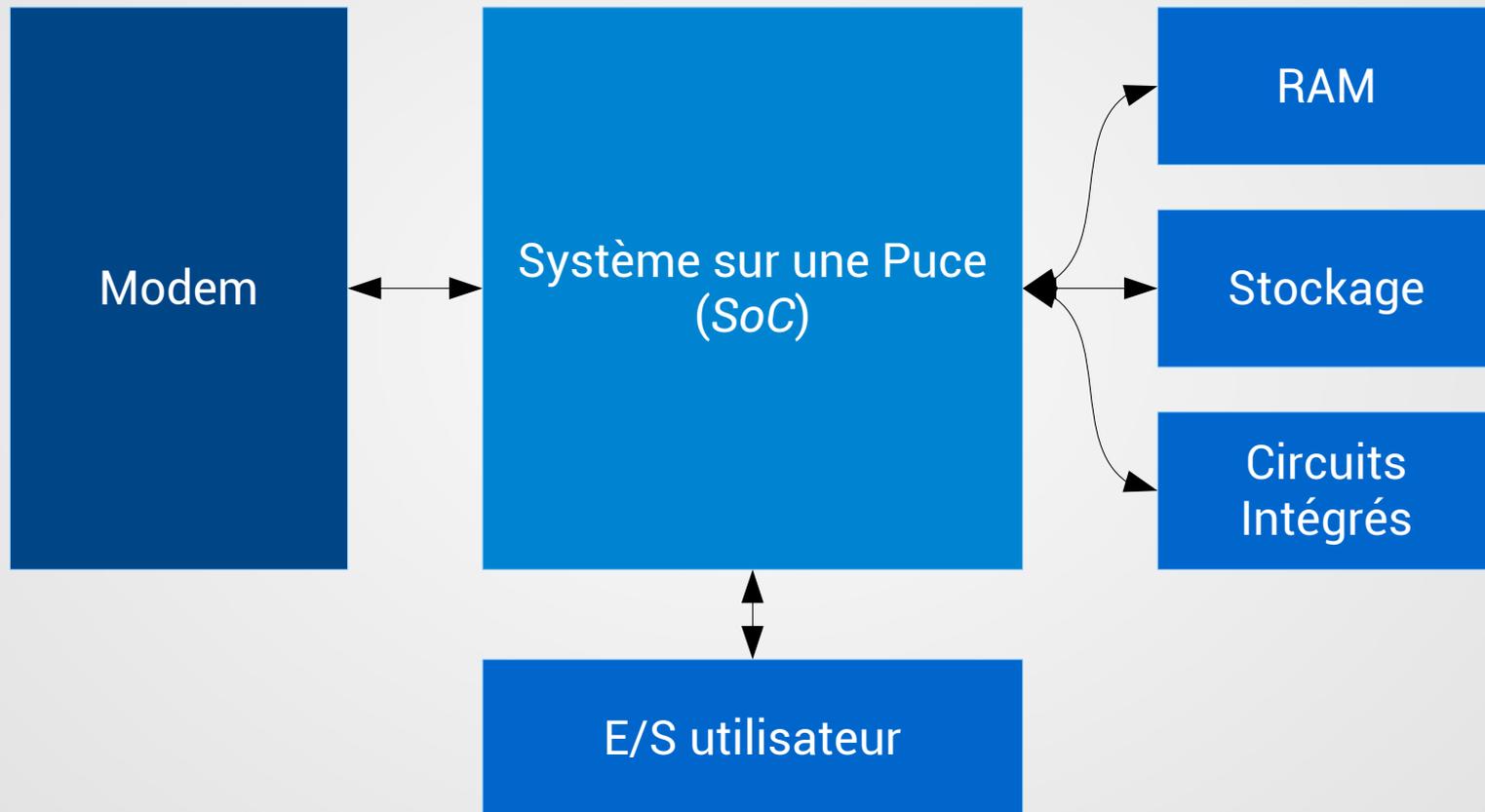
Raisons éthiques :

- Garder le contrôle plutôt qu'être contrôlé  
4 **libertés** fondamentales du logiciel libre
- Aider sa **communauté**
- **Confiance** et **sécurité** pour les **données** et **communications**
- Contrôler les informations qu'il **collecte**

Raisons **techniques** :

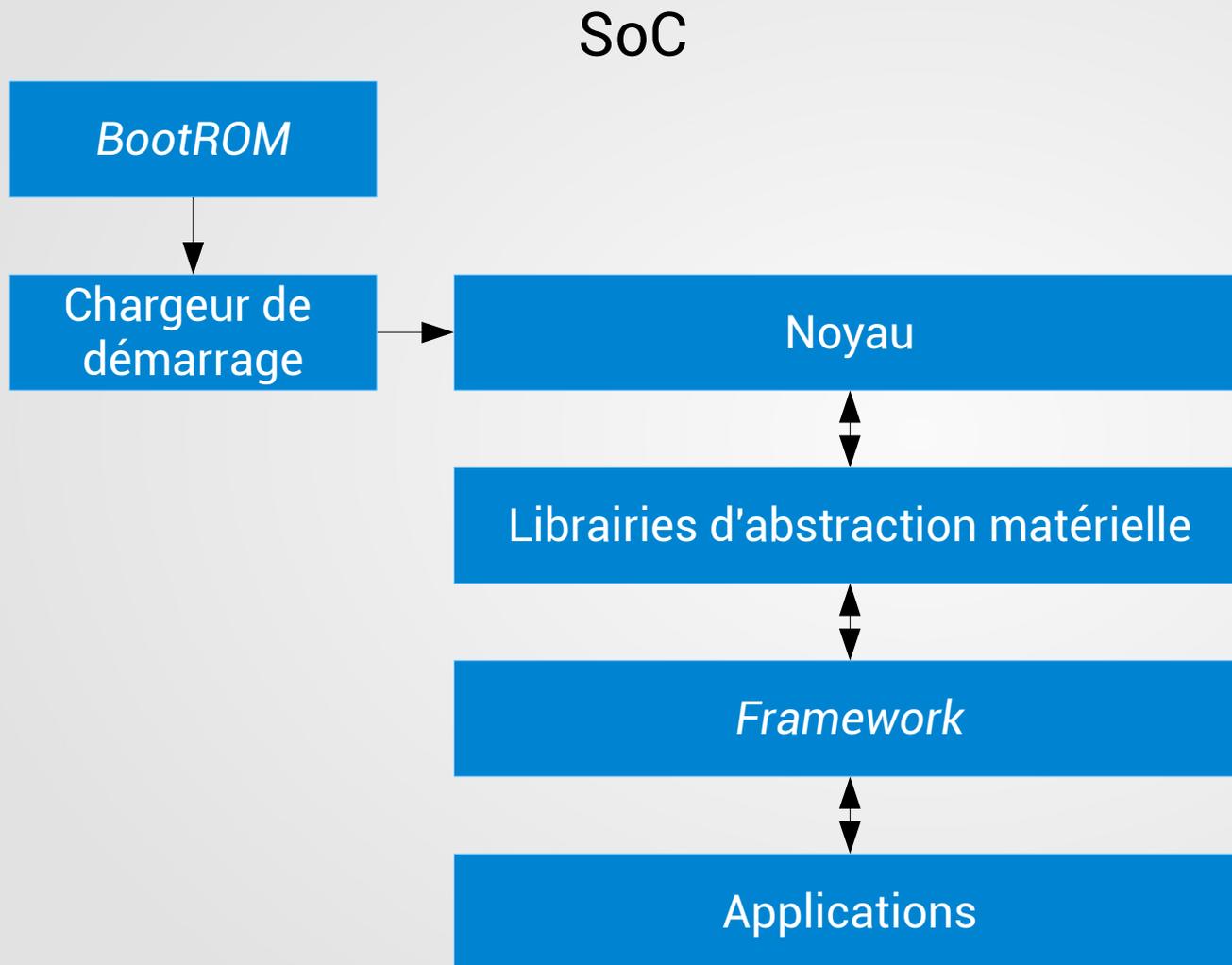
- **Adapter** le logiciel pour ses besoins
- Suivre les changements d'interfaces, les **nouvelles versions**

# Appareils mobiles : synthèse simplifiée



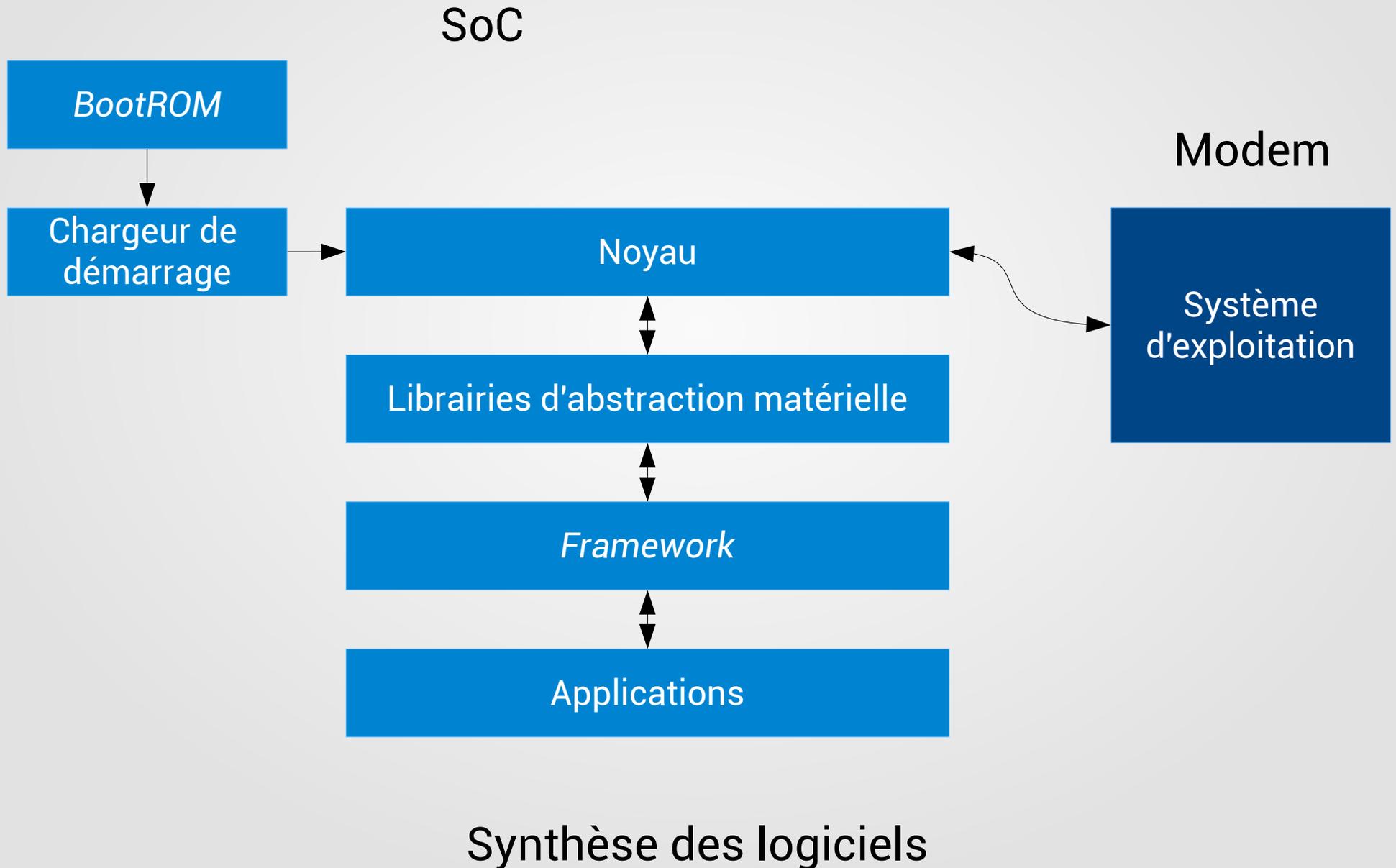
Synthèse du matériel

# Appareils mobiles : synthèse simplifiée

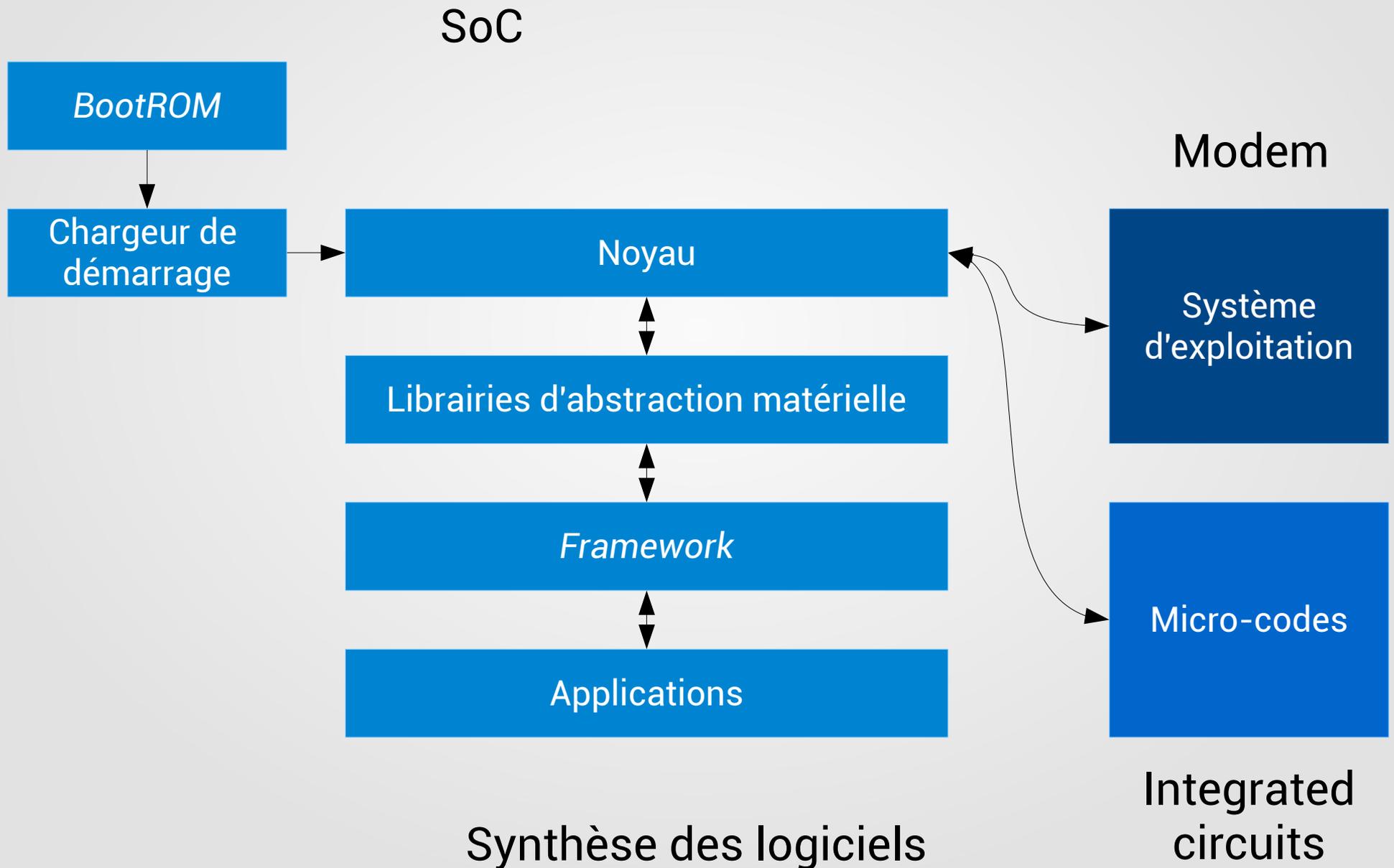


Synthèse des logiciels

# Appareils mobiles : synthèse simplifiée



# Appareils mobiles : synthèse simplifiée



# Scénario idéal

Liberté complète sur appareils mobiles :

- ✓ **Matériel libre**
- ✓ **Micro-codes libres**
- ✓ **Système du modem libre**
- ✓ **Bootrom et chargeur de démarrage libre**
- ✓ **Système et applications libres**

# Scénario idéal

Liberté complète sur appareils mobiles :

- ✓ **Matériel libre**
- ✓ **Micro-codes libres**
- ✓ **Système du modem libre**
- ✓ **Bootrom et chargeur de démarrage libre**
- ✓ **Système et applications libres**

Garanties des opérateurs de téléphonie mobile :

- ✓ Accès **neutre** à Internet
- ✓ Pas **d'interception** des données
- ✓ Pas de collecte des **positions** des utilisateurs

... mais quelle est la réalité aujourd'hui ?

# Opérateurs de téléphonie mobile

Opérateurs de téléphonie mobile :

- x Appliquent souvent des **filtres** sur leurs réseaux de données mobiles
- x Gardent trace des **messages** et **appels**
- x Collectent souvent la **position en temps réel** des utilisateurs
- x Offrent souvent accès aux **agences de renseignement**

Tout ceci dépend de **l'opérateur**, du **pays**, du **gouvernement**.

# Opérateurs de téléphonie mobile

Opérateurs de téléphonie mobile :

- x Appliquent souvent des **filtres** sur leurs réseaux de données mobiles
- x Gardent trace des **messages** et **appels**
- x Collectent souvent la **position en temps réel** des utilisateurs
- x Offrent souvent accès aux **agences de renseignement**

Tout ceci dépend de **l'opérateur**, du **pays**, du **gouvernement**.

En résumé :

- Situation mauvaise
- Tendance à l'empirer
- Peu de solutions techniques
- Exigez le changement !

# Matériel libre

Le matériel libre n'existe pas aujourd'hui, ou à peine :

- Modifier du matériel est presque **impossible** (nouvelle fournée)
- Les **circuits imprimés** ont parfois des plans (Arduino)
- Produire un circuit imprimé d'appareil mobile coûte **cher**
- Les **circuits intégrés** ne sont pas du matériel libre

En résumé :

- Le matériel tout à fait libre n'existe pas encore
- Quand partiellement possible, jamais aussi simple que :  
*gcc -o code code.c*

# Micro-codes

À propos des circuits intégrés :

- Micro-codes **propriétaires** : majorité des circuits intégrés
- Pas toujours possible de les remplacer ( $\simeq$  matériel ?)
- Micro-codes libres **difficiles** à écrire
- Micro-codes libres existent pour du **matériel spécifique** :  
exemples : Arduino, BusPirate, Milkymist One
- Micro-codes **libérés** par le **constructeur** :  
exemple : **ath9k\_htc**

En résumé :

- La plupart des micro-codes sont **propriétaires**
- La situation progresse **très lentement**

# Systeme du modem

Systeme du modem :

- Systematiquement **proprietaire**
- Pile GSM libre : **OsmocomBB**
- **Vieux** appareils prise en charge
- OsmocomBB a besoin d'un **ordinateur hôte**
- Certification du logiciel et reseaux publics



# Systeme du modem

Systeme du modem :

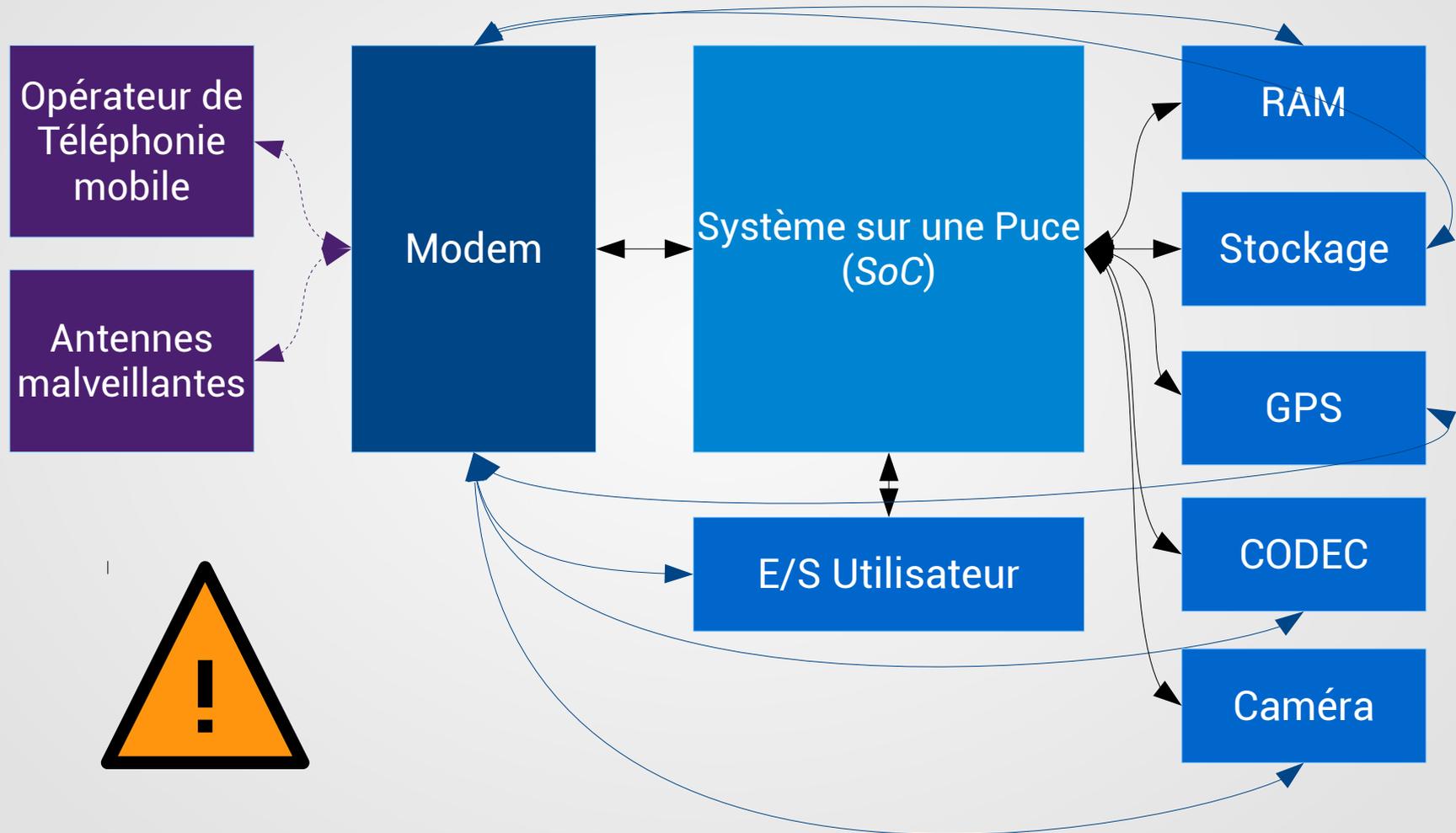
- Systematiquement **proprietaire**
- Pile GSM libre : **OsmocomBB**
- **Vieux** appareils prise en charge
- OsmocomBB a besoin d'un **ordinateur hôte**
- Certification du logiciel et reseaux publics



Composant crucial pour la **vie privée/sécurité** :

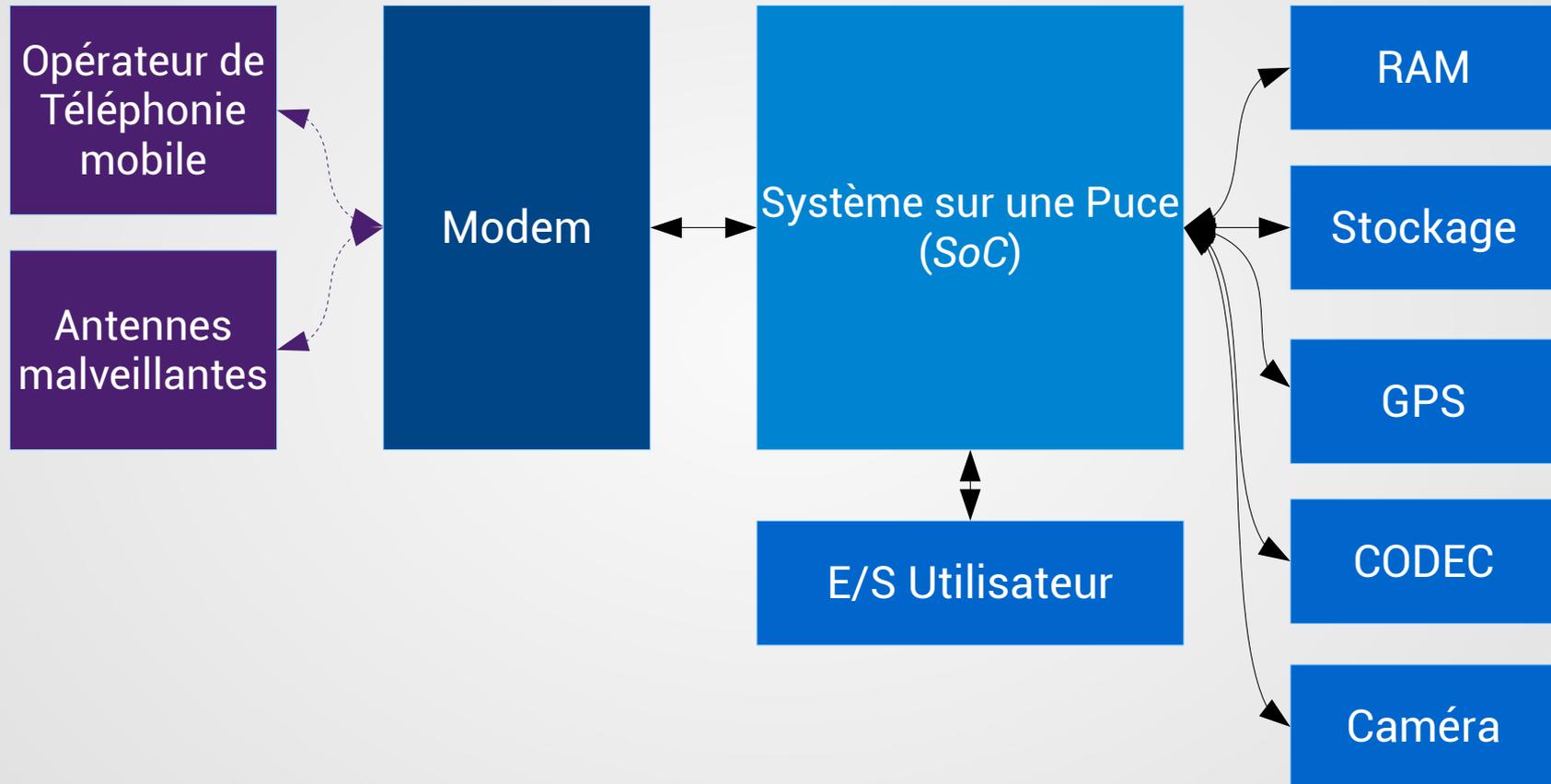
- **Quasiment toujours** connecté au reseau GSM
- **Contrôle à distance**
- **Accès direct** à certains composants **critiques**

# Isolation du modem



Mauvaise isolation du modem

# Isolation du modem



Bonne isolation du modem

# Isolation du modem

Solution de contournement : l'isolation du modem

- Vérifier qu'il n'a pas accès à **plus que le nécessaire**
- Vérifier qu'il ne peut pas être utilisé pour **espionner**
- Ne résout pas les problèmes de **liberté**
- Autres moyens **d'espionner** l'utilisateur

Problème : comment vérifier l'**isolation** ?

- **Documentation** fuitée
- Indices d'une **mauvaise situation** : noyau Linux, documentation, tout-en-un
- Pas de **hardware libre** !
- Bonne foi et **confiance**

# Isolation du modem

En résumé :

- Les **smartphones** exécutent un logiciel **propriétaire** sur le modem
- Situation **difficile** à améliorer
- **Isolation** du modem : utile mais **fiabilité** difficile
- Éviter les mauvaises plate-formes

À propos des **téléphones mobiles simplistes** :

- Isolation du modem **inexistante**
- Logiciels **propriétaires partout**

# BootROM, chargeur de démarrage

À propos du processeur principal :

- *BootROM* : propriétaire, pas remplaçable ( $\simeq$  matériel ?)
- Chargeur de démarrage : situation **différente** selon la **plate-forme**
- Plusieurs **étages** de chargeurs de démarrage
- Vérifications de **signatures**, clés **pas remplaçables**

Exemples de bonnes plate-formes :

- Freescale i.MX
- Allwinner Ax (quand pris en charge par la communauté)
- TI OMAP (GP), nVidia Tegra (non-ODM)

En résumé :

- De bonnes plate-formes existent
- Vérifications de **signatures** très communes
- Chargeurs de démarrage propriétaires pour la plupart des appareils

# Systeme d'exploitation

Le systeme d'exploitation coordonne l'ensemble :

- Accès à chaque **circuit intégré** (E/S, caméra, microphone, GPS)
- Accès aux **données** de l'utilisateur
- Prend en charge les **communications** de l'utilisateur

Point le plus critique pour la vie privée/sécurité !

- Interaction directe avec l'utilisateur  
modifications, compréhension, améliorations
- Détient le savoir du fonctionnement du matériel

Donc très important pour la liberté !

# Systeme d'exploitation

Systemes d'exploitation pour appareils mobiles :

Systemes plutot libres :

- Android
- Firefox OS
- Ubuntu Touch
- Tizen
- Open webOS

Systemes plutot proprietaires :

- Apple iOS
- Windows Phone

# Systeme d'exploitation

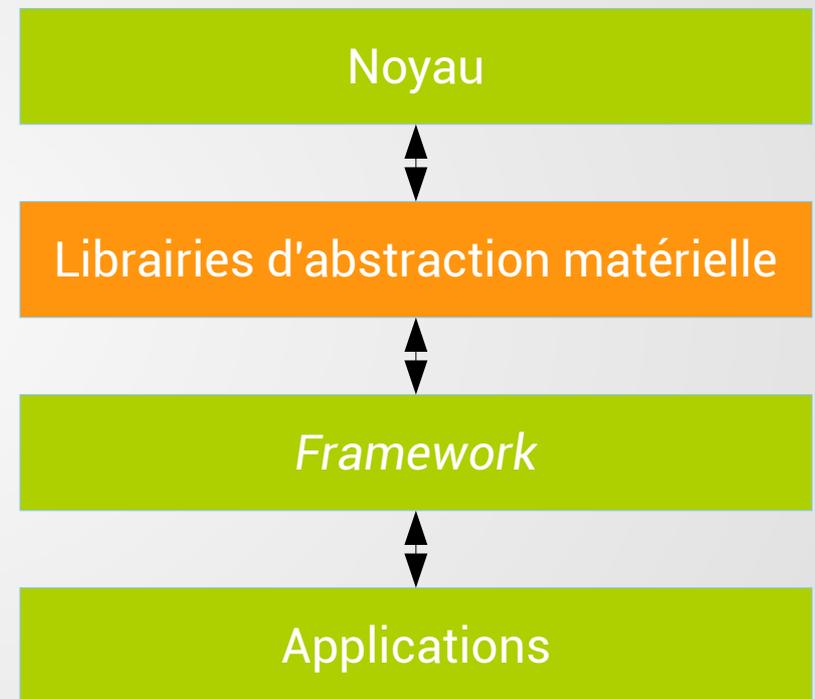
Systemes d'exploitation pour appareils mobiles :

Systemes plutot libres :

- Android
- Firefox OS
- Ubuntu Touch
- Tizen
- Open webOS

Sur la plupart d'entre eux :

- Noyau Linux
- *Drivers* proprietaires
- *Framework* libre
- Applications de base libres
- Diverses applications libres



Composants libres

Composant proprietaire

# Situation actuelle

Résumé de la situation actuelle :

- x Pas de matériel libre
- x Micro-codes propriétaires dans les circuits intégrés
- x Systèmes de modems propriétaires
- x *Bootroms* propriétaires
- ✓ Isolation du modem (fiabilité difficile)
- ✓ Chargeurs de démarrage libres et non-signés
- ✓ Systèmes essentiellement libres
- ✓ Applications libres

La situation est imparfaite :

- Si on veut une liberté sans compromis ou qu'une activité sérieuse est en jeu : mieux vaut **ne pas utiliser d'appareil téléphonique mobile**
- Sinon, il faut accepter des **compromis**

# Faire progresser la situation

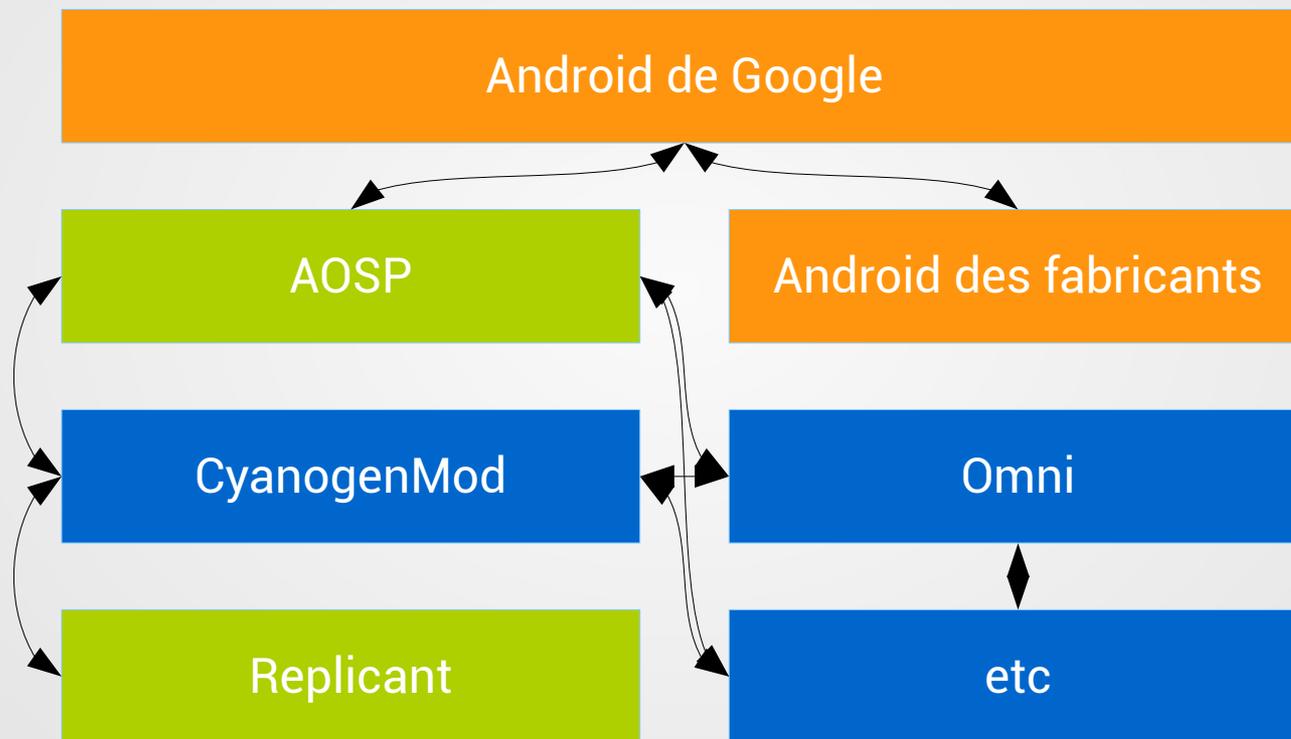
Plutôt que de laisser tomber, faisons progresser la situation !

En 2008 : Openmoko FreeRunner, Google/HTC Dream :



# Vision plus détaillée d'Android

Android est véritablement une famille de systèmes d'exploitation :



Versions propriétaires d'Android

Versions plutôt libres d'Android

Versions entièrement libres d'Android

# Vision plus détaillée d'Android

À propos de du projet Open Source Android (AOSP) :

- AOSP est presque entièrement libre
- AOSP prend partiellement en charge les appareils Nexus de Google
- AOSP ne peut pas être exécuté tel quel sur les appareils

Pour fonctionner sur les appareils :

- Des programmes (démons, bibliothèques d'abstraction matérielle) et des micro-codes propriétaires sont nécessaires

Versions communautaires d'Android :

- Incluent souvent les programmes et micro-codes propriétaires
- Incluent parfois des applications propriétaires
- Encouragent parfois les applications propriétaires de Google
- Incluent parfois des fonctionnalités *malveillantes*

# Introduction à Replicant

Idées à la base de Replicant :

- Faire d'Android un système entièrement libre
- Garder un système utilisable (fluidité, audio, téléphonie)
- Remplacer ou supprimer les parties propriétaires
- Ne pas encourager l'utilisation de logiciels propriétaires
- Désactiver les fonctionnalités malveillantes

# Introduction à Replicant

Idées à la base de Replicant :

- Faire d'Android un système entièrement libre
- Garder un système utilisable (fluidité, audio, téléphonie)
- Remplacer ou supprimer les parties propriétaires
- Ne pas encourager l'utilisation de logiciels propriétaires
- Désactiver les fonctionnalités malveillantes

Techniquement :

- Commencé comme un dérivé d'AOSP
- Maintenant basé sur CyanogenMod (pris en charge des appareils)
- Distribué avec F-Droid, un dépôt d'applications libre



# Développement de Replicant

Développement de Replicant:

- Mené par un développeur, sur le temps libre
- Nettoyage du code source de CyanogenMod pour Replicant : fonctionnalités malveillantes, adaptation pour les fonctionnalités
- Faire fonctionner le matériel, avec peu de documentation
- Différents aspects : **audio, caméra, modem, capteurs**

Essentiel du travail sur Replicant : ingénierie inverse

- Comprendre le fonctionnement des composants propriétaires et du matériel
- Écrire des remplacements libres

Tâches complexes que Replicant ne prend pas en charge :

- Accélération graphique (Freedreno, Lima)
- Micro-codes
- Système du modem

# Développement de Replicant

Au fil du temps, plusieurs remplacements libres ont été écrits :

- **RIL** (30000 lignes, 9 appareils)
- **Caméra** (5500-10000 lignes, 2 appareils)
- **Audio** (4500 lignes, 3 appareils)
- **Capteurs** (3000-4000 lignes, 8 appareils)

Coopération avec d'autres communautés (e.g. teamhacksung)

- Inclusion des remplacements
- Intégration du travail de Replicant dans e.g. CyanogenMod
- Meilleur pour la liberté
- Souvent meilleur techniquement
- Nouvelles versions d'Android

# Prise en charge par Replicant

À ce jour, Replicant 4.2 prend en charge 12 appareils différents !

- Fonctionnalités et apparence héritées de CyanogenMod
- Essentiellement des appareils Google Nexus et Samsung Galaxy
- Utilisable au quotidien, avec des fonctionnalités manquantes

Samsung Galaxy S 2 (I9100), Galaxy Note (N7000), Galaxy Nexus (I9250), Galaxy Tab 2 7.0 (P3100), Galaxy Tab 2 10.1 (P51xx), Galaxy S 3 (I9300), Galaxy Note 2 (N7100) :

- Chargeurs de démarrage propriétaires et signés
- Isolation du modem supposément bonne

Nexus S (I902x), Galaxy S (I9000):

- Chargeurs de démarrage propriétaires et signés
- Mauvaise isolation du modem

# Prise en charge par Replicant

À ce jour, Replicant 4.2 prend en charge 12 appareils différents !

- Fonctionnalités et apparence héritées de CyanogenMod
- Essentiellement des appareils Google Nexus et Samsung Galaxy
- Utilisable au quotidien, avec des fonctionnalités manquantes

Goldelico GTA04 :

- Chargeur de démarrage libre
- Isolation du modem supposément bonne
- Début de prise en charge par Replicant
- Travail en cours
- Protocoles bien documentés

# Replicant

Prochaines images de Replicant 4.2 :

- Réécriture de Samsung-RIL (stabilité)
- Corrections de sécurité

Un aperçu du futur de Replicant :

- Rester à la version 4.2 pendant un moment
- Concentration des efforts sur les appareils plus respectueux de la liberté : GTA04, P970 (Optimus Black)
- Prise en charge de tablettes Wi-Fi : Allwinner, Kindle Fire, Nexus 7
- Intégrer des améliorations pour la vie privée et la sécurité

Le projet a besoin de vous !

- Replicant mérite plus qu'un seul développeur
- Les dons sont bienvenus (les appareils coûtent cher)

# Replicant

En apprendre plus à propos de Replicant :

- Site web : <http://www.replicant.us/>
- Blog : <http://blog.replicant.us/>
- Wiki/tracker : <http://redmine.replicant.us/>

Rejoignez la communauté :

- Forums
- Liste de diffusion
- Canal IRC : #replicant chez freenode

Passez dire bonjour sur le stand Replicant !



*That's all Folks!*



Text and schematics:

- © 2013-2014 Paul Kocialkowski  
Creative Commons BY-SA 3.0 license

Images:

- **Replicant robot**, © Mirella Vedovetto, Paul Kocialkowski,  
Creative Commons BY-SA 3.0 license
- **Openmoko Neo FreeRunner**, © FIC/OpenMoko,  
Creative Commons BY-SA 3.0 license
- **HTC Dream**, © Paul Kocialkowski  
Creative Commons BY-SA 3.0 license
- **F-Droid logo**, © William Theaker, Robert Martinez  
Creative Commons BY-SA 3.0 license