EthyloSSTIC

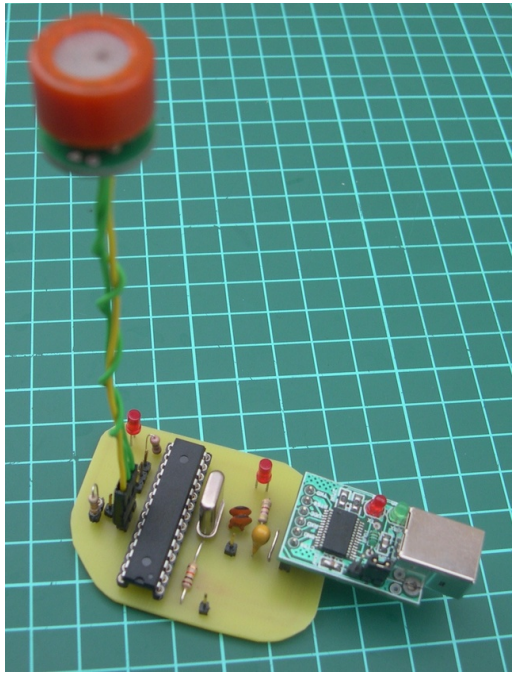
Denis Bodor Sebastien Tricaud

GNU/Linux Mag France / INL

Rump SSTIC (Rennes) 2009

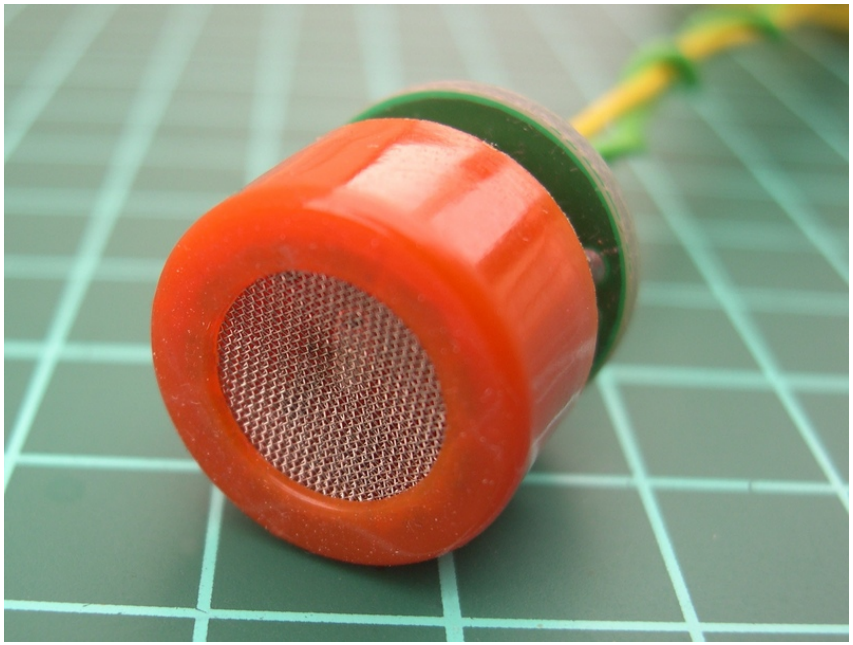
EthyloSSTIC

Un coté hard



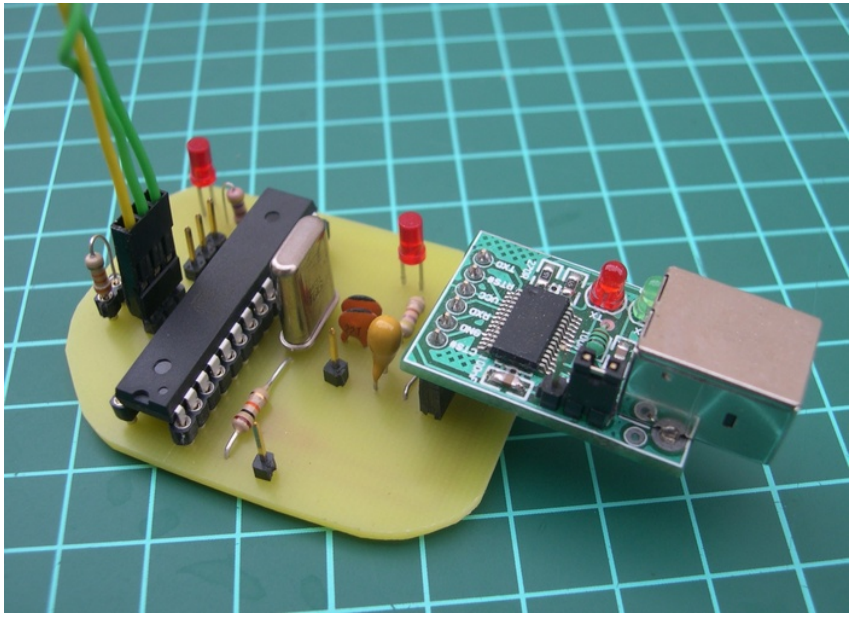
- Capteur d'alcool/éthanol MQ-3
- Microcontrôleur AVR Atmega8
- Convertisseur Série TTL vers USB

Capteur MQ-3



- Détection par dioxyde d'étain (SnO2)
- Temps de chauffe
- Injection courant, mesure tension
- Résultats très variables

Atmel AVR Atmega8



- 8K de Flash
- 1K de SRAM
- Convertisseur A/N 6 canaux
- USART (synchrone ou asynchrone)
- Programmation en C (avr-gcc + avr-libc)

Ça fera combien M. l'agent ?

- Atmega8 = 1 à 2 euros
- MQ-3 = 4 euros
- convertisseur = 15 euros
- Programmeur : 0 à 20 euros
- Le reste = 0 à 4 euros
- Du temps = 0 euro (You can sleep when you're drunkˆWdead)

Where can I saddle my horse?

- une série de tests
- pam_breathalizer (/etc/security/pam_breathalizer.conf)
- Pong[1]

- Évolutions avec le pare-feu météo

[1] Dindinx rocks

Des tests. . . très durs

- À l'allumage, valeur reçue = 800
- Attendre 5 mn (300)
- On commence avec de l'eau

Des tests. . . très durs

- À l'allumage, valeur reçue = 800
- Attendre 5 mn (300)
- On commence avec de l'eau de vie!

Des tests. . . très durs

- À l'allumage, valeur reçue = 800
- Attendre 5 mn (300)
- On commence avec de l'eau de vie!
- On souffle
  - chaud!
  - **astuce1**: souffler froid fait diminuer la valeur

Des tests. . . très durs

- À l'allumage, valeur reçue = 800
- Attendre 5 mn (300)
- On commence avec de l'eau de vie!
- On souffle
  - chaud!
  - **astuce1**: souffler froid fait diminuer la valeur (merci sergent Laurent A. pour l'info!)
  - **astuce2**: sucer un arlequin fait diminuer la valeur aussi

Des tests. . . très durs

- À l'allumage, valeur reçue = 800
- Attendre 5 mn (300)
- On commence avec de l'eau de vie!
- On souffle
  - chaud!
  - **astuce1**: souffler froid fait diminuer la valeur (merci sergent Laurent A. pour l'info!)
  - **astuce2**: sucer un arlequin fait diminuer la valeur aussi (merci Pierre C. pour l'info!)

/dev/ttyUSB0

- Quelques flags
  - termios_p.c_cflag = B19200;
  - termios_p.c_cflag |= CS8;
- Ne pas oublier
  - get\r
  - sleep(1)

Module PAM: Configuration

/etc/security/pam_breathalizer.conf

```
serial_port = /dev/ttyUSB0
speed       = 19200

getstr = get

denyval > 800
```

Module PAM: Syslog

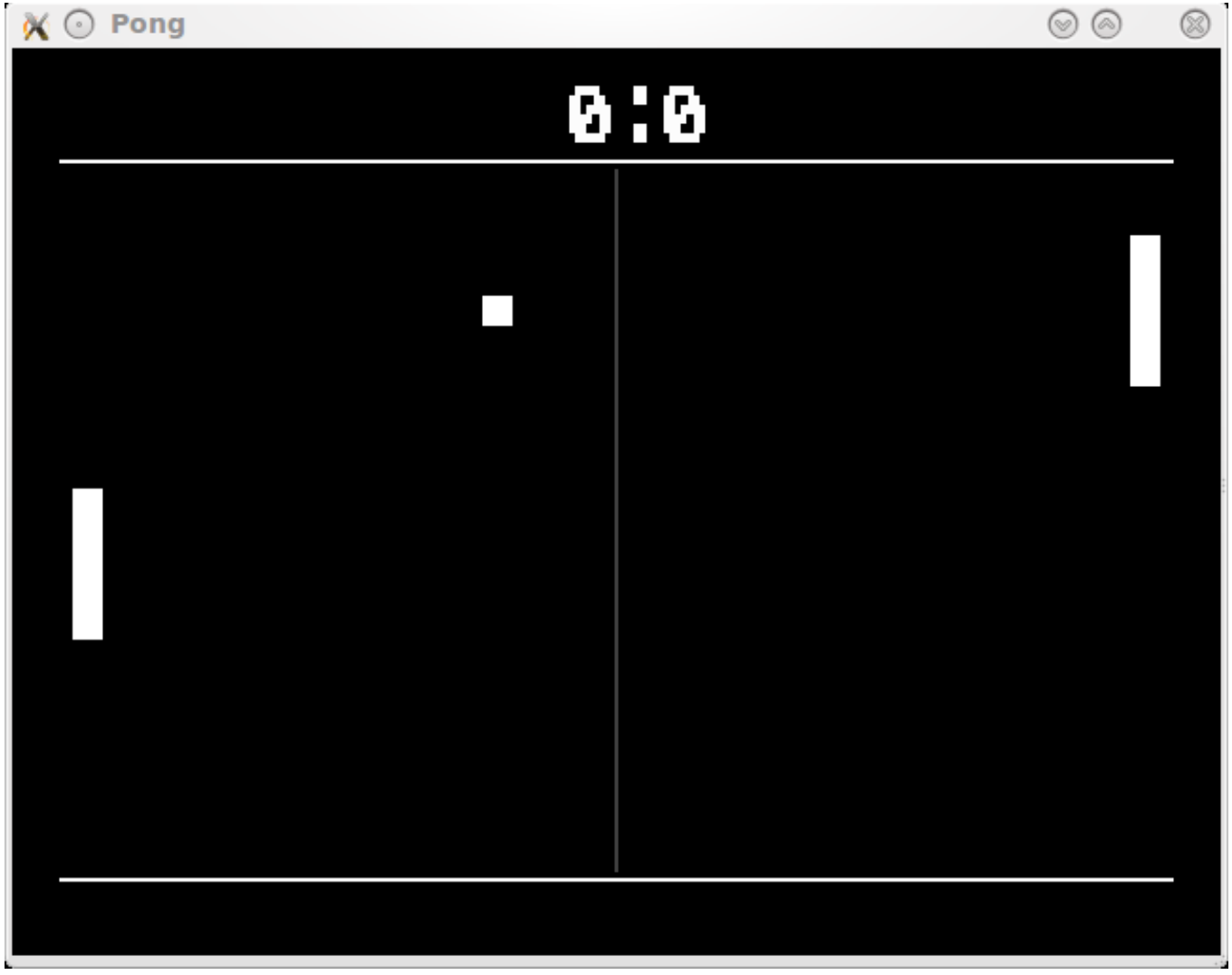
Si tu habites Rennes

```
Alcoholic people forbiden on this system
```

Si tu n'as pas bu

```
The guy is not drunk. Authentication success!
```

Pong



Evolutions

- Script subversion de post-commit
- Intégration au pare-feu météo