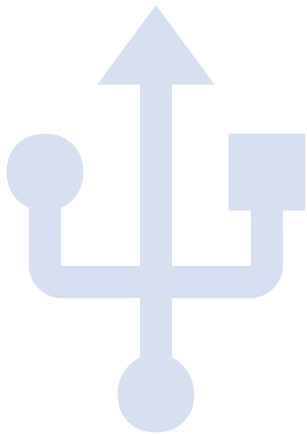


Echte USB-toevalsgenerator

twee PIC's voor de prijs van één AVR



Matthias Wolf (Duitsland)

Een goede toevalsgenerator (True Random Number Generator, TRNG) is handig om te hebben. Veilige gegevensversleuteling is bijvoorbeeld bijna onmogelijk zonder. Gaming- en goktoepassingen vereisen ook TRNG's van topklasse. Elektor heeft in 2017 een analoge TRNG gepresenteerd; in deze update voegen we daar USB aan toe.

De Echte Random Number Generator (TRNG) met goedkope componenten van Luka Matic [1] gebruikte een SD-kaart om de gegenereerde toevalsreeks op te slaan. Hier presenteren we een uitbreiding van dit project waarbij de SD-kaart is vervangen door een USB-interface.

De nieuwe schakeling (**figuur 1**) heeft twee PIC-microcontrollers van Microchip in plaats van een enkele ATtiny2313A: één voor de analoge signaalverwerking (PIC16F19156) en één voor de USB-interface (PIC18F25K50). Beide MCU's communiceren met elkaar via een SPI-bus, galvanisch geïsoleerd met snelle optocouplers om te voorkomen dat ruis van het digitale USB-gedeelte het analoge signaal verstoort.

Filterkalibratie

Er is een kleine PC-applicatie geschreven om de analoge filters op een gemakkelijke manier in realtime te kalibreren (**figuur 2**).

Mijn instellingen voor de analoge filters zijn als volgt:

- S5: C37,C38,C39,C40,C41 ON met C39 = 109 pF
- S6: C45,C46,C47 ON met C47 = 25 pF
- S7: schakelaar 1 ON met P6 = 409 Ω

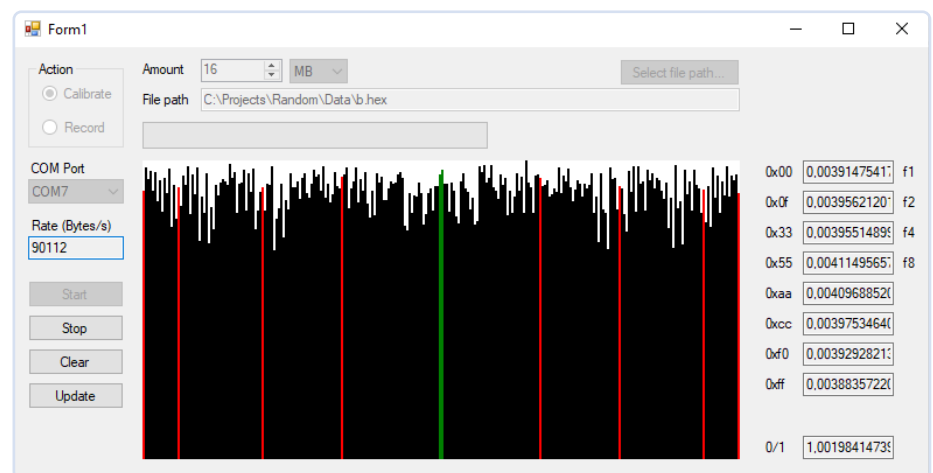
Deze instellingen zijn afhankelijk van de componenten die zijn gebruikt om de TRNG te bouwen; eventueel heb je andere nodig. Welke zenerdiodes worden gebruikt is ook belangrijk. In eerste instantie gebruikte ik de BZX384C12-E3-08 van Vishay, maar diens ruis was onbruikbaar.

Ten slotte heeft de PIC16, vergeleken met de originele TRNG van Luka, een iets hogere bemonsteringsfrequentie (800 kHz, 1,25 µs per sample).

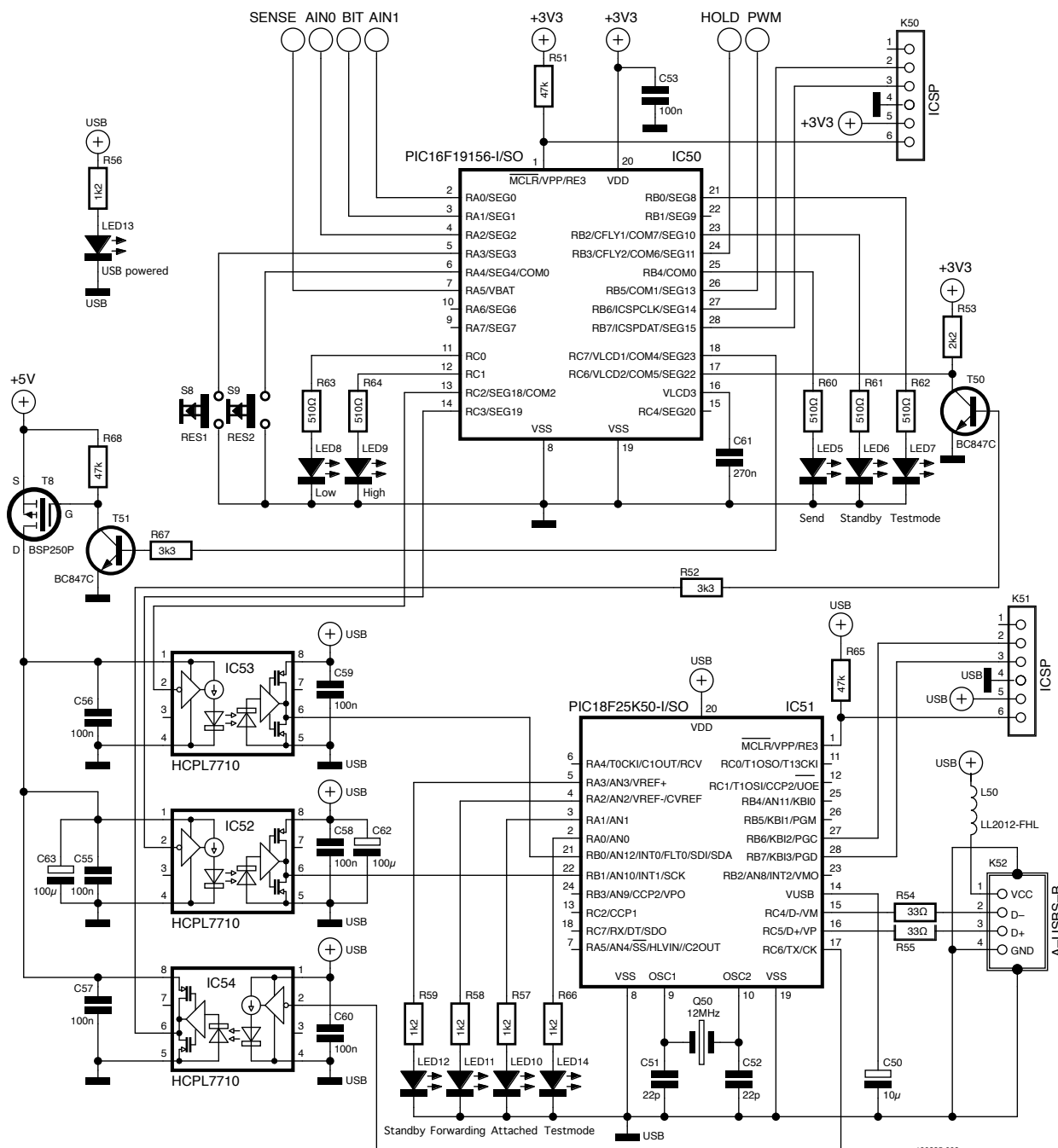
Haal de bestanden op!

Alle projectbestanden kunnen worden gedownload van [2]. Ze omvatten de schema's (drie pagina's), het Target 3001 CAD-project, firmware voor de PIC16 (analoge sampling, MPLAB X IDE met PCM C-compiler van CCS), firmware voor de PIC18 (USB-verwerking, MPLAB X IDE met XC8), en de desktop-applicatie (C#, Visual Studio 2017 community-editie). ◀

190235-03



Figuur 2. Screenshot van de PC-desktoptoepassing voor het kalibreren van de analoge filters en het opslaan van toevalsdata.



Figuur 1. Het digitale gedeelte van de originele TRNG uit 2017 met zijn ATtiny2313A MCU is vervangen door twee PIC-microcontrollers. De USB-poort vervangt de SD-kaarthouder.

Vragen of opmerkingen?

Hebt u technische vragen naar aanleiding van dit artikel? Stuur een e-mail naar de redactie van Elektor via redactie@elektor.com.



Gerelateerde producten

- > **L. Matic, *Electronic Security and Espionage* (Elektor 2021, SKU 19903)**
www.elektor.com/electronic-security-and-espionage

WEB LINKS

- [1] L. Matic, "Echte Random Number Generator", Elektor maart/april 2017:
<http://www.elektormagazine.nl/magazine/elektor-201703/40197>
- [2] Dit project op Elektor Labs: <https://www.elektormagazine.com/labs/usb-random-number-generator>