

Anatomie van smart plugs

welke zijn hacker-vriendelijk?

Mathias Claußen (Elektor)

Slimme stekkers of stopcontacten met WiFi-functionaliteit ("smart plugs" in goed neo-Nederlands) zijn tegenwoordig verkrijgbaar voor minder dan 15 euro. Hiermee kunnen lampen en andere consumentenapparaten op afstand worden bediend (sommige modellen kunnen zelfs het stroomverbruik van het apparaat registreren). Voor elektronici is de kous daarmee niet af. Vragen als "Welke hardware gebruiken ze eigenlijk?" en gedachten als "Misschien kan ik de firmware aanpassen en een ander cloudplatform gebruiken dan wat door de fabrikant is gespecificeerd" spelen altijd door ons hoofd. Om de ingewanden van een aantal van deze slimme stekkers te onderzoeken en uit te vinden welke modellen hacker-vriendelijk zijn, heb ik schroevendraaiers, een ijzerzaag, een camera en een vergrootglas uit mijn gereedschapskist gehaald.



Pas op: netspanning! De hier besproken elektronica werkt bij de DC-topwaarde van de netspanning! Gebruik deze niet buiten de beschermende behuizing, aangezien dit levensgevaarlijk kan zijn. Ondeskundig gebruik leidt tot potentieel dodelijke elektrische schokken.



Figuur 1. De Gosund SP211 (bron: <https://bit.ly/3wAWu6g>).



Figuur 2. Amazon Smart Plug (bron: <https://bit.ly/3wCtife>).



Figuur 3. Shelly Smart Plug S (bron: <https://bit.ly/3D9TjtQ>).

Er zijn tegenwoordig tal van slimme stopcontacten verkrijgbaar die radiografisch of via WiFi worden aangestuurd. Wat hun functionaliteit en de netwerkverbinding (meestal WiFi) betreft, verschillen de verschillende modellen meestal slechts in de software en de bijbehorende cloud-service. Ook prijstechnisch zijn ze redelijk aan elkaar gewaagd. Interessant is hoe de verschillende fabrikanten hun producten daadwerkelijk hebben ontworpen. U hoeft maar te googelen op "smart plug" om het grote aanbod van dergelijke apparaten te zien (zie de voorbeelden in **figuren 1, 2 en 3**). Van buitenaf is het bijna onmogelijk om te achterhalen wat er van binnen zoal in kan zitten. Om dit nader te onderzoeken,

koos ik drie populaire smart plugs om voor dit onderzoek op te offeren. Ik was geïnteresseerd in deze vragen: welke componenten worden gebruikt? Hoe zijn deze bedraad? Kan het apparaat het verbruikte vermogen en de netspanning meten, en zo ja, hoe? Is er een overbelastingsbeveiliging?

De interessantste vragen zijn waarschijnlijk welke van deze modellen het gemakkelijkst te hacken zijn en of de standaard-firmware van de fabrikant verbeterd kan worden. Om deze vragen te beantwoorden heb ik de schema's van drie modellen getekend en (voor zover mogelijk) de gebruikte componenten geïdentificeerd. Zo werd niet alleen duidelijk welke microcontrollers waren ingebouwd,

maar kwamen ook enkele slimmigheden in het ontwerp aan het licht waarmee kosten bespaard konden worden.

De slimme stekkers

Voor een nader onderzoek concentreer ik me op drie contactdozen van verschillende fabrikanten: de EU6S van Aoyocor (**figuur 4**), de Tapo P100 van TP-Link (**figuur 5**) en de S26R2 van Sonoff (**figuur 6**). Daarnaast heb ik vrij recent ook nog een TRÅDFRI-contactdoos van IKEA uit elkaar gehaald (**figuren 7 en 8**) omdat ik een paar onderdelen voor een ander project wilde gebruiken.

Tabel 1 geeft de belangrijkste technische gegevens van de drie onderzochte contact-



Figuur 4. De Aoyococr EU6S.



Figuur 5. De TP-Link Tapo P100.



Figuur 6. De S26R2 van Sonoff.



Figuur 7. De TRÅDFRI van Ikea.



Figuur 8. Het inwendige van de TRÅDFRI.

dozen. De fabrikanten specificeerden een maximale laststroom van 10 A (2,3 kW bij 230 V $\approx$) voor de EU6S- en Tapo P100-modellen. Met de S26R2 verlegt Sonoff de grenzen van wat mogelijk is: deze gaat tot 16 A (3,6 kW bij 230 V $\approx$), wat handig is voor het schakelen van grotere belastingen zoals waterkokers of elektrische radiatoren.

Deze apparaten kunnen niet worden gerepareerd; ze kunnen alleen bij onbeschadigde behuizing veilig gebruikt worden. Ik kon alleen de EU6S en S26R2 smart plugs openmaken (en weer in elkaar zetten) zonder ze te vernielen. Helaas heeft de TP-Link Tapo P100 een gelijmde behuizing; hoewel het mogelijk is om die open te maken, zal hij daarbij beschadigd worden. Overigens, voor de TRÅDFRI-plug van IKEA was een ijzerzaag nodig, hij kon daarna niet meer worden gebruikt.

Aoyococr EU6S

De EU6S-behuizing wordt bijeengehouden door vier Y-profiel schroeven (figuur 9), zodat het binnenwerk vrij gemakkelijk toegankelijk is. Als het deksel eraf is, blijkt de print op zijn plaats te worden gehouden door twee schroeven in de live- en neutral-stekkerpinnen en die daar contact mee maken. Om die schroeven te bereiken, hebt u een geschikt gereedschap nodig (te vinden in de iFixit-kit uit de Elektorshop [1]). Figuur 10 toont de interne schroefdraad in de stekkerpinnen, waarop de print (figuur 11) wordt vastgeschroefd. Figuur 12

toont de onderdelenzijde van de print, waarop zich alle componenten behalve de voedings-aansluitingen bevinden. Deze layout maakt reverse engineering eenvoudiger.

Ik heb de print in drie functiegroepen verdeeld. Figuur 13 toont de voedingssectie (geel), de WiFi/MCU-module (oranje) en het relais inclusief bedrading (magenta). Shuntweerstand R7 en IC U3 (figuur 14) worden hier gebruikt om de stroom te meten die de geschakelde belasting trekt. Wat duidelijk ontbreekt in deze configuratie is een transformator die normaal zou zorgen voor galvanische scheiding in een

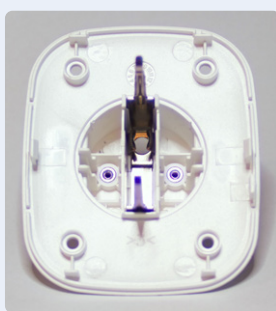
Tabel 1. Technische gegevens van drie smart plugs.

Naam	Max. belasting	WiFi	BLE	MCU/SoC
Aoyococr EU6S	2,3 kW (10 A @ 230 V $\approx$)	2,4 GHz	Nee	ESP8266
TP-Link Tapo P100	2,3 kW (10 A @ 230 V $\approx$)	2,4 GHz	Ja*	RTL8720CF
Sonoff S26R2	3,6 kW (16 A @ 230 V $\approx$)	2,4 GHz	Nee	ESP8285

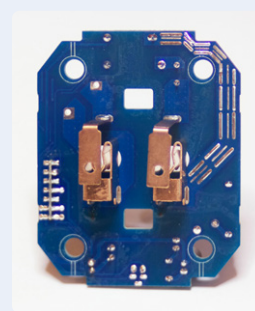
*alleen gebruikt om WiFi te configureren



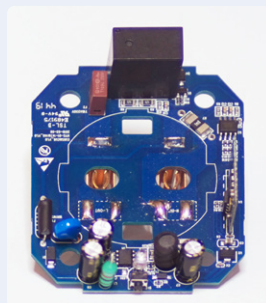
Figuur 9. De behuizing van de EU6S is met vier schroeven dichtgeschroefd.



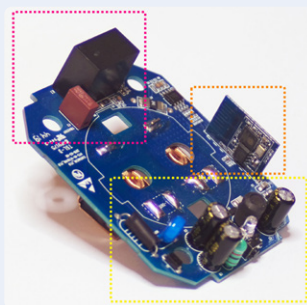
Figuur 10. Moeilijk bereikbare bevestiging van de EU6S-print.



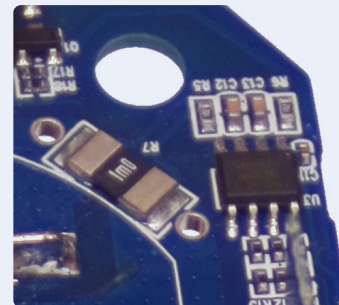
Figuur 11. Onderzijde van de EU6S-print met bevestiging.



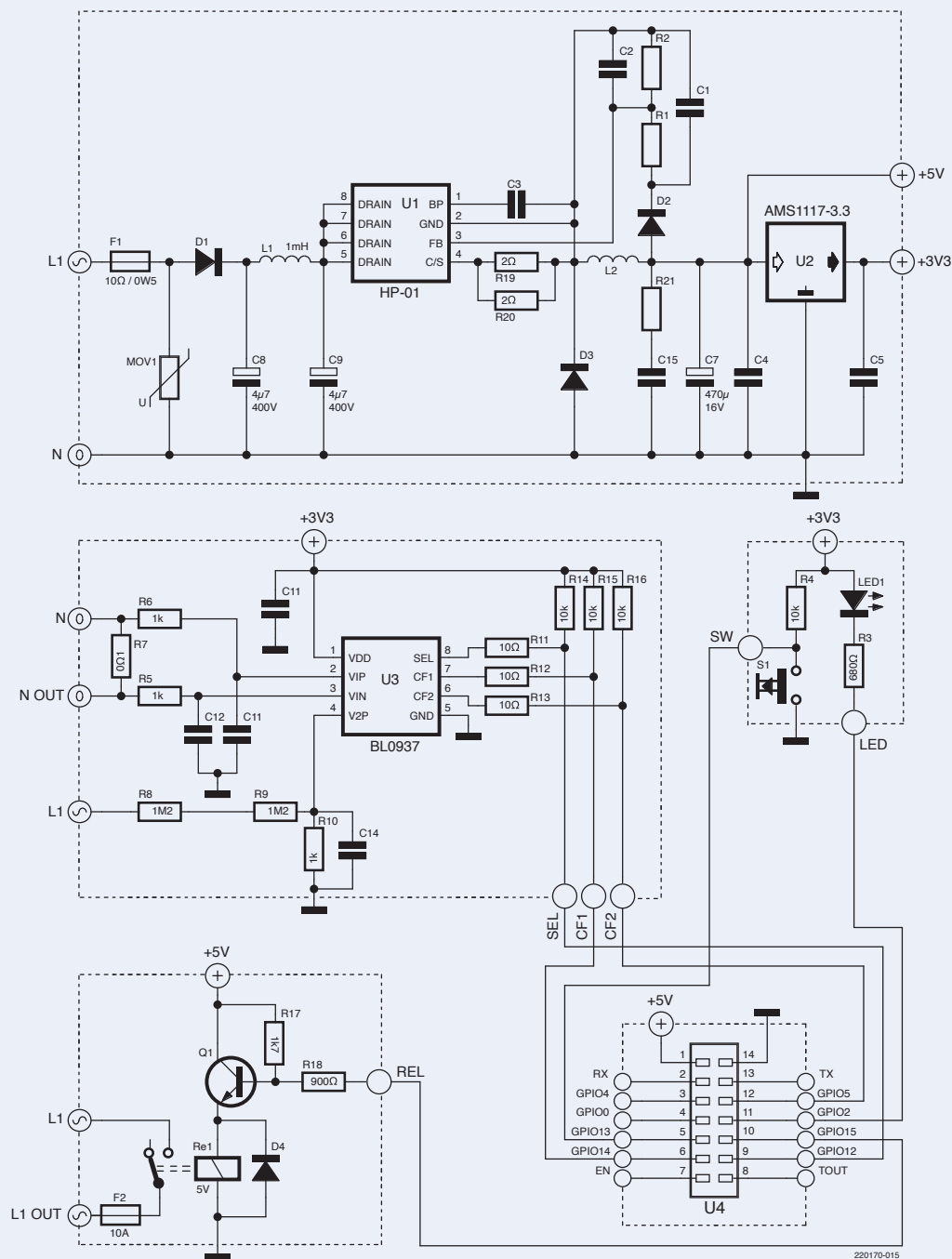
Figuur 12. Componentenzijde van de EU6S-print.



Figuur 13. Functiegroepen op de EU6S-print.



Figuur 14. Close-up van U3 en de shuntweerstand.



Figuur 15. Schema van de EU6S smart plug.

ontwerp met een schakelende voeding. Laten we die eerst eens bekijken.

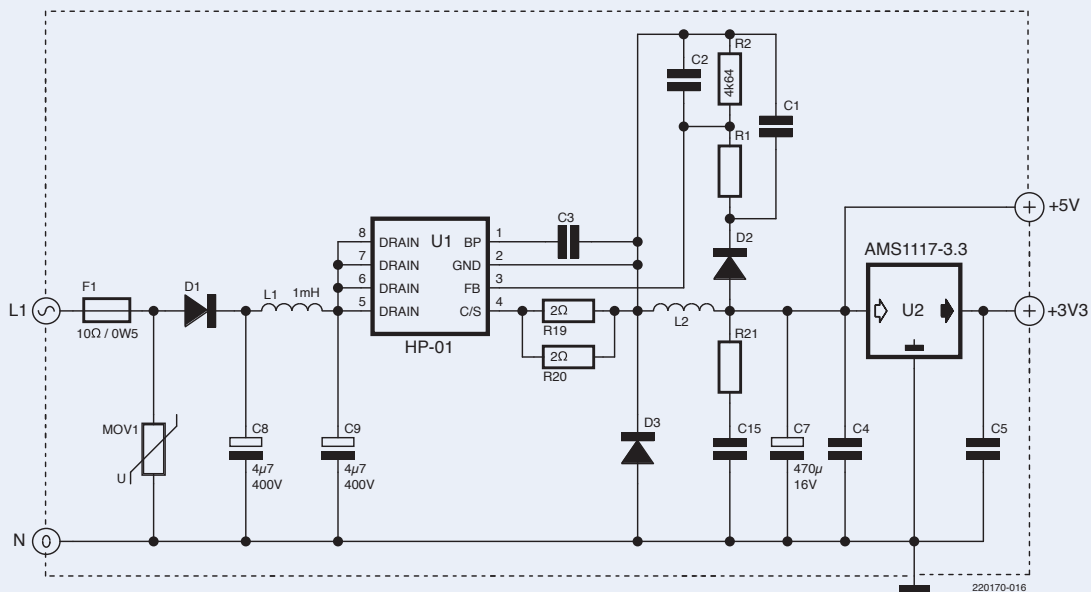
De voeding

In het bovenste gedeelte van **figuur 15** is het schema van de voeding te zien, opgebouwd rond IC U1 (HP-01 AL93PH.1, **figuur 16**). Helaas leverde een zoektocht op Internet geen datasheet voor dit IC op. Ik heb het schema

gereconstrueerd met alle componenten die op deze chip zijn aangesloten, om de functie van de diverse pinnen te achterhalen.

De netspanning komt links binnen via F1, een weerstand van 10 Ω die hier als 0,5W-zekeerling wordt gebruikt (**figuur 17**). Varistor MOV1 vormt de overspanningsbeveiliging. Diode D1 is een goedkope enkelzijdige gelijkrichter. C8, C9 en L1 vormen een pi-filter om de resul-

terende gelijkspanning af te vlakken. Deze spanning staat dan op pinnen 5..8 van U1. De twee parallelgeschakelde shuntweerstand R19 en R20, diode D3 en spoel L2 samen met het terugkoppelnetswerk gevormd door D2, C1, C2, R1 en R2 maken het waarschijnlijk dat U1 een schakelende buck-regelaar is die 5 V_{DC} maakt van de 325 V_{DC} op condensator C9, en die door condensator C7 wordt



Figuur 16. De belettering van de HP-01 AL93PH.1 (U1) was beter leesbaar met valse kleuren.

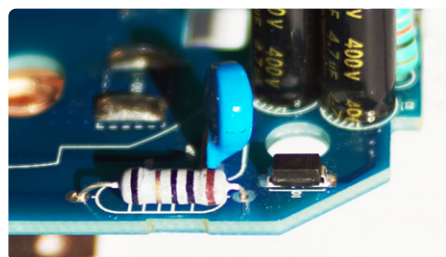
afgevlakt. De schakeling heeft 5 V nodig voor relais K1, waarmee de stroom naar de belasting wordt geschakeld.

IC U2 is de bekende AMS1117-3.3 lineaire low-drop regelaar die de 5 V omzet in een stabiele 3,3 V. Deze spanning is nodig voor de microcontroller en de WiFi-hardware, die

geen 5 V verdragen.

Ik heb vergelijkbare voedingsconfiguraties gezien in gewone lichtnet-LED-lampen met een E14- of E27-fitting. Hoewel ik geen datasheet kon vinden voor dit specifieke IC (U1), kan ik hieruit afleiden dat het een soortgelijke functie heeft als de MPS MP4050A [2] (figuur 18) of Power Integration LNK302 [3] (figuur 19) die vaak in LED-lampen worden gebruikt. Hun datasheets geven informatie over de pinning en aansluiting waaruit blijkt dat ze compatibel zijn met de functie van U1. **Figuur 20** toont het blokschema van het inwendige van de MPS MP4050A. Hoewel GND de referentie is voor het stuursignaal en de gatedriver, is die niet de referentie voor de uitgangsspanning. Het ligt voor de hand dat U1 hier op soortgelijke wijze wordt gebruikt.

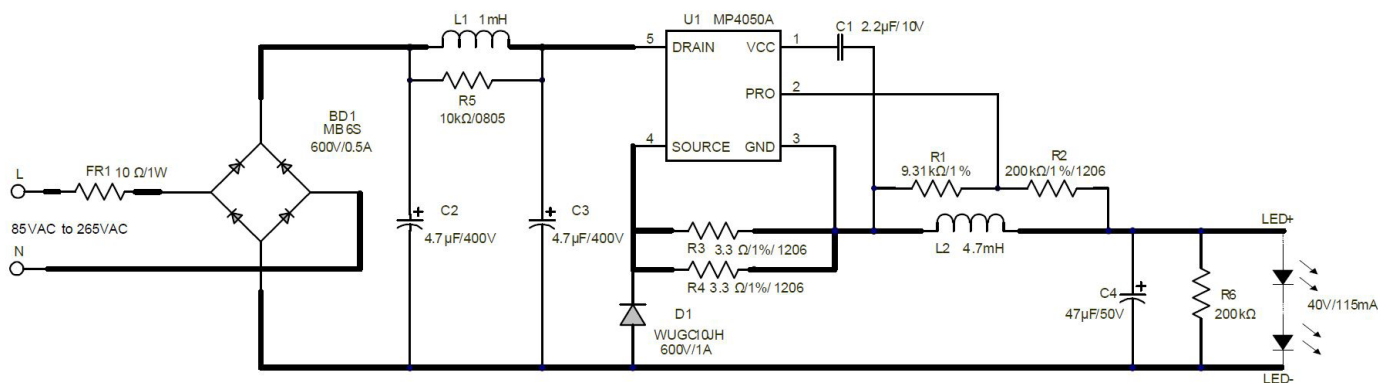
De bedrading en layout voor een toepassing met de MPS MP4050A is vergelijkbaar met de configuratie van U1 in de schakeling van de UE6S smart plug.



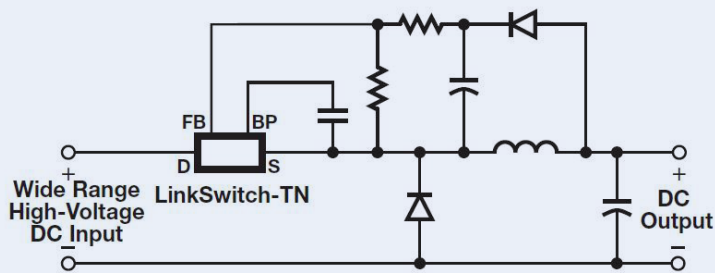
Figuur 17. F1 is een weerstand van 10 Ω.



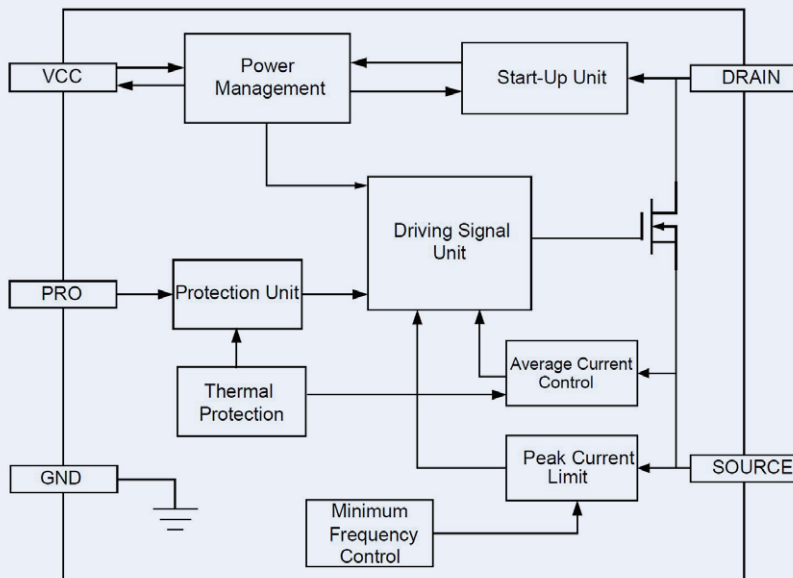
Opgepast! Bij gebruik van een niet-geïsoleerde voeding zonder galvanische scheiding kan de massa van de print dezelfde potentiaal hebben als de fase, afhankelijk van de polariteit van de bedrading van de contactdoos. Het aanraken van de massa van het schakeling en van bijna alle componenten en printen is daarom levensgevaarlijk!



Figuur 18. Toepassingsvoorbeeld met de MPS MP4050A (bron: [2]).



Figuur 19. Basisschakeling met de Power Integration LNK302 (bron: [3]).



Figuur 20. Intern blokschema van de MPS MP4050A (bron: [2]).

Het gebruik van niet-geïsoleerde DC/DC step-down converters is een goedkope manier om de elektronica in smart plugs en vele andere elektrische producten te voeden. De print en alle bedieningselementen en LED's zitten in een kunststof behuizing; bij normaal gebruik en met een intacte behuizing bestaat

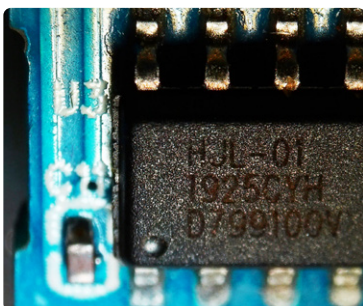
er geen gevaar dat u per ongeluk spanningvoerende onderdelen aanraakt. Alle elektrische producten moeten voorzien zijn van markeringen die aangeven dat zij voldoen aan de huidige normen voor elektrische veiligheid. De schakelende regelaar-IC's die in deze ontwerpen worden gebruikt, hebben

een breed ingangsspanningsbereik en werken vaak met wisselspanningen tussen 80 en 250 V (bij 50 en 60 Hz) zodat het product compatibel is met de netspanning waar ook ter wereld.

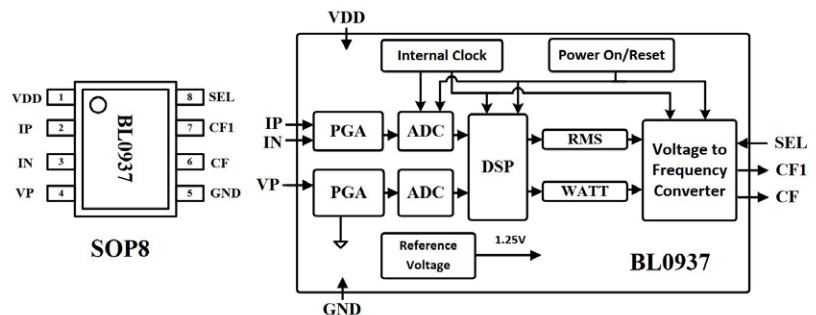
Metten van het vermogen

Deze smart plug kan de stroom en dus het vermogen meten en waarschijnlijk ook de stroom die aan de belasting wordt geleverd. Het deel van de schakeling links in figuur 15, met daarin U3, is verantwoordelijk voor deze functie. De belettering van U3 is te zien in **figuur 21**. Met wat moeite zien we "HJL-01" plus andere cijfers en letters, maar helaas was er op het internet geen spoor te vinden van een datasheet. Verder zoeken bracht gelijksoortige, pincompatibele chips aan het licht, zoals de BL0937 en de HLW8012. Aangezien U3 gevoed wordt met 3,3 V, lijkt hij waarschijnlijk meer op de BL0937, de HLW8012 heeft een 5V-voeding nodig. Blijft de vraag wat U3 doet?

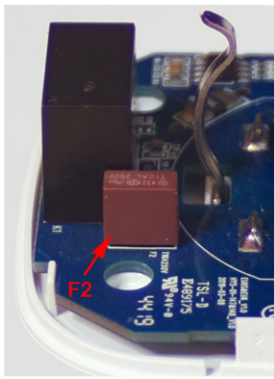
De BL0937 is een slim meet-IC voor smart plugs en vergelijkbare applicaties om het vermogen te meten in enkelfase-netwerken. De pinning en het blokschema van de BL0937 zijn te zien in **figuur 22**. Op pin CF van deze chip staan continue 38µs-pulsen met een herhalingsnelheid die evenredig is met het gemeten actieve vermogen. Pin CF1 levert een soortgelijke pulstrein met een herhalingsnelheid die een maat is voor de RMS-waarde van de actieve stroom (wanneer de SEL-ingang '0' is) of de RMS-waarde van de actieve spanning (als de SEL-ingang '1' is). Bij vergelijking van de schakeling rond U3 in figuur 15 met de referentieschakeling van de BL0937 uit het datasheet [4] valt op dat de waarden van de weerstandsdeler voor de spanningsmeting niet hetzelfde zijn. U3



Figuur 21. In de EU6S wordt een HJL-01 chip gebruikt.



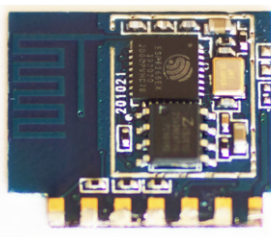
Figuur 22. Pinning en blokschema van de BL0937 (bron: [4]).



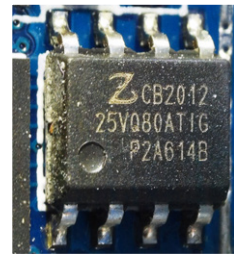
Figuur 23. De Aoyocor EU6S gebruikt een trage zekering van 10 A (F2).



Figuur 26. De TP-Link Tapo P100 is een compact apparaat.



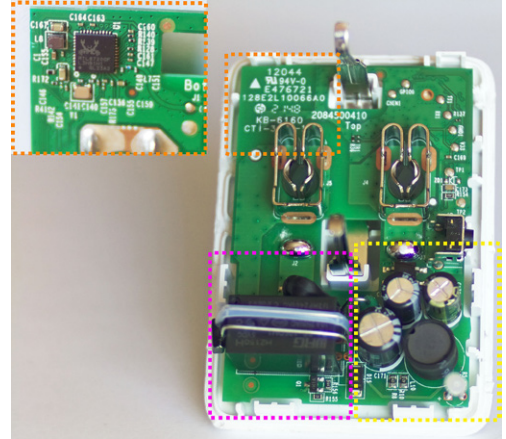
Figuur 24. De ESP8266-module.



Figuur 25. Een ZB25VQ80ATIG 8-Mb flash-IC.



Figuur 27. De pinnen in het midden zijn vastgesoldeerd.



Figuur 28. De printplaat kan in drie functionele secties worden verdeeld.

gebruikt een deler verhouding van 2400:1 in plaats van 1980:1 zoals bij de BL0937, wat belangrijk zou kunnen zijn als alternatieve firmware wordt overwogen.

De stroom wordt gemeten via de spanningsval over een shuntweerstand van 1 mΩ (R7) in de neutrale (N) aansluiting. De spanning over R7 gaat via R6 en R5 naar pinnen 2 en 3 van U3. Samen met C11 en C12 vormen zij een laagdoorlaatfilter die storingen op de licht-netspanning wegwerken.

De pinnen *SEL*, *CF1* en *CF* hebben serieweerstanden van 10 Ω en pull-up weerstanden van 10 kΩ voor de signalen, die vervolgens rechtstreeks naar de MCU-pinnen gaan. De interface is zo eenvoudig en goedkoop mogelijk. De HJL-01 chip is waarschijnlijk goedkoper dan een BL0937, die voor minder dan 60 dollarcent over de toonbank gaat. Ter vergelijking: het HLW8012 alternatief is ongeveer 30% duurder.

Het relais, de LED en de drukknop

Verbruikers die in het stopcontact zijn geprikt, worden geschakeld door relais K1, een NHLC 932-5VCD-SL-AH met een maximale belasting van 10 A bij 250 V_~. Relais met deze specificaties kosten doorgaans zo'n 50 dollarcent. De besturing is linksonder in figuur 15 getekend. De relaispoel Re1 ligt aan 5 V en wordt geschakeld door transistor Q1. Deze schakelt 5 V/0,4 W door de spoel op commando van het 3,3 V signaal van de controller. D4 zorgt ervoor dat de tegen-EMK die bij het

schakelen van de inductieve relaispoel wordt opgewekt, veilig naar de voedingsrail wordt afgevoerd.

De trage minizekering F2 (figuur 23) heeft een nominale stroomsterkte van 10 A en beschermt het relais en de print tegen beschadiging wanneer de geschakelde belasting te veel stroom trekt. De zekering kan gemakkelijk en goedkoop worden vervangen om de smart plug weer aan de praat te krijgen.

LED1 heeft een 680Ω-serieweerstand (figuur 15, midden rechts). Deze kleine stroom kan rechtstreeks door de MCU-pen *LED* worden geleverd. De drukknop-ingang heeft een 10-kΩ pull-up weerstand (R4).

De draadloze microcontroller

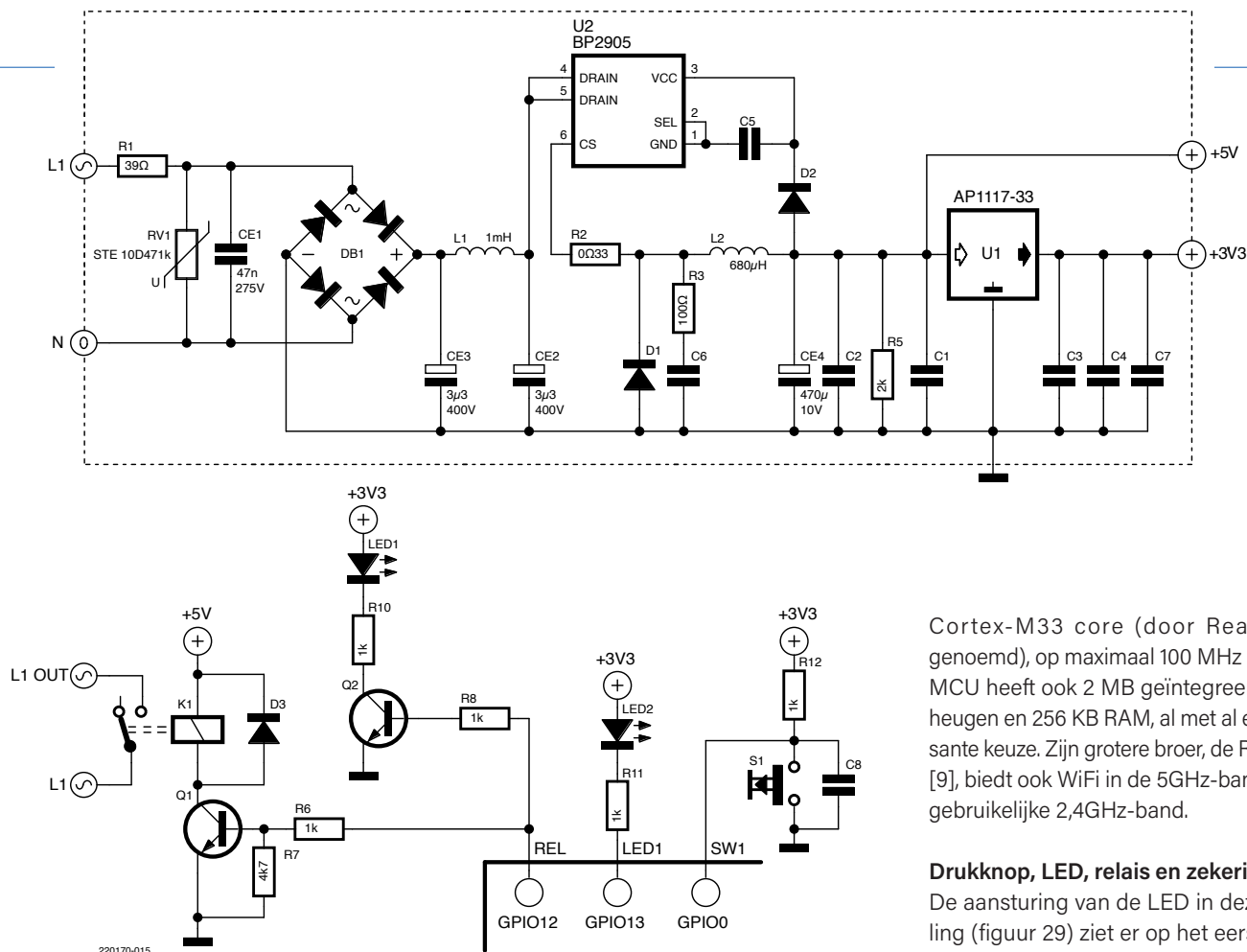
De MCU die hier wordt gebruikt is een ESP8266, met ingebouwde WiFi conform IEEE 802.11 b/g/n. Samen met enkele andere componenten zit die op een eigen klein printje (figuur 24) dat haaks op de hoofdprint is gemonteerd. Behalve een *RESET* is er geen ander testpunt op de module gemarkeerd. Naast de MCU zit een ZB25VQ80ATIG (flash-) geheugenchip met een capaciteit van 8 Mb (figuur 25). Ik heb dit kleine printje losgesoldeerd om te zien welke componenten met de ESP8266 verbonden zijn. Daarna kon ik de pintoewijzingen van de module afleiden en er functies aan toewijzen. Deze informatie is in het schema van figuur 15 verwerkt.

MCU's zoals de ESP8266 kunnen gemakkelijk van eigen firmware worden voorzien. Het is

bijvoorbeeld mogelijk om de MCU te besturen via ESPHome [5] of Tasmota [6]. Naast het aan-/uitschakelen van de belasting via het relais, is het ook mogelijk om het energieverbruik van het aangesloten apparaat te meten en uit te lezen. De metingen van U3 moeten echter ook gekalibreerd worden voordat men op de verzamelde gegevens kan vertrouwen. Alle programmeercontacten van de MCU bevinden zich aan de onderzijde van de print, zodat die uit de behuizing moet worden gehaald als u ESPHome of Tasmota naar de MCU wilt flashen. De schroeven zijn niet zo gemakkelijk te bereiken – het weer in elkaar zetten is moeilijker dan de demontage. U kunt de behuizing echter openen zonder die te beschadigen, wat een voordeel is.

De TP-Link Tapo P100

De Tapo P100-contactdoos (figuur 26) van TP-Link is veel compacter dan het product van Aoyocor. Aan de buitenkant zijn geen schroeven zichtbaar, want het Tapo P100 model heeft een behuizing waarvan de onderdelen met klemmen of clips bij elkaar worden gehouden. Het openen van de behuizing zal zijn sporen achterlaten, zelfs als u voorzichtig bent. Met het juiste gereedschap kunt u vrij snel bij het binnenwerk komen. Helaas kan de print niet zo gemakkelijk uit de behuizing worden gehaald, omdat hij aan de contacten van de stekkerpennen is gesoldeerd (figuur 27). Ik heb hem gedesoldeerd om de onderkant van de print te kunnen bekijken.



Figuur 34 Schema van de Sonoff S26R2.

De print kan (op basis van functionaliteit) ruwweg worden verdeeld in de drie secties voeding, relais en MCU, zoals in **figuur 28** aangegeven. Een IC om stroom te meten is in dit ontwerp niet aanwezig (**figuur 29**).

De voeding

De voedingsschakeling was gemakkelijk te achterhalen omdat de IC-labels leesbaar waren en de datasheets beschikbaar waren. De eerdere ervaring met de EU6S kwam van pas: ook hier zien we een 10Ω-weerstand (R168) – nu met een vermogen van 2 W – als zekering en stroombegrenzer. De hoofchip U4 is een schakelende regelaar van het type BP2525 [7] (**figuur 30**). Ook hier wordt een niet-geïsoleerde step-down converter gebruikt; deze genereert (selecteerbaar) 5 V of 3,3 V uit maximaal 500 VDC aan de ingang. Een bruggelijkrichter zet de wisselspanning om in een gelijkspanning, die vervolgens wordt afgevlakt met een pi-filter bestaande uit C176, L101 en C171.

U4 levert (afhankelijk van de uitvoering) een uitgangsspanning van 5 V bij maximaal 500 mA. De bedrading is gemakkelijk te begrijpen uit het gegevensblad en de componenten zijn goed te identificeren. Er is niet veel verschil met de EU6S-voeding. Er wordt geen spanning van 3,3 V gegenereerd in dit ontwerp. De hier gebruikte MCU (zie verderop) maakt duidelijk waarom dit het geval is.

De RTL8720CF met WiFi en BLE

De Tapo P100 gebruikt niet de alomtegenwoordige ESP8266-microcontroller maar in plaats daarvan de RTL8720CF van Realtek (**figuur 31**). De datasheet [8] geeft aan dat deze aan een enkele 5V-voeding genoeg heeft omdat hij zelf een 3,3V-regelaar aan boord heeft. De maximale belasting van deze 3,3V-voeding bedraagt 450 mA. WiFi wordt ondersteund in de 2,4GHz-band en Bluetooth Low Energy 4.2 is ook beschikbaar. De MCU is gebaseerd op een ARM

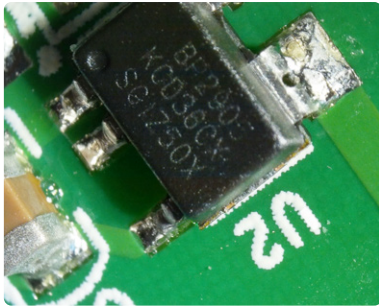
Cortex-M33 core (door Realtek KM4 genoemd), op maximaal 100 MHz geklokt. De MCU heeft ook 2 MB geïntegreerd flashgeheugen en 256 KB RAM, al met al een interessante keuze. Zijn grotere broer, de RTL8720DN [9], biedt ook WiFi in de 5GHz-band naast de gebruikelijke 2,4GHz-band.

Drukknop, LED, relais en zekering

De aansturing van de LED in deze schakeling (**figuur 29**) ziet er op het eerste gezicht een beetje vreemd uit. Weerstand R5 en een tweekleurige LED D10 worden rechtstreeks aangesloten tussen de pinnen *GPIOA_9* en *GPIOA_10* van de microcontroller. Via PWM-signalen op deze twee pinnen kan een reeks LED-kleuren worden geproduceerd. Transistor Q1 schakelt het relais en D14 dient als vrijloopdiode. *GPIOA_7* stuurt de basis van Q1 aan via R155. R158 fungeert als pull-down weerstand, zodat de transistor uitgeschakeld blijft tijdens het laden van de firmware bij het opstarten. Bijzonder is hier F2 (**figuur 32**). Deze niet-resetbare thermische zekering (AUPO A1-1A-F [10]) barst bij oververhitting open wanneer het relais wordt overbelast. Hierdoor wordt de stroom naar de spoel onderbroken, zodat het relais uitvalt en afkoelt, maar de zekering wordt niet gereset. Vervanging van de zekering is tamelijk lastig, zodat alle P100-toestellen die dit lot beschoren is, waarschijnlijk deel zullen worden van de groeiende berg elektronisch afval. De ingebouwde knop is klassiek aangesloten met een pull-up weerstand van 10 kΩ naar 3,3 V, een condensator voor het ontdenderen en een weerstand van 100 Ω naar *GPIOA_17*.

De Sonoff S26R2TPF

Tegen de tijd dat ik aan de demontage van de Sonoff toe was, wist ik wat ik kon verwachten en was ik alleen maar nieuws-



Figuur 35. De BP2905 is compatibel met de BP2525.

gierig naar de manier waarop de verschillende functies waren geïmplementeerd. Het model S26R2TPF van Sonoff (figuur 33) kan maximaal 16 A schakelen bij 250 V; het schema is gereconstrueerd in figuur 34.

De voeding

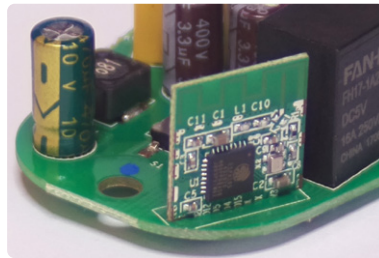
Het voedingsgedeelte is opgebouwd rond U2, een schakelende regelaar met het opschrift BP2905 (figuur 35). Helaas kon ik hier geen datasheet van vinden. Uit het ontwerp van de behuizing, de pinnen en de bedrading naar externe componenten kan worden afgeleid dat het hoogstwaarschijnlijk een pincompatibel familielid is van de BP2525.

Ook in deze schakeling fungeert weerstand R1 als zekering. De bruggelijkrichter DB1 wordt gevolgd door een pi-filter bestaande uit CE2, L1 en CE3. De BP2905 produceert een stabiele 5 V over buffercondensator CE4. Net als bij de EU6S wordt een lineaire spanningsregelaar gebruikt die de 3,3 V voor U1 levert.

Drukknop, relais en LED

De bedrading van de knop S1 is eenvoudig en vereist slechts een pull-up weerstand van 1 kΩ plus een condensator voor de ontddering. Hij wordt rechtstreeks aangesloten op de SW1-ingang van de MCU, zonder enige serieweerstand.

De anode van LED2 ligt aan de 3,3V-voeding, terwijl de kathode via serieweerstand R11 wordt geschakeld door een GPIO-pin van de MCU. LED1 wordt gevoed vanuit de 3,3V-voeding en heeft een eigen stuurtransistor Q2 die wordt geschakeld door hetzelfde GPIO-sigitaal van de MCU dat het relais bedient. Deze LED geeft aan wanneer de belasting is ingeschakeld. Het relais is aangesloten zoals in de eerdere varianten, waarbij één aansluiting van de spoel aan 5 V ligt en de andere aansluiting via Q1 naar massa wordt geschakeld met een 3,3V-stuursigitaal van de MCU. Een diode (D3) over de spoel maakt de tegen-EMK van de spoel weer onschadelijk. Net als bij de andere twee modellen voorkomt een weerstand tussen de basis en de emitter van



Figuur 36. De ESP8285-module in de S26R2.

de schakeltransistor dat het relais onbedoeld schakelt tijdens het opstarten.

De draadloze MCU

De ESP8285-MCU (U1) zit op een eigen miniprintje, dat haaks op de hoofdprint is gemonteerd (figuur 36). Dankzij het geïntegreerde flashgeheugen heeft deze ESP8266-variant geen separaat flash-IC nodig. De pinning is te vinden in het schema van figuur 34.

Software om een andere cloud te gebruiken

Hoewel we ons hebben geconcentreerd op de hardwareaspecten van smart plugs, kunnen we ook nadenken over het gebruik van het apparaat en de connectiviteit met een cloudgebaseerde server. De software van de fabrikant verbindt de plug meestal met WiFi thuis en moet vervolgens via een app worden geconfigureerd, zodat de smart plug kan worden gebruikt met een smartphone, Amazons Alexa, Google's Home of Apple's Homekit. Veel smart plugs maken gebruik van de cloudservice van een provider die ergens in de ether zijn servers heeft gehost en die uiteindelijk ook toegang hebben tot apparaat. Deze configuratie maakt het dan mogelijk om belastingen op afstand via het internet te schakelen. Helaas is zo'n cloud-verbinding niet volmaakt betrouwbaar, aangezien er geen garantie is dat een cloud-provider zijn service van de ene dag op de andere niet domweg staakt [11].

Zoals gezegd zijn er alternatieven voor smart plugs op basis van de ESP8266 wanneer we de open-source firmware TASMOTA [6] of ESPHome [5] installeren. Deze vervanging van de originele firmware maakt het dan mogelijk om het apparaat via uw eigen LAN te besturen via MQTT, WebUI, Alexa of andere protocollen. Als u geïnteresseerd bent in het gebruik van alternatieve firmware op de apparaten, is Tuya-Convert een zeer nuttige website over dit onderwerp [12]. Een aantal van deze smart plugs kan zelfs worden geflasht met alternatieve firmware zonder de noodzaak om de unit

fysiek te openen. Als uw model geopend moet worden, kunnen de meeste ESP8266-MCU's opnieuw geflasht worden met behulp van de Tasmotizer [13]. De juiste instellingen moeten worden gemaakt in overeenstemming met het model in kwestie.

Als u ESPHome wilt gebruiken, kunt u dit op sommige plugs over-the-air (OTA) via WiFi installeren zonder de behuizing te openen [14]. Bij sommige modellen zult u echter uw toevlucht moeten nemen tot schroevendraaier en soldeerbout.



Tweede waarschuwing: zoals uit dit artikel blijkt, gebruiken alle hier besproken plugs niet-geïsoleerde voedingen. Dat betekent dat delen van de schakeling onder piekspanning staan (bijna 400 V in Europa). Dit kan dodelijk zijn als u op een of andere manier daarmee in aanraking komt. Het veilige gebruik van deze smart plugs is gebaseerd op de integriteit van de isolerende behuizing om de consument te beschermen. Het aanraken van interne onderdelen tijdens gebruik is levensgevaarlijk. We kunnen het niet vaak genoeg zeggen: werk nooit aan schakelingen onder spanning en volg altijd de vigerende veiligheidsvoorschriften. Bovendien: de in de voedingsschakelingen gebruikte condensatoren aan de netspanningszijde kunnen na het uitschakelen nog geruime tijd geladen blijven en een hoogspanning van enkele honderden volt voeren. Alvorens aan deze (niet onder spanning staande) printen te werken, dient u ze voor alle zekerheid te ontladen.

ESP8266, ESP8285, RTL8720 en consorten

Als u nu overweegt om een smart plug te kopen met de bedoeling om alternatieve firmware te installeren, let er dan op dat zowel ESPHome als Tasmota momenteel alleen IC's uit de ESP-familie ondersteunen. Hoewel er voldoende documentatie is voor de RTL8720CF, betekent dit niet dat alternatieve firmware-ondersteuning beschikbaar is.



Naast de MCU's die we zijn tegengekomen, treft u wellicht andere typen zoals de Realtek RTL8710, Beken BK7231T of de XradioTech XR809 in andere merken smart plugs aan. Zoals altijd is het verstandig om voor aankoop zoveel mogelijk achtergrondonderzoek te doen. Als u geluk hebt, heeft een andere toegewijde knutselaar al het harde analysewerk gedaan en zijn bevindingen op het web gepubliceerd. Een ander belangrijk aspect is dat fabrikanten hun producten in een bepaalde reeks in de loop van de tijd plegen te optimaliseren, waarbij (bijvoorbeeld) een andere MCU wordt geïnstalleerd, waardoor het moeilijker (of interessanter) wordt om ze aan te passen.

Een handige hack

We ontdekten dat alle drie onderzochte smart plugs erg op elkaar lijken. Een niet-geïsoleerde voeding brengt de netspanning omlaag om een MCU met WiFi te voeden die een relais aanstuurt. De implementatie kan variëren – zoals de bescherming, de LED-aansturing of de toevoeging van een smart meter-IC. Hoewel IKEA's TRÅDFRI hier slechts zijdelings is genoemd, kan ik u wel verraden dat er ook in dat ontwerp niets bijzonders te ontdekken valt. Het was zeker leerzaam voor mij om in deze producten te hacken. Ik kreeg inzicht in een aantal veiligheidsaspecten van het ontwerp en hoe 'optimalisaties' de kosten kunnen drukken, wat een bijzonder belangrijk criterium is bij het ontwerpen van consumentenproducten die in grote aantallen geproduceerd worden. Ik kan die kennis gebruiken om andere producten te

beoordelen en de schakelingen als inspiratiebron gebruiken voor toekomstige projecten. Hebt u al eens gesleuteld aan smart plugs? Deel dan uw ervaringen (goede of slechte) met ons. Alle ongewone bevindingen en inzichten in het ontwerp van andere slimme stekkers zijn zeer welkom en kunnen anderen helpen. ◀

220170-03

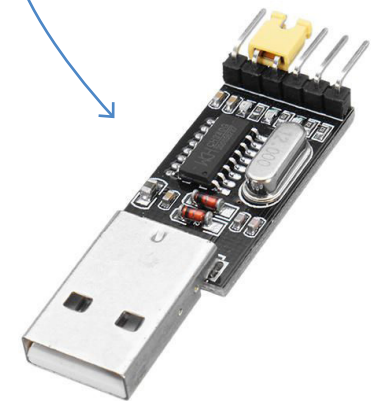
Vragen of opmerkingen?

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



GERELATEERDE PRODUCTEN

- > **Koen Vervloesem, Getting Started with ESPHome (Elektor 2021) (SKU 19738)**
www.elektor.nl/19738
- > **CH340 USB/TTL Converter Module CH340G (3.3 V/5.5 V) (SKU 19151)**
www.elektor.nl/19151
- > **OWON OW18B Digital Multimeter with Bluetooth (SKU 18777)**
www.elektor.nl/18777



WEBLINKS

- [1] iFixit Pro Tech Bit Set: www.elektor.com/ifixit-pro-tech-toolkit
- [2] MP4050A: www.monolithicpower.com/en/mp4050a.html
- [3] Power Integrations LNK302: www.power.com/products/linkswitch/linkswitch-tn/lnk302dg
- [4] BL0937: <https://bit.ly/37KY7Uo>
- [5] ESPHome: <https://esphome.io/>
- [6] Tasmota: <https://tasmota.github.io/docs/>
- [7] MP2565: www.monolithicpower.com/en/mp2565.html
- [8] RTL8720CF: <https://bit.ly/3DbrJ8Z>
- [9] RTL872xD: <https://bit.ly/3JESUf2>
- [10] AUPO A1-1A-F: www.tme.eu/en/details/a1-1a-f/thermal-fuses/aupo/
- [11] N. Statt, "Nest is permanently disabling the Revolv smart home hub," The Verge, April 4, 2016: <https://bit.ly/3ICGi6O>
- [12] Tuya Convert: <https://tasmota.github.io/docs/Tuya-Convert>
- [13] Tasmotizer: <https://github.com/tasmota/tasmotizer>
- [14] ESPHome OTA Installation: <https://bit.ly/3Jlps9>