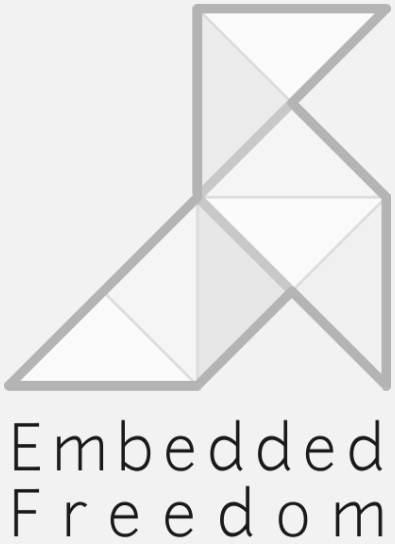
Origami-EC : vers un micrologiciel libre pour Embedded Controller

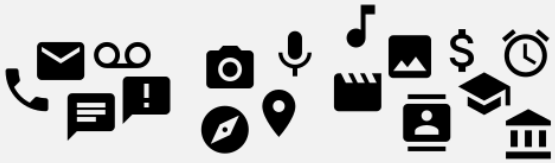


Paul Kocialkowski
contact@paulk.fr

Samedi 17 novembre 2018

Contrôle de notre vie numérique

Numérisation des modes de vie

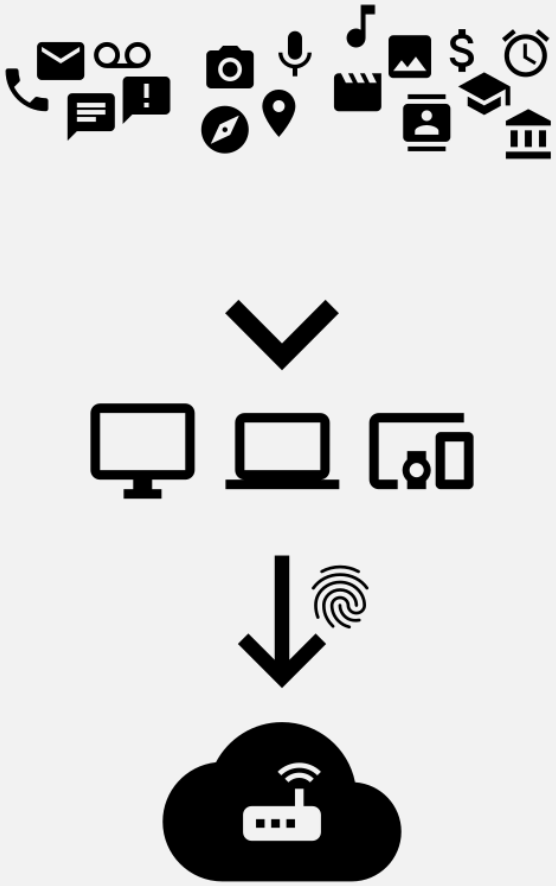


- Numérisation d'**aspects de la vie** :
  - communications, social
  - accès à l'information, divertissement

Numérisation des modes de vie

- Numérisation d'**aspects de la vie** :
  - communications, social
  - accès à l'information, divertissement
- **Appareils** du quotidien :
  - entrées/sorties multiples
  - collecte de données
  - capacités de traitement

Numérisation des modes de vie



- Numérisation d'**aspects de la vie** :
  - communications, social
  - accès à l'information, divertissement
- **Appareils** du quotidien :
  - entrées/sorties multiples
  - collecte de données
  - capacités de traitement
- **Infrastructure** des données :
  - quelles données, à qui, avec quelles conditions
  - empreinte numérique, méta-données

Impacts sur l'utilisateur

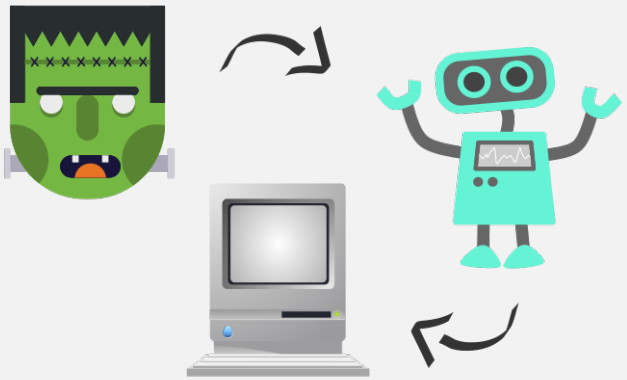
Impact majeur de la technologie sur la vie des utilisateurs

Impacts sur l'utilisateur

Impact majeur de la technologie sur la vie des utilisateurs

Dans la littérature :

- **Monstre** de Frankenstein
- **Lois de la robotique** d'Asimov
- **Télécran** d'Orwell (1984)

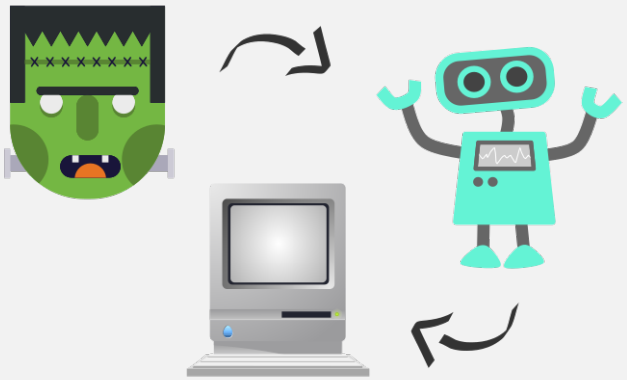


Impacts sur l'utilisateur

Impact majeur de la technologie sur la vie des utilisateurs

Dans la littérature :

- **Monstre** de Frankenstein
- **Lois de la robotique** d'Asimov
- **Télécran** d'Orwell (1984)



Comportement de la technologie numérique :

- Dicté par sa programmation, pas neutre
- Sert les intérêts du programmeur
- Accès des logiciels aux données

Garanties de liberté, sécurité et vie privée

Enjeux pour les utilisateurs :

- **Contrôle** des outils numériques
- **Confiance** dans la technologie
- **Vie privée** et **sécurité**

Garanties de liberté, sécurité et vie privée

Enjeux pour les utilisateurs :

- **Contrôle** des outils numériques
- **Confiance** dans la technologie
- **Vie privée** et **sécurité**

Garanties nécessaires :

- Possibilité de **remplacer les logiciels** :
  - choix d'utilisation, pas de conception
  - décorréler matériel et logiciel

Garanties de liberté, sécurité et vie privée

Enjeux pour les utilisateurs :

- **Contrôle** des outils numériques
- **Confiance** dans la technologie
- **Vie privée** et **sécurité**

Garanties nécessaires :

- Possibilité de **remplacer les logiciels** :
  - choix d'utilisation, pas de conception
  - décorréler matériel et logiciel
- **Révoquer les privilèges** des développeurs :
  - modification du comportement
  - confiance et hiérarchie des valeurs

Logiciels libres et effets associés

Liberté du logiciel *: capacité individuelle et collective d'utiliser, d'étudier, de modifier et de redistribuer le logiciel*

Logiciels libres et effets associés

Liberté du logiciel *: capacité individuelle et collective d'utiliser, d'étudier, de modifier et de redistribuer le logiciel*

Effets pour les utilisateurs :

- Contrôle individuel et collectif
- Choix personnel de confiance
- Mises à jour et correctifs
- Changement de cas d'utilisation
- Accès au savoir de la technologie

Composants, privilèges et accès aux données

Accès des logiciels aux données

Problématique : **quels logiciels avec quels privilèges d'accès aux données de l'utilisateur ?**

Accès des logiciels aux données

Problématique : **quels logiciels avec quels privilèges d'accès aux données de l'utilisateur ?**

Logiciels les plus visibles :

- Applications
- Système d'exploitation

Accès des logiciels aux données

Problématique : **quels logiciels avec quels privilèges d'accès aux données de l'utilisateur ?**

Logiciels les plus visibles :

- Applications
- Système d'exploitation

Mécanismes de restriction :

- droits UNIX, ACL, SELinux, cgroups
- modes d'exécution : utilisateur, superviseur, hyperviseur
- virtualisation de la mémoire
- sujets aux erreurs d'implémentation

Logiciels privilégiés

Logiciels moins visibles :

- Logiciel de démarrage (BIOS, UEFI, bootloader)
- Mode d'exécution privilégié (SMM, TrustZone)

Logiciels privilégiés

Logiciels moins visibles :

- Logiciel de démarrage (BIOS, UEFI, bootloader)
- Mode d'exécution privilégié (SMM, TrustZone)

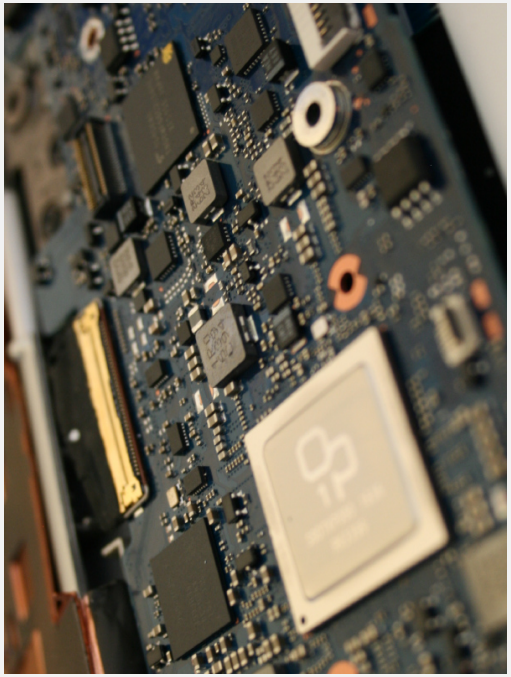
Particularités :

- Racine de confiance
- Accès privilégié au matériel
- Spécifique à l'appareil et préinstallé

Périphériques et contrôleurs

Au-delà du processeur principal :

- Processeurs auxiliaires
- Contrôleurs
- Périphériques



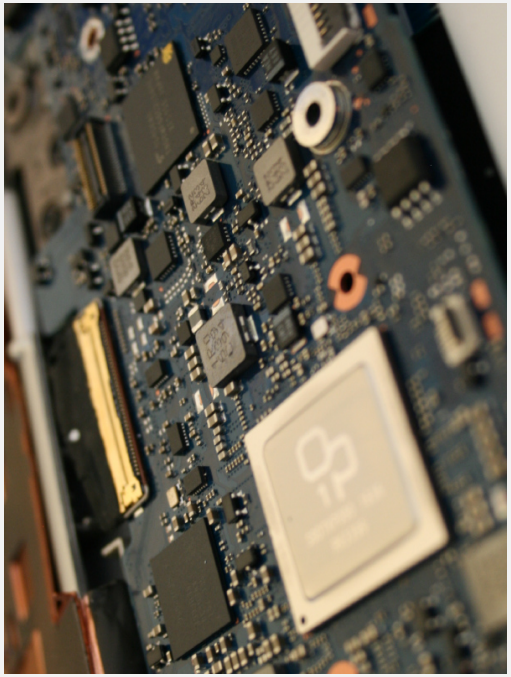
Périphériques et contrôleurs

Au-delà du processeur principal :

- Processeurs auxiliaires
- Contrôleurs
- Périphériques

Logiciels spécifiques :

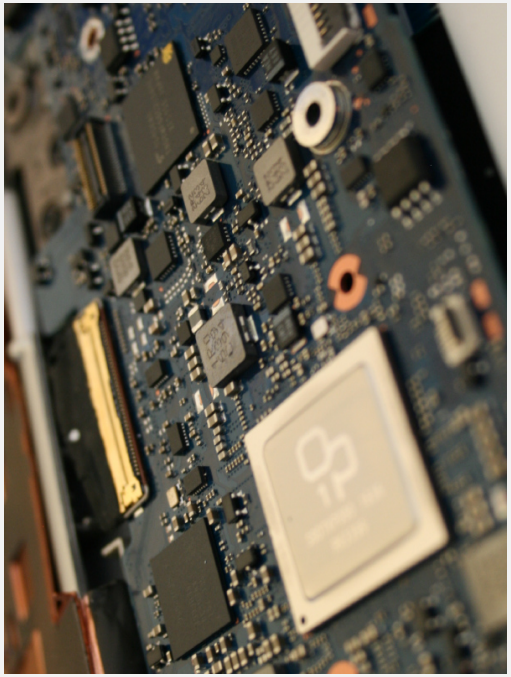
- Systèmes auxiliaires
- Micrologiciels



Périphériques et contrôleurs

Au-delà du processeur principal :

- Processeurs auxiliaires
- Contrôleurs
- Périphériques



Logiciels spécifiques :

- Systèmes auxiliaires
- Micrologiciels

Particularités :

- Accès aux entrées/sorties
- Accès à la mémoire système, IOMMU
- Logiciels spécifiques préinstallés ou chargés

Cas de l'Embedded Controller

Rôle de l'Embedded Controller

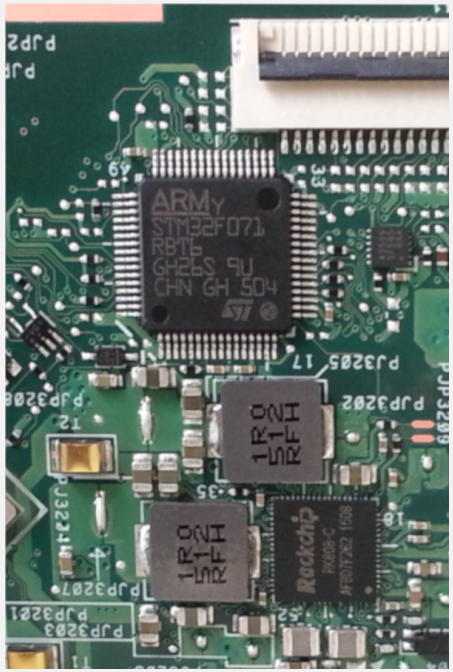
Embedded Controller : *microcontrôleur embarqué dans les ordinateurs portables*

Rôle de l'Embedded Controller

Embedded Controller : *microcontrôleur embarqué dans les ordinateurs portables*

En charge de plusieurs aspects :

- Démarrage, extinction
- Mise en veille, réveil
- Sources d'énergie, batterie
- Température, ventilateur, *throttle*
- LEDs, boutons, switches
- Clavier et touchpad
- Interface avec le CPU



Logiciel libre pour Embedded Controller

Intérêts particuliers de la liberté :

- Interaction avec l'utilisateur, modifications
  démarrage à l'ouverture du capot!
- Vie privée et sécurité
- Gestion de l'énergie et optimisations

Logiciel libre pour Embedded Controller

Intérêts particuliers de la liberté :

- Interaction avec l'utilisateur, modifications *démarrage à l'ouverture du capot!*
- Vie privée et sécurité
- Gestion de l'énergie et optimisations

Projets libres pour Embedded Controller :

- Chromium OS EC
- Project GSoC 2015 de Lynxis
- Ne couvre pas la majorité des appareils

Lenovo G505s et ENE KB9012

Intérêt pour le Lenovo G505s

Ordinateur portable candidat :

- Laptop Lenovo 15" de 2013
- FCH AMD Bolton M3
- APU x86 AMD série A (fam15h)

Intérêt pour le Lenovo G505s

Ordinateur portable candidat :

- Laptop Lenovo 15" de 2013
- FCH AMD Bolton M3
- APU x86 AMD série A (fam15h)

État de la prise en charge :

- Coreboot (AGESA)
- Option ROM/VGA BIOS
- Microcode CPU et mises à jour
- Micrologiciels :

Intérêt pour le Lenovo G505s

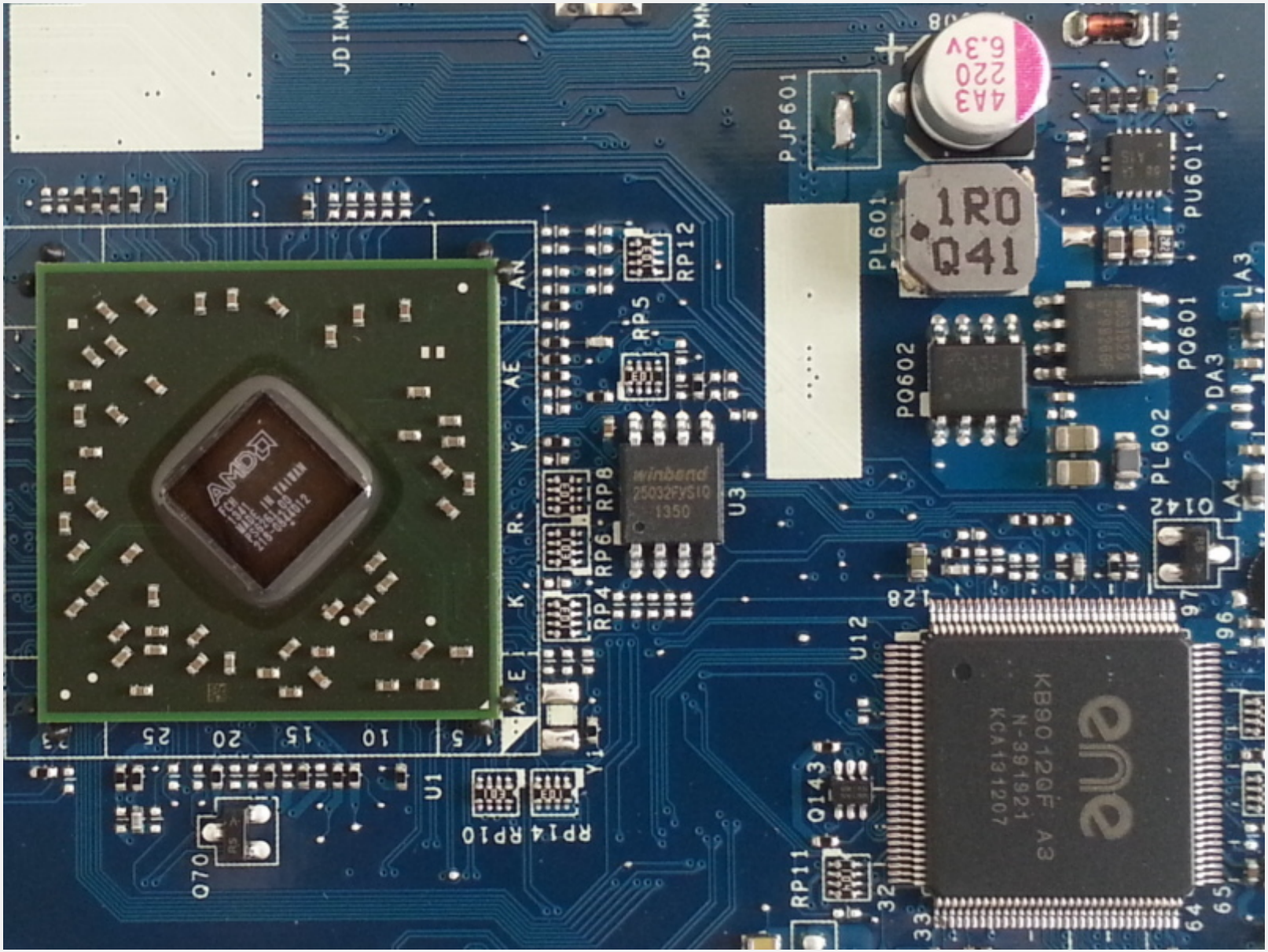
Ordinateur portable candidat :

- Laptop Lenovo 15" de 2013
- FCH AMD Bolton M3
- APU x86 AMD série A (fam15h)

État de la prise en charge :

- Coreboot (AGESA)
- Option ROM/VGA BIOS
- Microcode CPU et mises à jour
- Micrologiciels :
  - IMC
  - SMU
  - xHCI (USB 3)
  - Embedded Controller

Analyse du matériel



Documentation

Documentation du laptop (G505s) :

- Schéma complets :
  `Lenovo G405S Compal VALGC_GD LA-A091P.pdf`
- Diagramme de la séquence d'alimentation
- Pas de disposition de PCB ou labels

Documentation

Documentation du laptop (G505s) :

- Schéma complets :
  `Lenovo G405S Compal VALGC_GD LA-A091P.pdf`
- Diagramme de la séquence d'alimentation
- Pas de disposition de PCB ou labels

Documentation de l'EC (KB9012) :

- Vaste datasheet :
  - Description de la plateforme
  - Description des registres
- Quelques notes d'application

Description de la plateforme KB9012

- CPU basé sur le 8051 :
  - Horloge de 8 à 32 MHz
  - Mots de 8 bits
  - Disposition mémoire: *program*, *external*, *internal*, *SFR*
  - Contrôleur d'interruptions, timers
  - Extensions spécifiques

Description de la plateforme KB9012

- CPU basé sur le 8051 :
  - Horloge de 8 à 32 MHz
  - Mots de 8 bits
  - Disposition mémoire: *program*, *external*, *internal*, *SFR*
  - Contrôleur d'interruptions, timers
  - Extensions spécifiques
- Mémoire de stockage (flash de 128 kiB)
- Mémoire volatile (SRAM de 4 kiB)

Description de la plateforme KB9012

- CPU basé sur le 8051 :
  - Horloge de 8 à 32 MHz
  - Mots de 8 bits
  - Disposition mémoire: *program*, *external*, *internal*, *SFR*
  - Contrôleur d'interruptions, timers
  - Extensions spécifiques
- Mémoire de stockage (flash de 128 kiB)
- Mémoire volatile (SRAM de 4 kiB)
- Contrôleurs :
  - LPC, SMBUS (I2C), SPI
  - GPIO, ADC, DAC
  - Clavier, PS/2
  - IR, FAN, OW
  - Et quelques autres

Environnement de développement

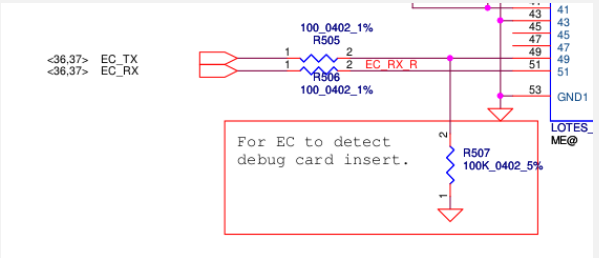
Environnement de développement

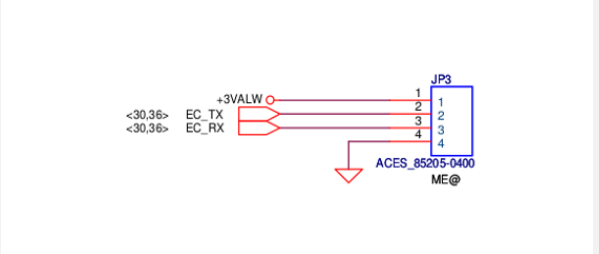
Matériel

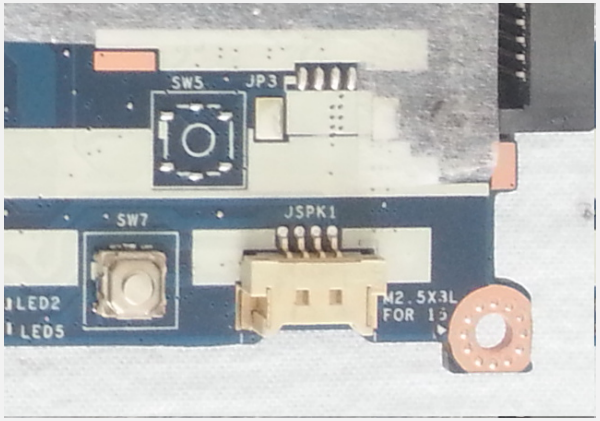
Port série et sortie de débogae

Port série :

- UART depuis le CPU 8051
- Exporté avec :
  - PCI-e
  - Pads (*JP3*)



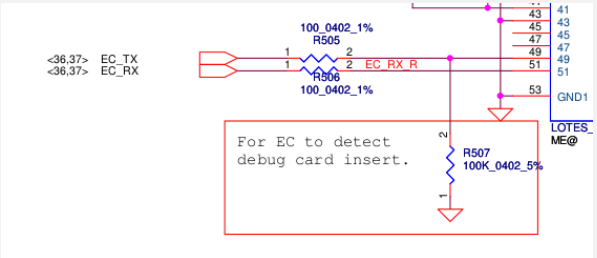


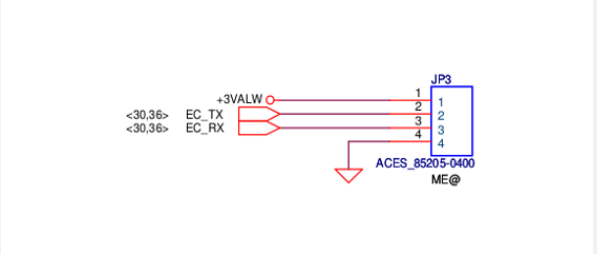


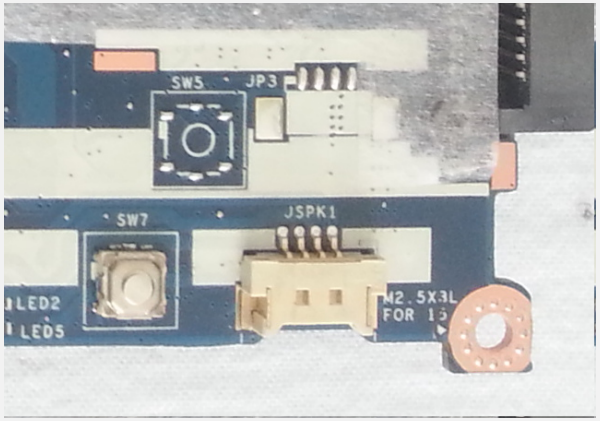
Port série et sortie de débogae

Port série :

- UART depuis le CPU 8051
- Exporté avec :
  - PCI-e
  - Pads (*JP3*)








```
KSTART!R
EF-01,E7,E0,ON01,NON1N2N3N3N4N5N6EXN7
EF-01,E0,F0,N8NANANANANANANBNBNBNBNBNBNB
I52,KC52,DA4,KDA4,OOO,NBO,
e59,Kc59,dE9,KdE9,
KxFF,NB
I52,KC52,DA4,KDA4,OOO,O,
e59,Kc59,NBdE9,KdE9,NBNBNBNB
MC4E,MDED,
EF-01,E0,ED,MrFF,
MC4E,MDEC,
EF-01,E0,EC,Mr06,NBVFF,NBC,RFA,OFA,RAA,K20
MC42,MDOO,
MC4E,MDEB,
EF-01,E0,EB,Mr55,O,NB
```

Écriture du micrologiciel

Accès à la mémoire interne :

- Interface X-Bus, commandes

Écriture du micrologiciel

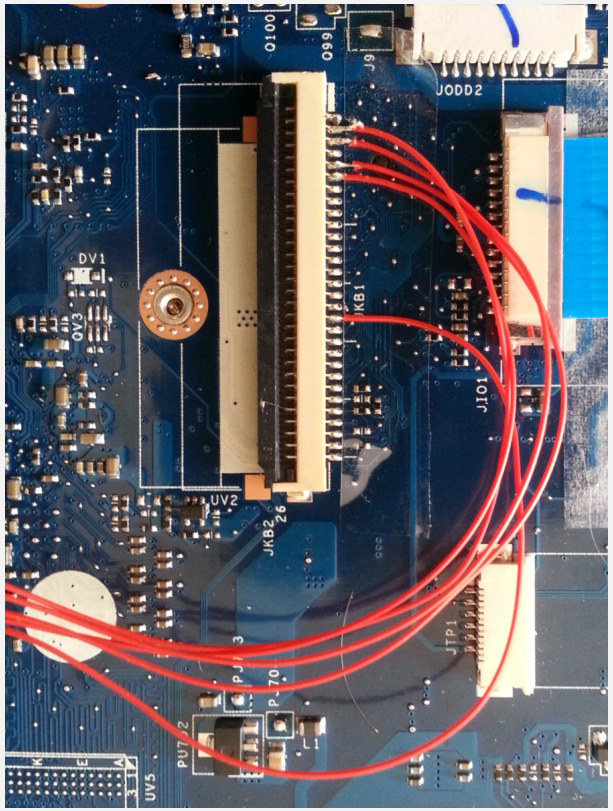
Accès à la mémoire interne :

- Interface X-Bus, commandes
- LPC Index-I/O:
  - Référence flashrom CrOS
  - Désactivé par micrologiciel

Écriture du micrologiciel

Accès à la mémoire interne :

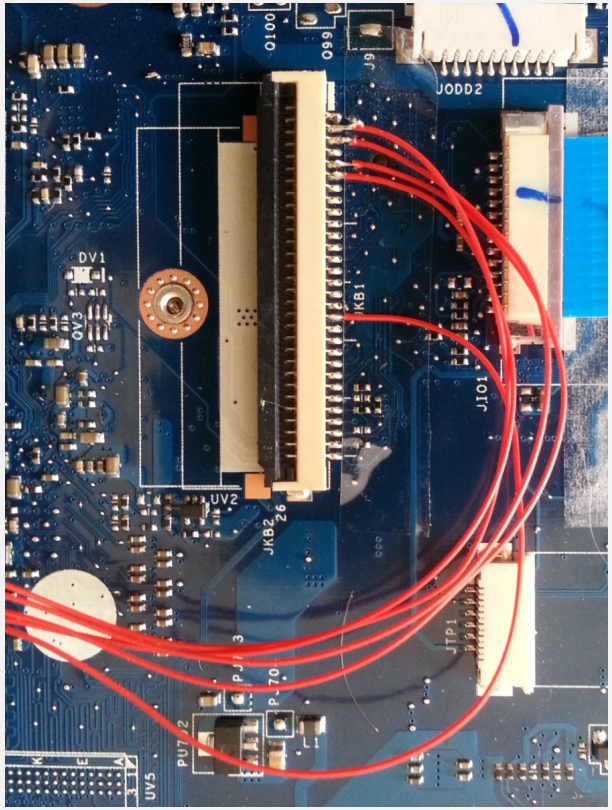
- Interface X-Bus, commandes
- LPC Index-I/O:
  - Référence flashrom CrOS
  - Désactivé par micrologiciel
- ENE Debug Interface (EDI):
  - Protocole SPI
  - Note d'application
  - Pins du clavier



Écriture du micrologiciel

Accès à la mémoire interne :

- Interface X-Bus, commandes
- LPC Index-I/O:
  - Référence flashrom CrOS
  - Désactivé par micrologiciel
- ENE Debug Interface (EDI):
  - Protocole SPI
  - Note d'application
  - Pins du clavier



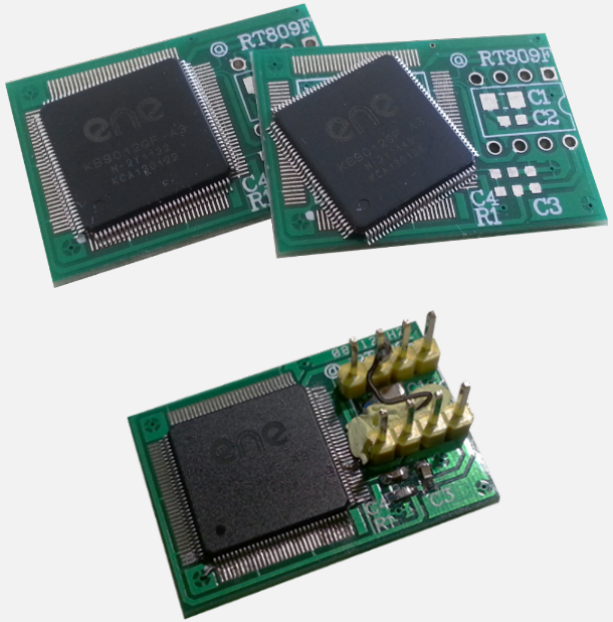
Pris en charge par **flashrom**:

```
# flashrom -p ch341a_spi -c "KB9012 (EDI)" -w flash.img
```

Plateforme minimale de développement

Carte de développement :

- Carte et puce séparées
- Soudure LQFP128
- Pins exposés
- Utilisé pour la programmation
- Peu d'intérêt autrement



Environnement de développement

Logiciel

Développement de micrologiciel

Première approche :

- ISA 8051
- *Opcodes* directs (*hexedit*)
- *Hello World!* port série, LED

```
90ff0d  mov dptr, 0xff0d
e0      movx a, @dptr
440c    orl a, 0xc
f0      movx @dptr, a
43a880  orl 0xa8, #0x80
758200  mov 0x82, #0x00
22      ret
```

Développement de micrologiciel

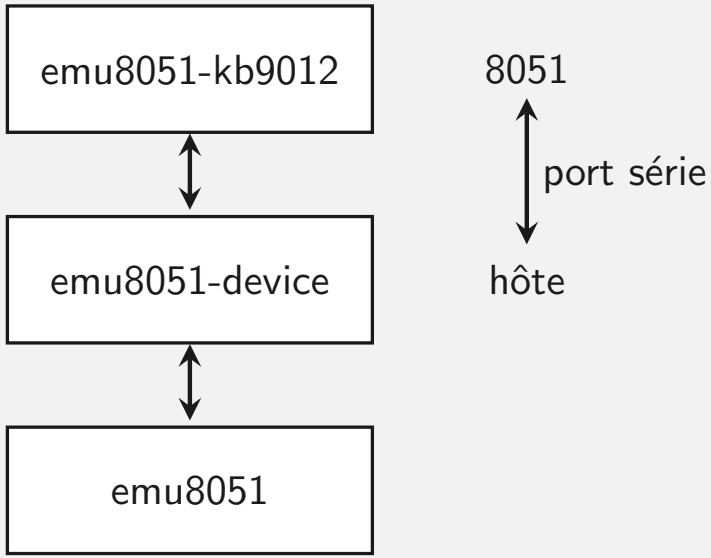
Première approche :

- ISA 8051
- *Opcodes* directs (*hexedit*)
- *Hello World!* port série, LED

```
90ff0d  mov dptr, 0xff0d
e0      movx a, @dptr
440c    orl a, 0xc
f0      movx @dptr, a
43a880  orl 0xa8, #0x80
758200  mov 0x82, #0x00
22      ret
```

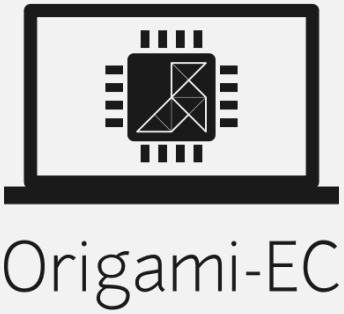
Véritable base de développement :

- Compilateur C : SDCC
- Modèle mémoire, pile
- Outils d'ingénierie inverse :
  - Statique : radare2 (8051)
  - Dynamique : emu8051, emu8051-device



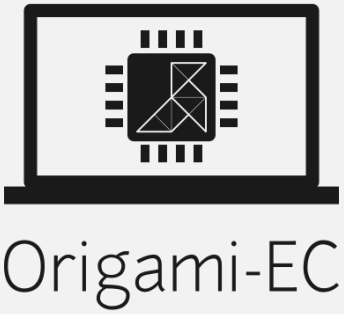
Micrologiciel libre Origami-EC

Origami-EC : Introduction



Une implémentation libre et flexible de micro-logiciel pour les Embedded Controller (8051).

Origami-EC : Introduction



Une implémentation libre et flexible de micro-logiciel pour les Embedded Controller (8051).

- Écrit en C, *toolchain* SDCC
- Implémentation flexible (pas seulement KB9012)
- Code source : `https://git.code.paulk.fr/`
- Licence GPLv3+

Origami-EC : Architecture

- APIs génériques
- Implémentations par plateforme et appareil
- Code commun (autant que possible)
- Tâches avec priorités
  pas de *context switching*

Origami-EC : État de la prise en charge

- Console, commandes
  avec historique
- LEDs
- Buttons, switches
- Début de séquence de démarrage
  pas encore fonctionnel
- Changement de segment mémoire
- Mise en veille de l'EC

Origami-EC : Travail restant

Priorités de développement :

- Gestion de l'énergie minimale
- Contrôleurs et périphériques critiques
- Communication avec l'hôte (LPC)
- Émulateur 8051, trace
- Carte d'évaluation (EVB)

Origami-EC : Travail restant

Priorités de développement :

- Gestion de l'énergie minimale
- Contrôleurs et périphériques critiques
- Communication avec l'hôte (LPC)
- Émulateur 8051, trace
- Carte d'évaluation (EVB)

Projet :

- Annonce publique
- Documentation
- Infrastructure :
  - Site web
  - Dépôt git
  - Liste de diffusion

Merci de votre attention !

Merci de votre attention !

Questions ?