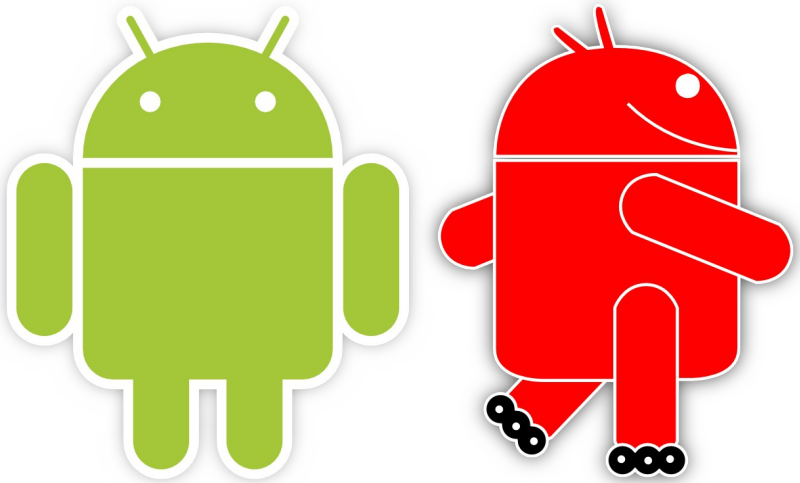
Libérer son Android : un aperçu du développement de Replicant



Paul Kocialkowski
paulk@replicant.us

Giroll Party Automne — Samedi 23 Novembre 2013

I. Téléphones portables et liberté

Présentation des appareils

Constat : téléphones portables et tablettes numériques sont de **véritables ordinateurs** !

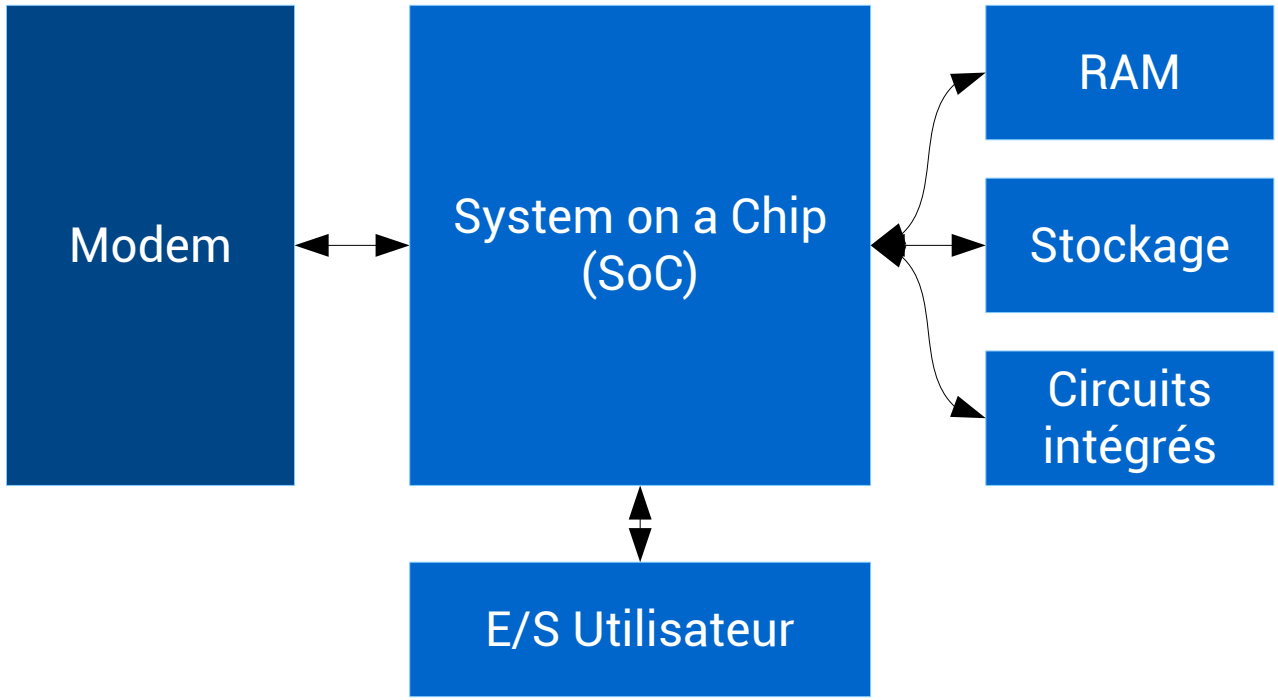
- Systèmes d'exploitation **complets**
- **Installation** de logiciels
- **Mises à jour** du système
- **Matériel** comparable

On ne peut donc ignorer la question du **logiciel libre** !

I. Téléphones portables et liberté

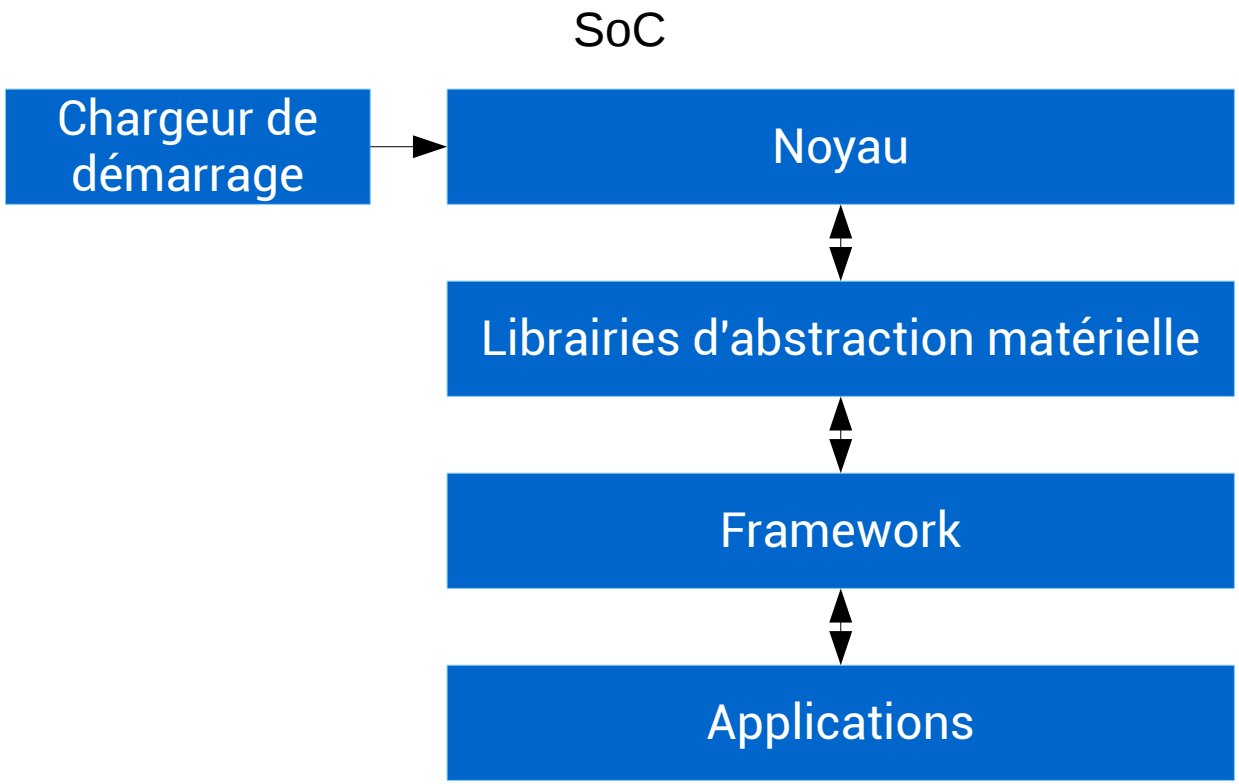
Présentation des appareils

Schéma simplifié de ces appareils :



Représentation côté matériel

Schéma simplifié de ces appareils :

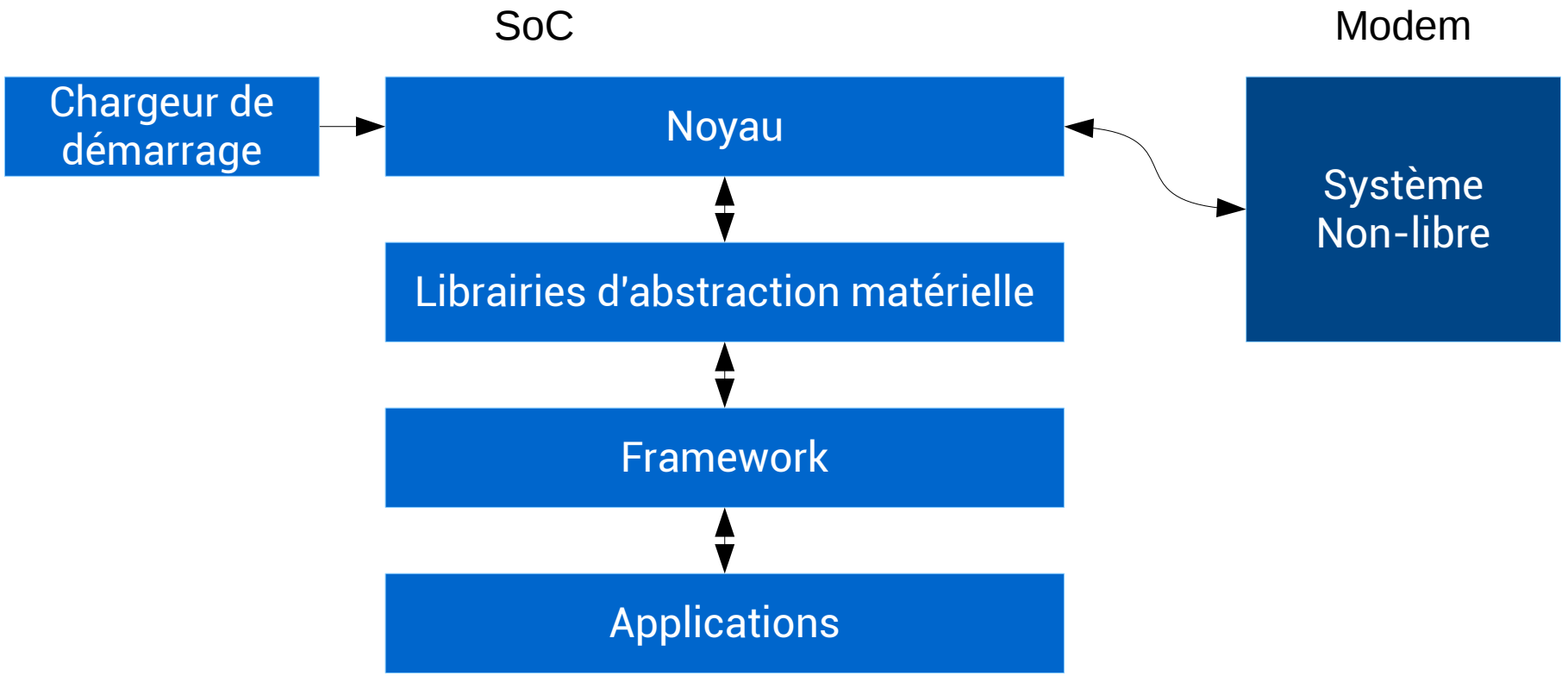


Représentation côté logiciel

I. Téléphones portables et liberté

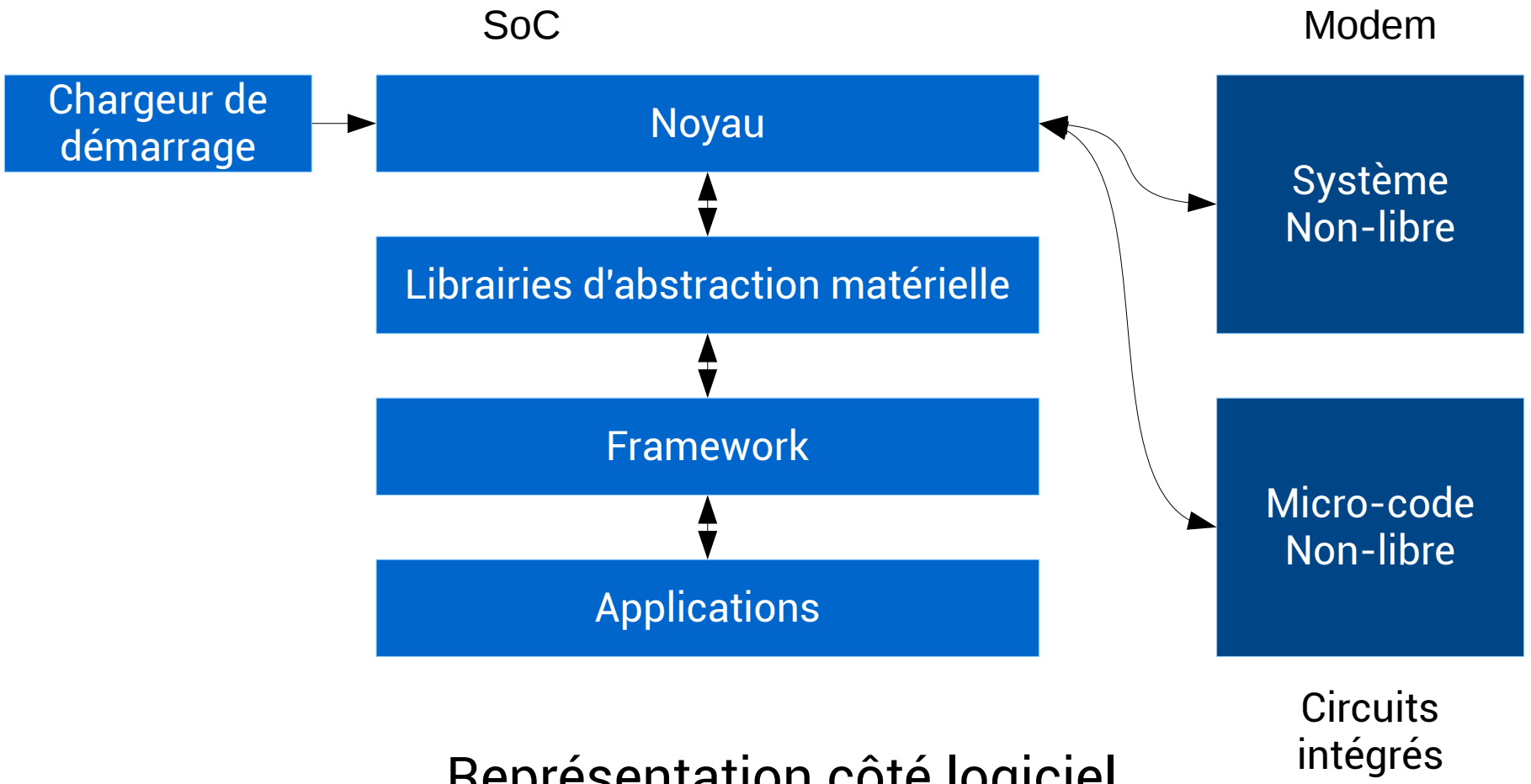
Présentation des appareils

Schéma simplifié de ces appareils :



Représentation côté logiciel

Schéma simplifié de ces appareils :



Représentation côté logiciel

I. Téléphones portables et liberté

Intérêt du logiciel libre

Importance du logiciel libre sur nos téléphones portables et tablettes numériques ?

Raisons d'ordre éthique :

- **Contrôler** son informatique :
  libertés essentielles du logiciel libre
- Garantir la **sécurité** des **données** et des **communications**
- **Contrôle des informations** que collecte le téléphone

I. Téléphones portables et liberté

Intérêt du logiciel libre

Importance du logiciel libre sur nos téléphones portables et tablettes numériques ?

Raisons d'ordre éthique :

- **Contrôler** son informatique :
  libertés essentielles du logiciel libre
- Garantir la **sécurité** des **données** et des **communications**
- **Contrôle des informations** que collecte le téléphone

Raisons techniques pratiques :

- **Adapter** les logiciels à des systèmes divers et variés
- Suivre les **changements de version et d'interface** du système

I. Téléphones portables et liberté

État des lieux et remédiations

Appareil **idéal**, dans le meilleur des mondes :

- ✔ **Matériel** libre
- ✔ **Micro-codes** libres
- ✔ **Système du modem** libre
- ✔ **Chargeur de démarrage** libre
- ✔ **Système** libre

I. Téléphones portables et liberté

État des lieux et remédiations : situation idéale

Appareil **idéal**, dans le meilleur des mondes :

- ✔ **Matériel** libre
- ✔ **Micro-codes** libres
- ✔ **Système du modem** libre
- ✔ **Chargeur de démarrage** libre
- ✔ **Système** libre

Garanties de la part des **opérateurs de téléphonie mobile** :

- ✔ Accès **neutre** au réseau
- ✔ Pas **d'interception des données** transmises
- ✔ Pas de collecte de la **position** des utilisateurs

Le tout assorti d'un cadre légal bien défini.

I. Téléphones portables et liberté

État des lieux et remédiations : opérateurs de téléphonie mobile

En pratique aujourd'hui, la situation est loin d'être idéale.

Opérateurs de téléphonie mobile :

- ✗ **Filtrent** leurs réseaux de données
- ✗ Gardent trace de tous les **messages** et **appels**
- ✗ **Collectent** et **fournissent aux gouvernements** la **position** des utilisateurs en temps réel

Degré plus ou moins élevé selon :

- Opérateur
- Pays
- Gouvernement

Tendance : **mise en place** de tels dispositifs

I. Téléphones portables et liberté

État des lieux et remédiations : microcode libre

En pratique aujourd'hui, la situation est loin d'être idéale.

Micro-codes :

- Micro-codes **pas libres** pour la **quasi-totalité** des circuits intégrés
- Pas forcément possible de **remplacer** le micro-code
- Micro-codes **libres** techniquement très **complexes** à écrire
- Projet de micro-codes **libres** pour un **matériel spécifique**
  Exemples : Aruduino, BusPirate, Milkymist One
- Micro-code **libéré** par le **constructeur** du matériel :
  Exemple : **ath9k_htc**

I. Téléphones portables et liberté

État des lieux et remédiations : système du modem libre

En pratique aujourd'hui, la situation est loin d'être idéale.

Système du modem :

- Pile GSM libre sur les téléphones : **OsmocomBB**
- Téléphones pris en charge déjà **vieux**
- **OmsocomBB** nécessite un **ordinateur** pour fonctionner
- Certification du logiciel et utilisation sur réseaux publiques

I. Téléphones portables et liberté

État des lieux et remédiations : système du modem libre

En pratique aujourd'hui, la situation est loin d'être idéale.

Système du modem :

- Pile GSM libre sur les téléphones : **OsmocomBB**
- Téléphones pris en charge déjà **vieux**
- **OmsocomBB** nécessite un **ordinateur** pour fonctionner
- Certification du logiciel et utilisation sur réseaux publiques

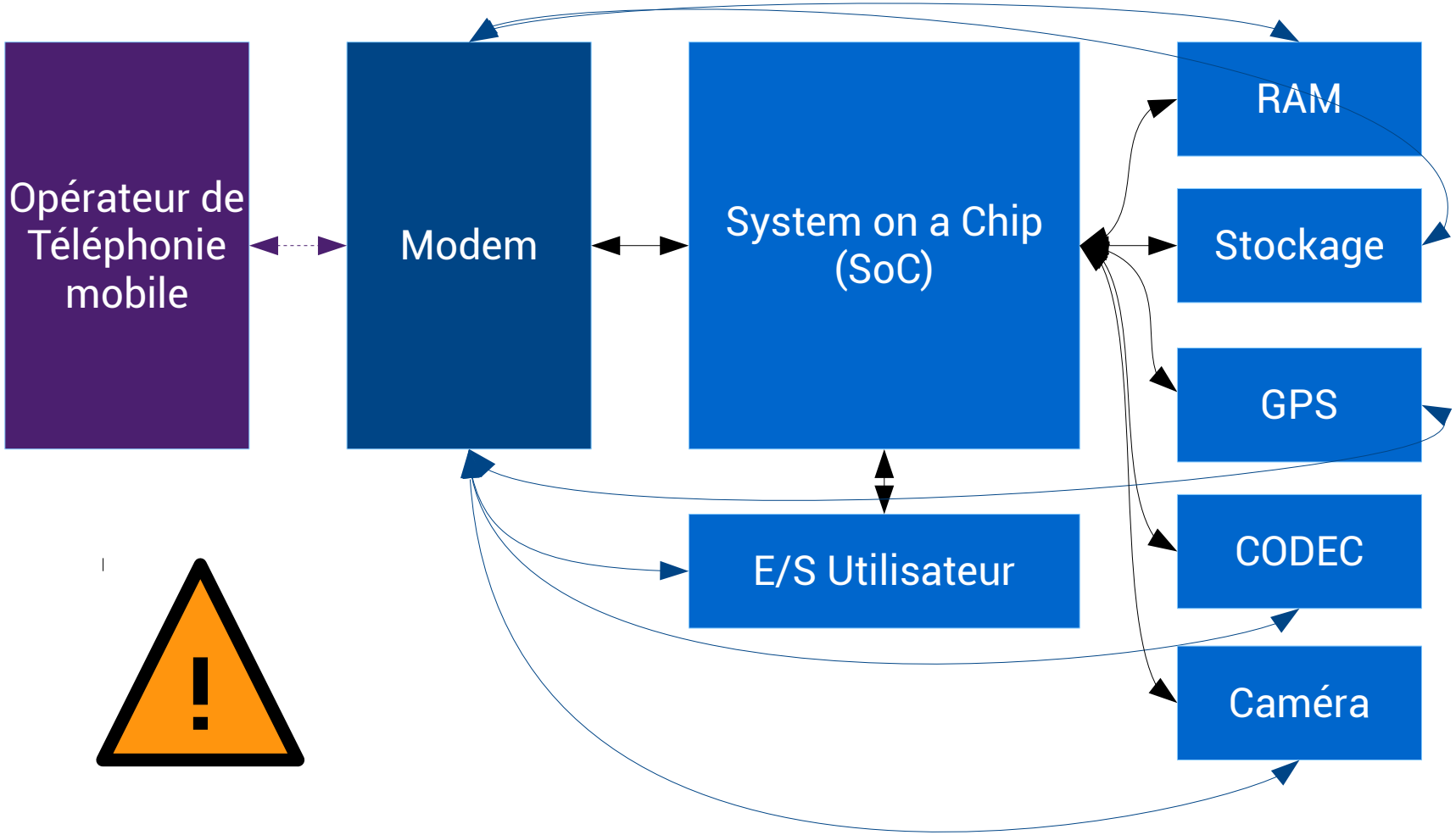
Pourtant, le **modem** est l'un des éléments les plus cruciaux pour la **sécurité** !

- Connecté **en permanence** au réseau GSM
- Peut être **contrôlé à distance**
- Peut potentiellement **accéder directement au matériel**

I. Téléphones portables et liberté

État des lieux et remédiations : système du modem libre

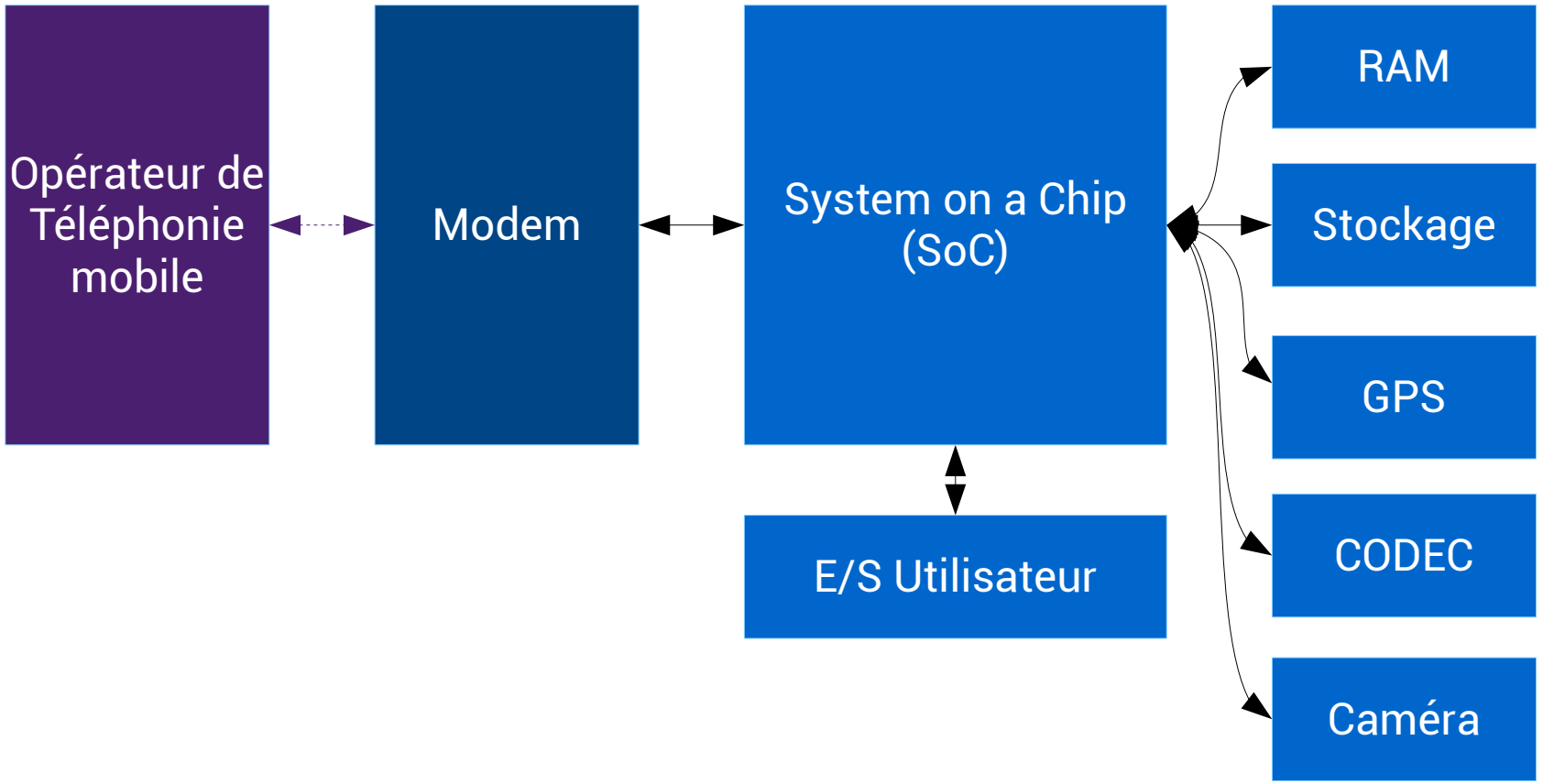
Mauvaise isolation du modem :



I. Téléphones portables et liberté

État des lieux et remédiations : système du modem libre

Bonne isolation du modem :



I. Téléphones portables et liberté

État des lieux et remédiations : chargeur de démarrage libre

En pratique aujourd'hui, la situation est loin d'être idéale.

Chargeurs de démarrage :

- Situation dépendante de la plateforme :

Plateforme	TI OMAP	Samsung Exynos	Qualcomm Snapdragon	Nvidia Tegra	Allwinner A1x
Chargeur primaire	Libre (X-Loader)	Non-libre	Non-libre	Non-libre	Libre
Chargeur secondaire	Libre (U-Boot)	Possible (U-Boot, Coreboot)	Non-libre	Possible (U-Boot)	Libre (U-Boot)
Signature	Dépend	Dépend	?	?	Non

I. Téléphones portables et liberté

État des lieux et remédiations : système libre

En pratique aujourd'hui, la situation est loin d'être idéale.

Plusieurs systèmes dits **libres** :

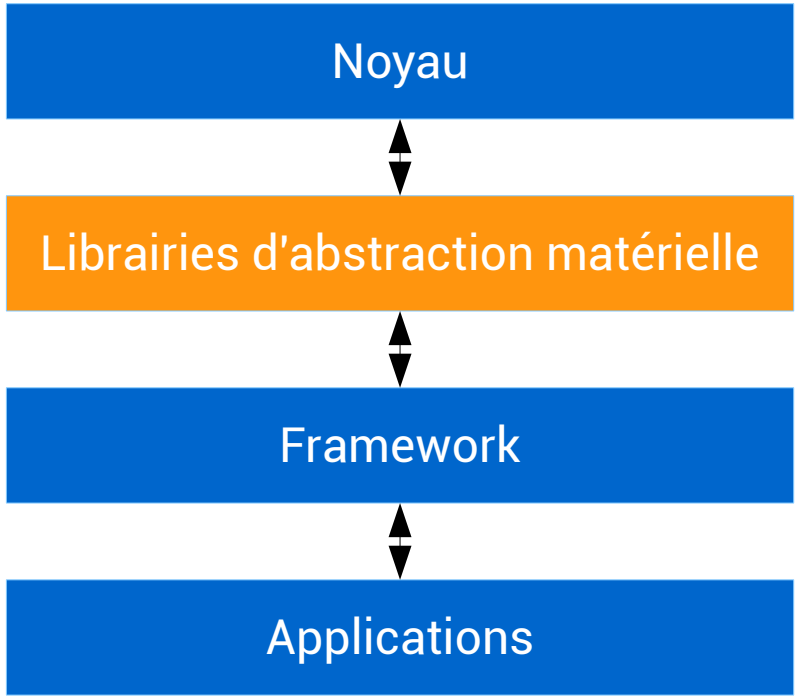
- Android
- Firefox OS
- Ubuntu Touch
- Tizen

En pratique aujourd'hui, la situation est loin d'être idéale.

Plusieurs systèmes dits **libres** :

- Android
- Firefox OS
- Ubuntu Touch
- Tizen

Composants propriétaires nécessaires pour que le système fonctionne !



Composants libres
Composants propriétaires

I. Téléphones portables et liberté

État des lieux et remédiations : bilan

Bilan de la situation actuelle du côté des appareils :

- ✗ Matériel non-libre
- ✗ Micro-codes non-libres
- ✗ Système du modem non-libre
- ✔ Isolation du modem possible
- ✔ Chargeur de démarrage libre et non-signé possible
- ✔ Système libre possible ?

Bilan général :

- Si vous tenez à votre liberté et sécurité sans compromis ou que les enjeux sont importants : **n'utilisez pas de téléphone portable !**
- Sinon, il est nécessaire de faire des compromis

I. Téléphones portables et liberté

À la recherche d'un système libre

Situation en 2008 :

Projet OpenMoko :

- Matériel libre en partie
- Modem isolé
- Chargeur de démarrage libre
- Systèmes GNU/Linux entièrement libres

Openmoko GTA02
FreeRunner

I. Téléphones portables et liberté

À la recherche d'un système libre

Situation en 2008 :

Projet OpenMoko :
- Matériel libre en partie
- Modem isolé
- Chargeur de démarrage libre
- Systèmes GNU/Linux entièrement libres

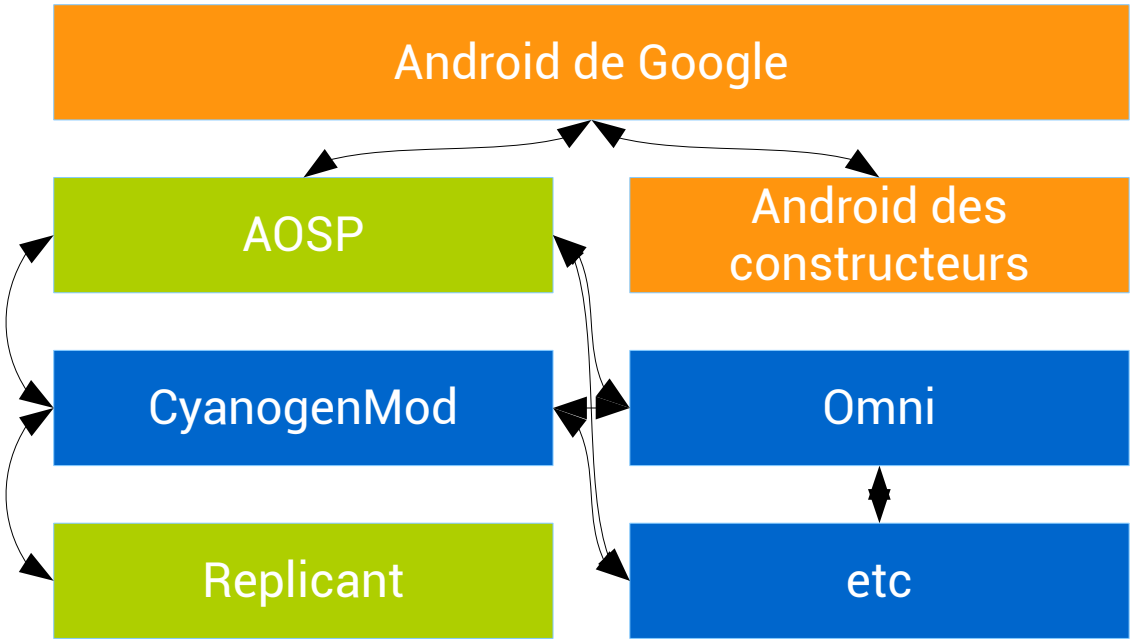
Android et le HTC Dream/Google G1/ADP1
- Chargeur de démarrage propriétaire
- Modem pas isolé du tout
- Système AOSP libre (android.git.kernel.org)
- Librairies d'abstraction matérielle propriétaires

Objectf : Libérer le HTC Dream. Replicant est né !

I. Téléphones portables et liberté

À la recherche d'un système libre

Android est une famille de systèmes d'exploitation mobiles :



Versions propriétaires d'Android
Versions open source d'Android
Versions entièrement libres d'Android

I. Téléphones portables et liberté

À la recherche d'un système libre

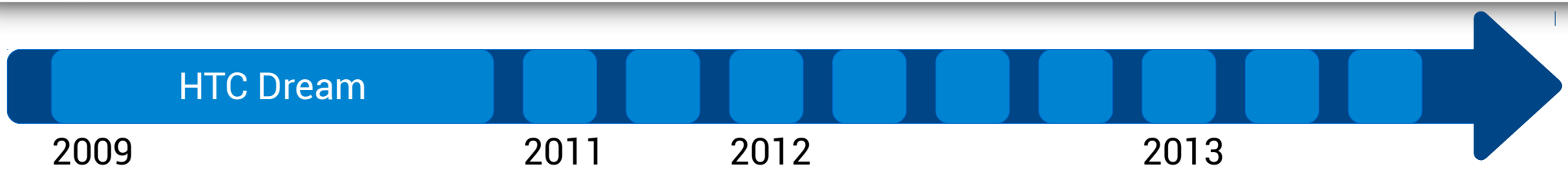
Replicant est un dérivé entièrement libre de CyanogenMod :

- Librairies d'abstraction matérielle remplacées ou évitées
- Micro-codes propriétaires pas distribués
- Fonctionnalités malveillantes désactivées

En plus d'un système libre, des applications libres avec F-Droid !

II. Développement de Replicant

Chronologie et challenges

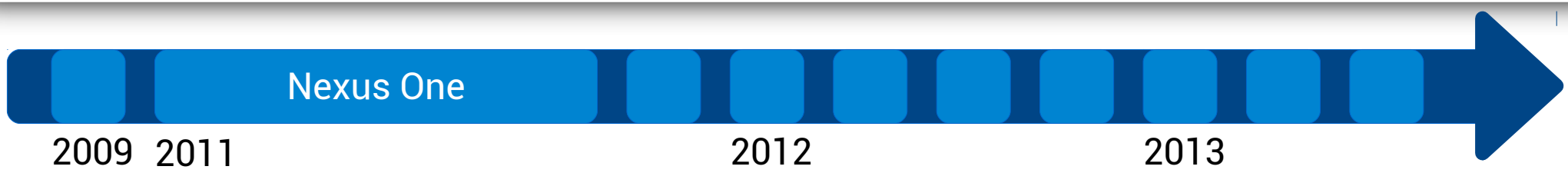


HTC Dream :

- Mauvaise isolation du **modem**
- **Chargeur de démarrage** non-libre
- **Microcodes** non-libres pour WiFi, bluetooth
- **Audio** : librairies en partie propriétaires
  Implémentations libres existantes et adapables
- **Modem** : protocole connu (AT)
  Implémentation libre de référence adaptable
- **GPS** : protocole connu (NMEA)
  Implémentation libre adaptable, problèmes
- Autres composans non pris en charge :
  3D, caméra, capteurs

II. Développement de Replicant

Chronologie et challenges



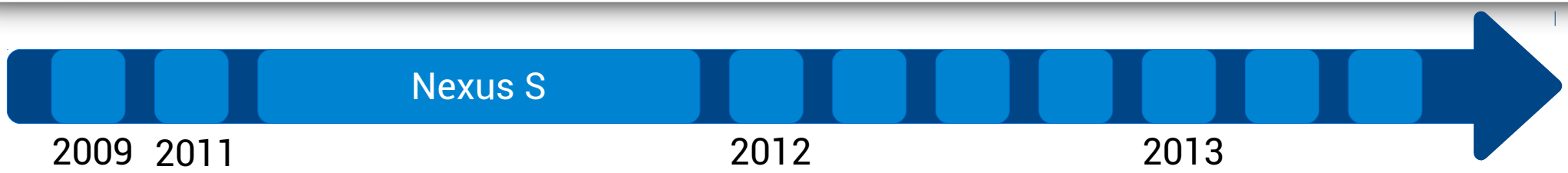
Nexus One :

- Mauvaise isolation du **modem**
- **Chargeur de démarrage** non-libre
- **Microcodes** non-libres pour WiFi, bluetooth et **audio**
- **Audio** : logiciel hérité du HTC Dream
- **Modem** : logiciel hérité du HTC Dream
- **GPS** : logiciel hérité du HTC Dream
- Autres composans non pris en charge : **3D, caméra**

- Premiers problèmes graphiques
- Implémentation libre existante en cherchant

II. Développement de Replicant

Chronologie et challenges

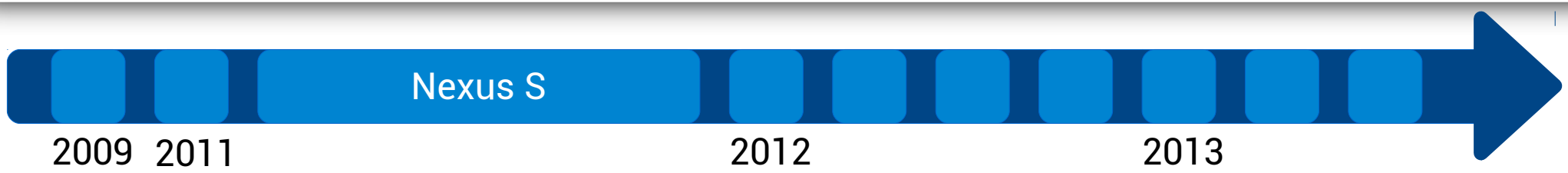


Nexus S :

- Isolation incomplète du **modem**
- **Chargeur de démarrage** non-libre et signé
- **Microcodes** non-libres pour WiFi, bluetooth, NFC, MFC
- Problèmes **graphiques** de plus en plus sérieux
- **GPS** : protocole inconnu
- **Capteurs** : en partie libre et en partie remplacé
- **Modem** : protocole de Samsung **sans documentation ni implémentation libre** !
- Autres composans non pris en charge : **accélération graphique, 3D, compas**

II. Développement de Replicant

Chronologie et challenges



Nexus S :

- **Modem** : Protocole de Samsung **sans documentation ni implémentation libre** !

Le défi principal a été la prise en charge du modem

- Librairie initiale pour le Samsung H1
- Démarrage du modem et transport
- Interface avec le système Android
- Collaboration entre développeurs (SHR, Replicant)

Après plusieurs mois de travail, le premier appel utilisant notre implémentation a pu être passé !

II. Développement de Replicant

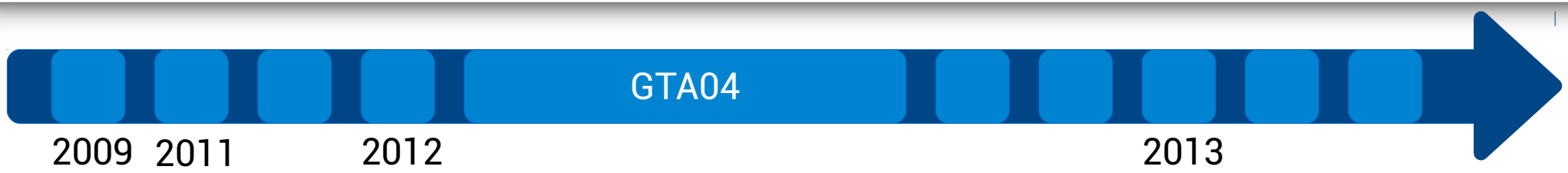
Chronologie et challenges

Galaxy S :

- Matériel similaire au **Nexus S**
- **Modem** : même protocole mais procédure de démarrage et transport différents
- Protocole non-standard pour « **flasher** » les images du système
- Implémentation libre côté ordinateur : **Heimdall**
- Port simple et **sans difficulté** particulière

II. Développement de Replicant

Chronologie et challenges



GTA04 :

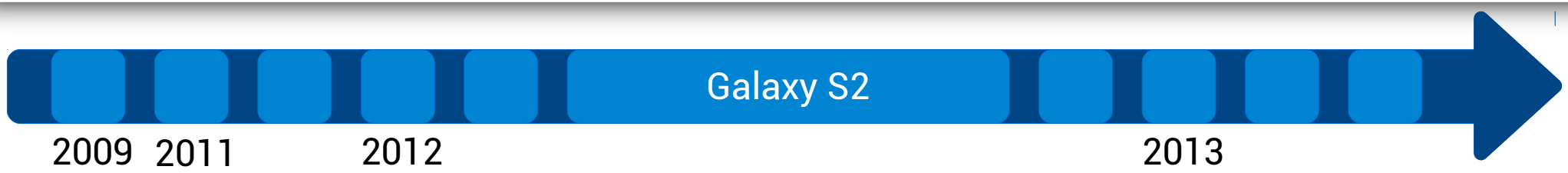
- Bonne isolation du modem
- Chargeurs de démarrage libres
- Microcode pour le WiFi
- Pas d'**accélération graphique** et **3D** libres
- Interfaces et protocoles standards pour :
  Audio, modem, caméra, GPS

Le Goldelico GTA04 est donc quasi-idéal, pourtant jusqu'à présent, le port de Replicant est un échec :

- Pas de version stable du noyau pour Android
- Beaucoup de code reste à écrire

II. Développement de Replicant

Chronologie et challenges

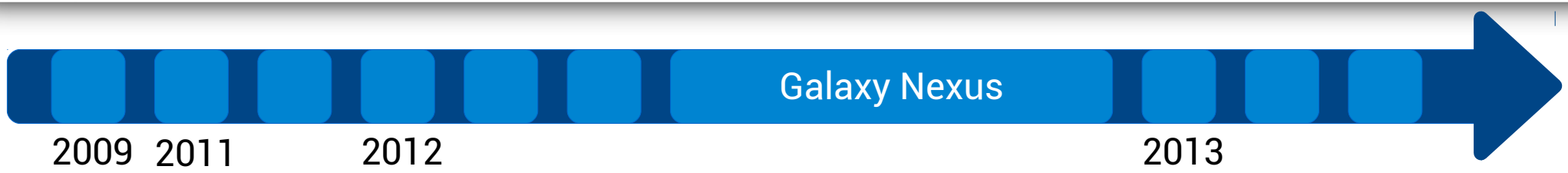


Galaxy S2 :

- Bonne isolation du **modem**
- **Chargeur de démarrage** non-libre et signé
- **Microcodes** non-libres pour WiFi, bluetooth, MFC
- Pas de problèmes **graphiques**
- **GPS** : protocole inconnu
- **Capteurs** : en partie libre, en partie remplacé et implémentation du constructeur
- **Modem** : même protocole que le **Nexus S**
- **Audio** : écriture d'une implémentation libre interface standard (**ALSA**) et spécifique
- **Caméra** : écriture d'une implémentation libre interface standard (**V4L2**) et spécifique

II. Développement de Replicant

Chronologie et challenges



Galaxy Nexus :

- Bonne isolation du **modem**
- **Chargeur de démarrage** non-libre et signé
- **Microcodes** non-libres pour WiFi, bluetooth, MFC
- et caméra
- **GPS** : protocole inconnu
- **Modem** : même protocole que le **Nexus S**
- **Caméra** : implémentation libre existante dépendance à l'accélération graphique

II. Développement de Replicant

Chronologie et challenges

Galaxy Tab 2 7.0 et 10.1 :

- Matériel similaire au **Galaxy Nexus**
- **GPS** : protocole différent mais pas documenté non-plus
- **Capteurs** : écriture d'une implémentation libre
- Port simple et **sans difficulté** particulière

II. Développement de Replicant

Chronologie et challenges

Galaxy S3 :

- Bonne isolation du **modem**
- **Chargeur de démarrage** non-libre et signé
- **Microcodes** non-libres pour WiFi, bluetooth, MFC
- Pas de problèmes **graphiques**
- **GPS** : protocole inconnu
- **Capteurs** : écriture d'une implémentation libre
- **Modem** : même protocole que le **Nexus S**
- **Caméra** : écriture d'une implémentation libre basée sur celle du Galaxy S2, interface standard (**V4L2**) et spécifique

II. Développement de Replicant

Chronologie et challenges

Galaxy Note :

- Très semblable au **Galaxy S2**
- Port simple et **sans difficulté** particulière

II. Développement de Replicant

Remplacer les composants propriétaires

- Système entièrement libre et fonctionnel
- Remplacer les composants propriétaires
- Beaucoup de code à écrire, peu de documentation
- Champs variés : **audio**, **caméra**, **modem**, **capteurs**, etc

Tâches sont particulièrement complexes et pas traitées par le projet Replicant :

- Microcodes (pas remplacés, pas distribués)
- Accélération graphique (manquante, adaptation du système)

Certains projets dédiés existent :

- Freedreno
- Lima

II. Développement de Replicant

Remplacer les composants propriétaires

Bien souvent, il est possible de comprendre le fonctionnement d'un composant propriétaire :

- En traçant l'exécution et les appels système
- En traçant les interactions avec le matériel au niveau du noyau
- En étudiant les logs

Une approche statique peut également porter ses fruits :

- Étude des chaines de caractère, noms des fonctions
- Décompilation et analyse de l'assembleur

Dans les meilleurs cas, on pourra disposer :

- De documentation (complète ou non) du protocole en jeu
- D'implémentations libres similaires et/ou adaptables

Dans biens des cas, comprendre le fonctionnement des composants propriétaires n'est pas aussi complexe qu'on pourrait le croire !

II. Développement de Replicant

Remplacer les composants propriétaires

Il reste alors à implémenter un remplacement libre :

- Avec autant de fonctionnalités que possible
- Code robuste et fiable
- Implémentations utilisées par CyanogenMod
- Échange de code et nouvelles fonctionnalités

Code de Replicant inclus dans CyanogenMod :

- Modules audio et caméra du Galaxy S2
- Modules capteurs et caméra du Galaxy S3
- Module capteurs des Galaxy Tab 2

II. Développement de Replicant

Futur du projet

Perspectives futures pour Replicant :

- Nouvelles versions d'Android (Replicant 4.2)
- Plus d'appareils pris en charge
- Plus de fonctionnalités prises en charge
- Base Omni plutôt que CyanogenMod ?

Besoin fort de nouveaux développeurs :

- Guides pour installer, compiler et développer sur Replicant
- Guide pour porter un nouvel appareil sur Replicant
- Compétences requises : C, make, git

Contributions financières bienvenues !

Site web : http://replicant.us
Wiki/tracker : http://redmine.replicant.us


That's all Folks!

Texte :

- © 2013 Paul Kocialkowski
  Licence Creative Commons BY-SA 3.0

Images :

- **Android robot**, © Google
  Licence Creative Commons BY 3.0
- **Replicant robot**, © Mirella Vedovetto, Paul Kocialkowski,
  Licence Creative Commons BY-SA 3.0
- **Openmoko Neo FreeRunner**, © FIC/OpenMoko,
  Licence Creative Commons BY-SA 3.0
- **Autres images** : © Paul Kocialkowski
  Licence Creative Commons BY-SA 3.0