générateur **de nombres réellement aléatoires** avec interface USB

deux PIC pour le prix d'un AVR

Matthias Wolf (Allemagne)

Il est utile de disposer d'un bon générateur de nombres réellement aléatoires (TRNG). Sans ce dernier, le cryptage des données de manière sécurisée est presque impossible. Les applications de jeux et de paris nécessitent également des TRNG de top-niveau. Elektor a publié un projet d'un TRNG analogique en 2017 ; dans cette mise-à-jour, nous avons rajouté une interface USB.

Le générateur de nombres réellement aléatoires (TRNG) basé sur des composants abordables par Luka Matic [1], utilise une carte SD pour enregistrer la séquence aléatoire produite. Dans ces pages, nous présentons une adaptation de son travail, où l'emplacement de la carte mémoire est remplacé par une interface USB.

Le nouveau circuit (**figure 1**) possède deux microcontrôleurs PIC de Microchip Technology au lieu d'un seul ATtiny2313A : un pour la partie traitement de signal analogique (PIC16F19156) et un pour l'interface USB (PIC18F25K50). Les deux microcontrôleurs communiquent entre eux via un bus SPI, isolé galvaniquement avec des optocoupleurs à haute vitesse pour empêcher au bruit numérique du circuit USB de perturber le signal analogique.

Étalonnage du filtre

Un petit programme sur PC a été écrit pour étalonner les filtres analogiques en temps réel de manière simple (**figure 2**).

Mes réglages pour les filtres analogiques sont les suivants :

- S5 : C37,C38,C39,C40,C41 ON avec C39 à 109 pF
- S6 : C45,C46,C47 ON avec C47 à 25 pF
- S7 : Switch1 ON et P6 à 409 Ω

Ces paramètres dépendent des composants utilisés pour construire le TRNG, vous pouvez en utiliser d'autres.

Le type de diode zener utilisée est également important. J'ai d'abord utilisé la BZX384C12-E3-08 de Vishay, mais le bruit généré était mauvais.

Finalement, le PIC16 utilise un taux d'échantillonnage légèrement plus élevé (800 kHz, 1,25 µs par échantillon) par rapport au TRNG original de Luka.

Allez chercher les fichiers !

Tous les fichiers du projet peuvent être téléchargés [2]. Ils comprennent les schémas (trois pages), le fichier CAD Target 3001, le micrologiciel pour le PIC16 (échantillonnage analogique, EDI MPLAB X avec le compilateur PCM C de CCS), le micrologiciel pour le PIC18 (traitement USB, EDI MPLAB X avec XC8), et l'application de bureau (C#, Visual Studio 2017 version *commmunity*).

190235-04

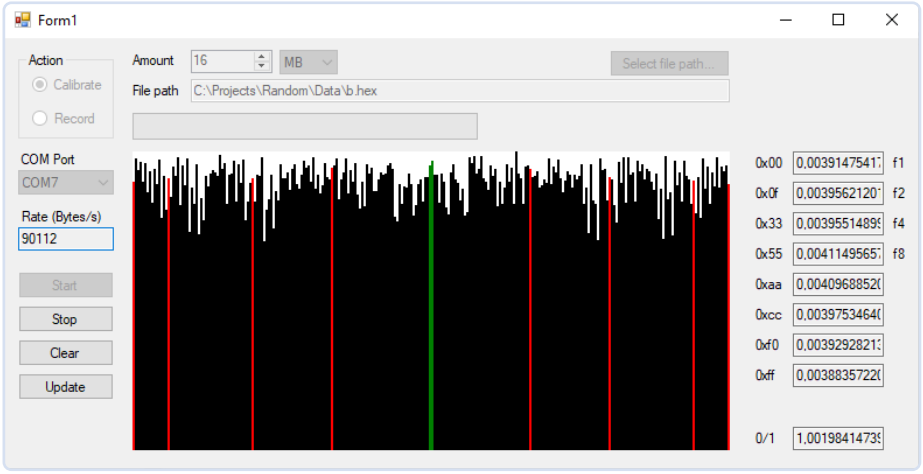

Figure 2. Copie d'écran du programme pour PC permettant d'étalonner les filtres analogiques et d'enregistrer des données aléatoires.

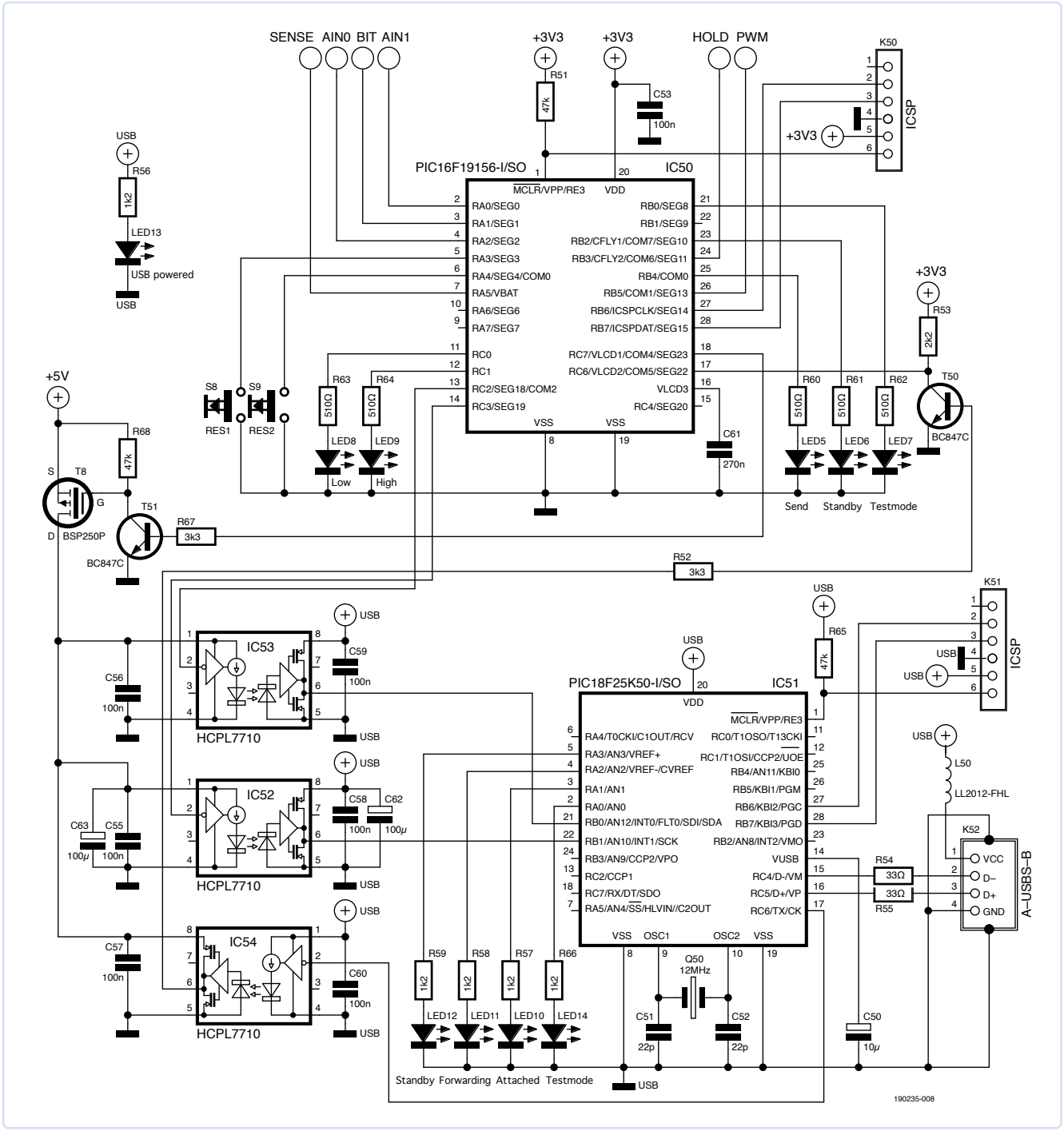

Figure 1. La partie numérique du TRNG original de 2017 avec son processeur ATtiny2313A a été remplacée par deux microcontrôleurs PIC. Le port USB remplace l'emplacement pour carte SD.

Des question, des commentaires ?

Contactez Elektor redaction@elektor.fr.

Produits

- **Livre en anglais « *Electronic Security and Espionage* », L. Matic (Elektor 2021, SKU 19903)**
  www.elektor.fr/electronic-security-and-espionage

LIENS

[1] L. Matic, générateur de nombres réellement aléatoires, Elektor 3/2017 : https://www.elektormagazine.fr/magazine/elektor-201703/40251
[2] Ce project sur Elektor Labs : https://www.elektormagazine.fr/labs/usb-random-number-generator