Nachträge

Controller & Zubehör lässt sich günstig mit Rechnung von https://www.az-delivery.de/?ls=de bestellen. Mengenrabatte & Kombipakete beachten

https://fritzing.org/home/ ist ideal um Boards vorab „virtuell“ zu designen und am Beamer etc zu präsentieren

LANDWEHR
software

Programm

- Introduction
  - Wer bin ich?
  - NodeMCU ESP 8266?
  - Warum IT-Sicherheit anhand von ESP 8266 ?!
- Mögliche Unterrichtsinhalte
- Mit dem ESP 8266 spielen

WLAN “NoFreeWifi” verbinden, Abcd1234

LANDWEHR
partner-netzwerk

Vorstellung

Michael Plas

ABI'11 am TG / GBS Nordhorn
FISI'14 bei LANDWEHR / BBS Lingen

Bei LANDWEHR

- IT-Sicherheitsbeauftragter
- LANDWEHR Cloud Administrator

Im Privatleben

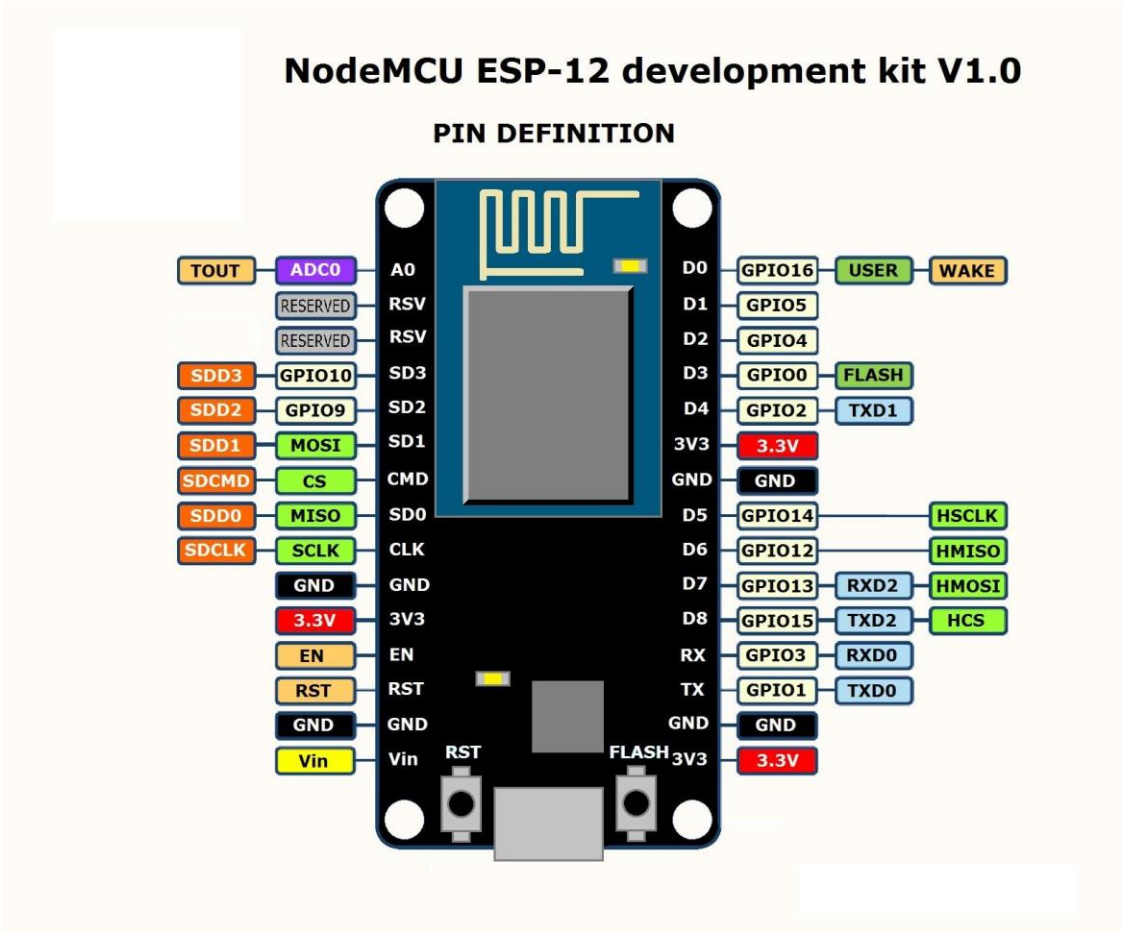
- Aktivist
- Weltenbummler

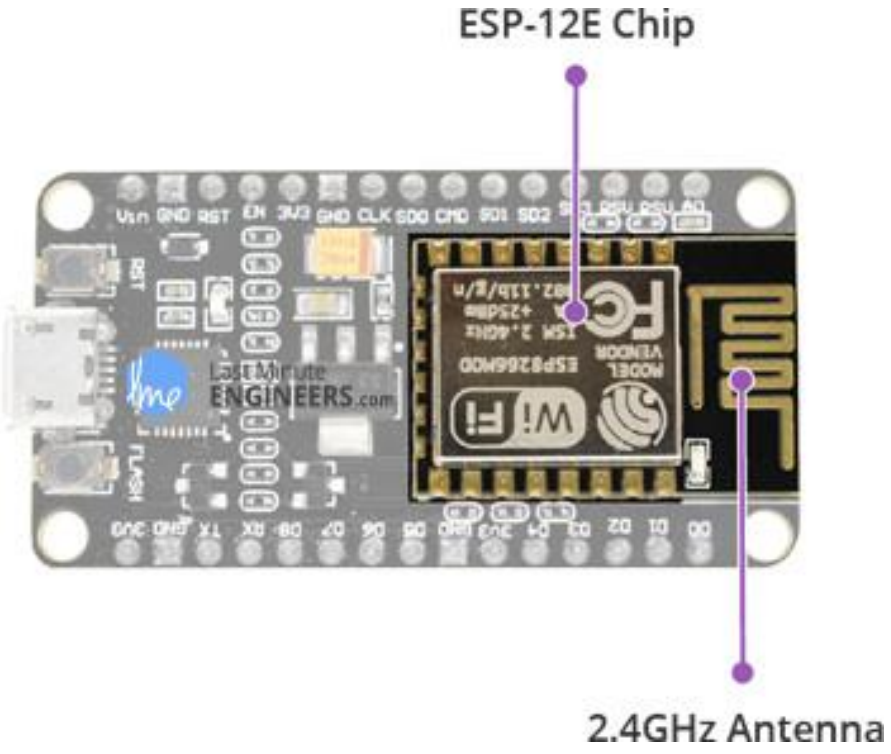
NodeMCU ESP 8266

NodeMCU ESP 8266 ist eine Open Source IOT Plattform für die Entwicklung von IOT-Devices mit ein paar Zeilen Lua Script.

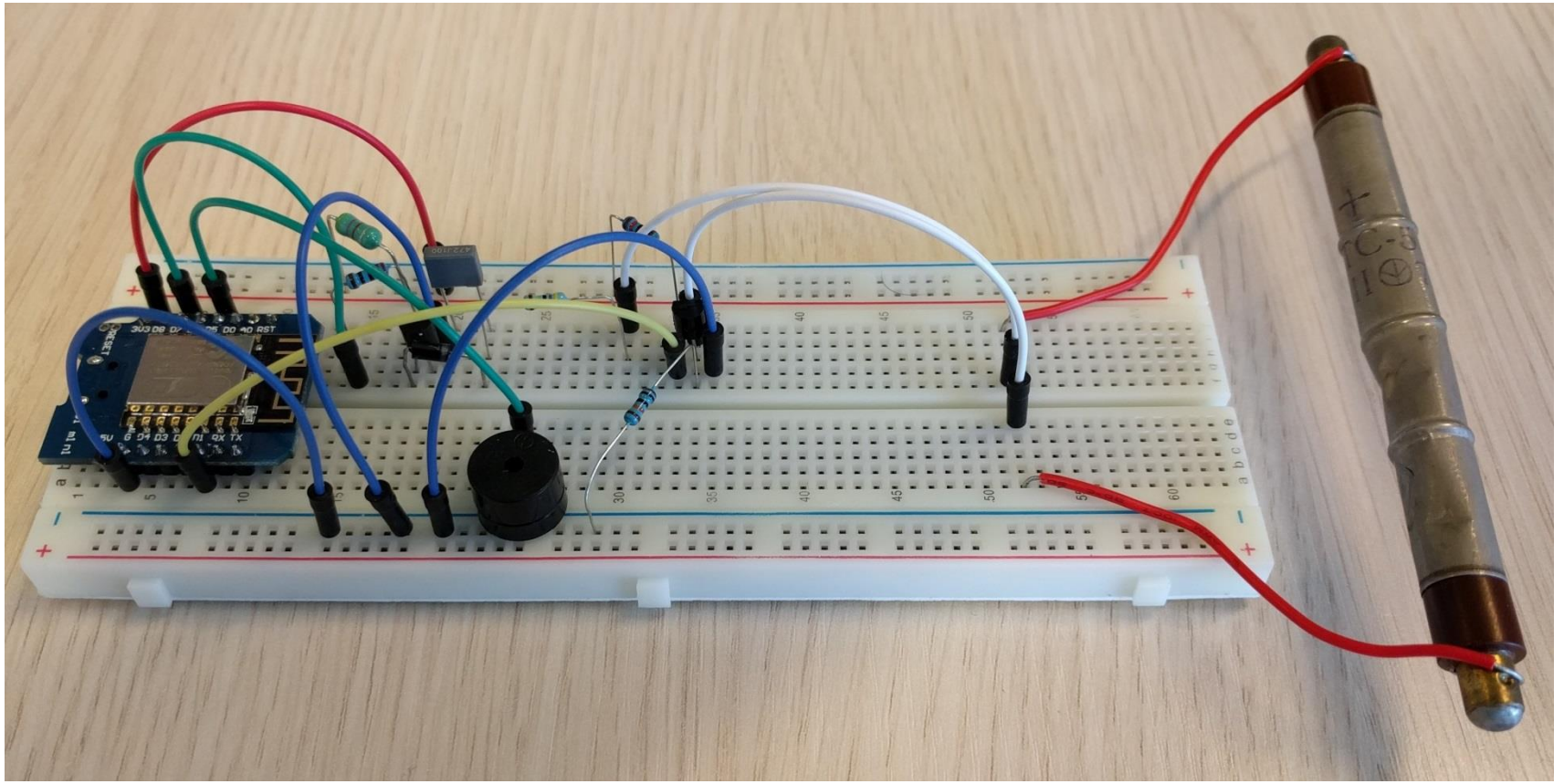
- Ähnlich dem Arduino
- Hauptkompontente ESP 8266
- Mit programmierbaren Pins
- Und eingebautem WLAN (!)
- Stromversorgung über USB oder Pin‘s
- 3.3V, 250mA
- Kostet keine 5 Euro

NodeMCU ESP 8266

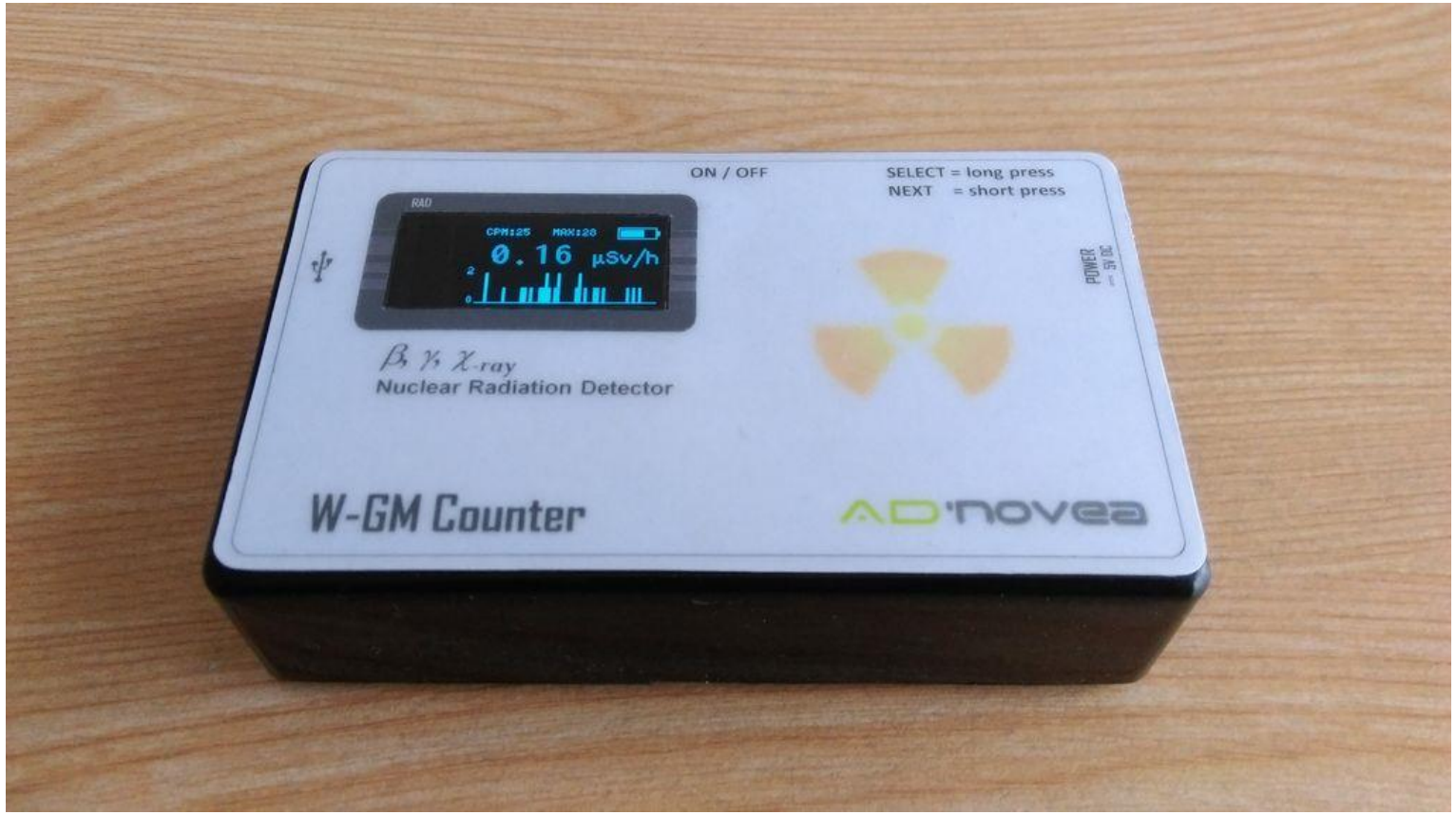




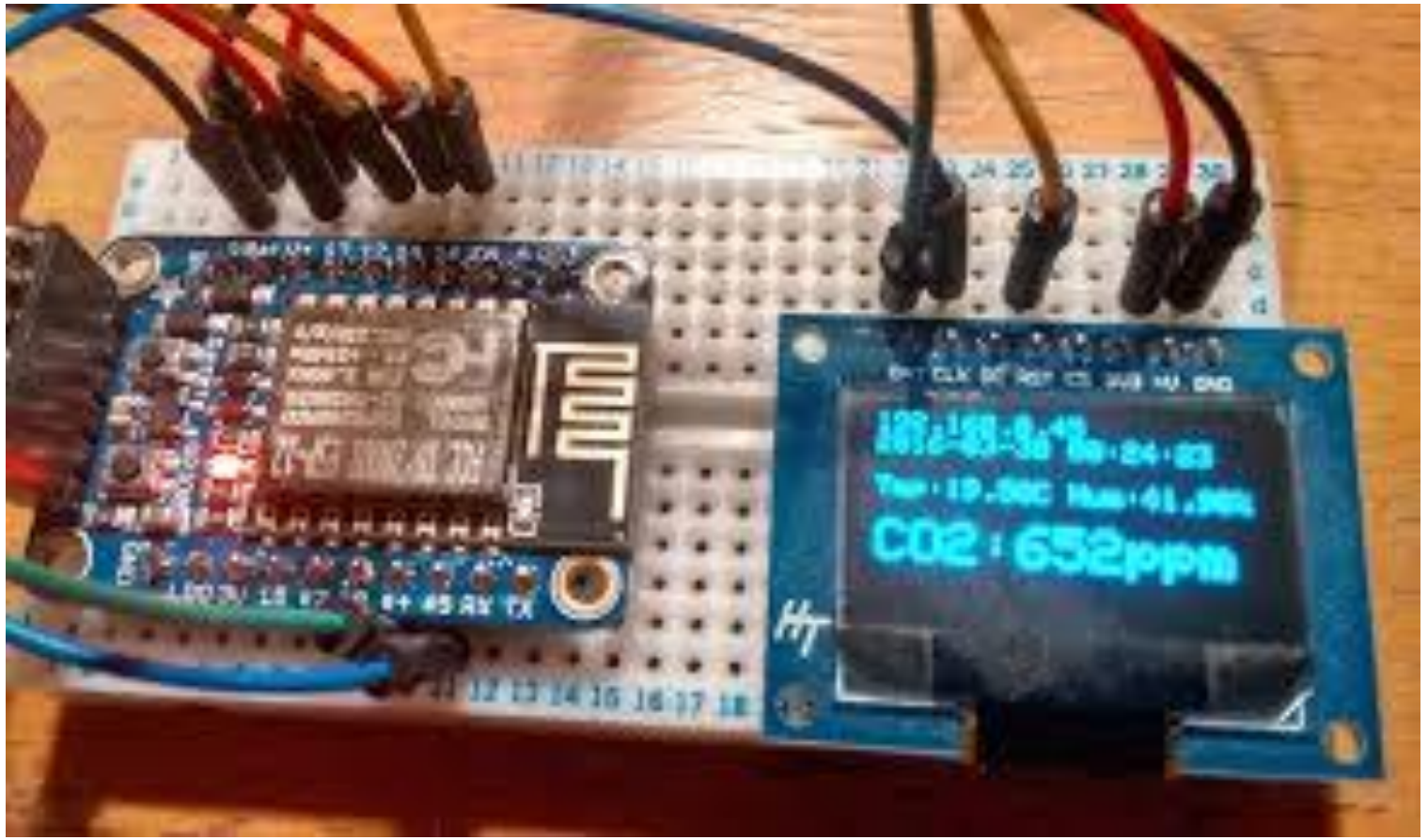
ESP8266 Anwendungen



ESP8266 Anwendungen



ESP8266 Anwendungen



ESP8266 Anwendungen

Mögliche Anwendungen / Ideen

https://hackaday.io/projects?tag=ESP8266 kennt 942 Projekte

Bei LANDWEHR: Kaffeefüllstand an Telegram-Api / Chat übermitteln

Aber was ist nun mit IT-Sicherheit?!

- IOT Devices, wie solche die auf ESP8266 basieren, verwenden, gibt es zu Millionen. Oft werden diese ohne Sicherheitsaudits & Funktionen ausgeliefert.

- Aber die sind doch nur im Heimischen WLAN….

→Hacker bringt Schadcode auf einen PC / Smartphone, diese schaut nach IOT‘s und führt angriffe durch

→Angriffe „over the air“

→Angriffe auf die Cloudsysteme der Smart-Device/Home Anbieter

Aber was ist nun mit IT-Sicherheit?!

- Thermometer Shares Casino’s Customer Data
- Light Bulb Shares Your Wi-Fi Password
- IoT-Powered Botnet Takes Down the Web (ESP8266! Password in FLASH)
- Smart Speaker Records Private Conversation
- smartTV show False Nuclear Missile Alert
- Implanted Cardiac Devices Could Have Been Hacked
- Hackers Take Control of a Jeep

LANDWEHR
partner-netzwerk

WLAN Hacks mit esp8266 deauther

Mögliche Inhalte für einen Schulunterricht

Im Schulungsblock Softwareentwicklung oder auch Elektrotechnik:

Eigene Anwendung z.B. Sensor der Daten übermittelt entwickeln

Mögliche Inhalte für einen Schulunterricht

Im Schulungsblock Netzwerk-Technik WLAN

Simple Angriffsszenarien WLAN wie Deauthing, Broadcaststorms, usw. zeigen

Komplexe Angriffsszenarien wie Man-In-The-Middle zeigen (auch super mit Wireshark!)

Mögliche Inhalte für einen Schulunterricht

Im Schulungsblock Netzwerk-Technik WLAN oder auch Elektrotechnik:

WLAN, RFID, 866MHZ usw. sind Funkübertragungstechniken und somit angreifbar by Design.

- Tolle Beispiele:
  - Unverschlüsselte E-Tankstellen, kein Standard, fast alles hackbar
  - RFID in Geldkarten
  - Geragentore, Türschlösser

WLAN Sicherheit wie WPA2, IEEE_802.1X,

Mögliche Inhalte für einen Schulunterricht

Im Schulungsblock Netzwerk-Technik :

Aufklärung:

Wenn ich einmal ein WLAN-Netzwerk gespeichert habe, verbindet sich mein Gerät meist automatisch mit dem Netz. Beispiel: Hotspot der DB oder LANDWEHR-Gast.

Mein Handy sendet permanent Informationen zu gespeicherten WLAN‘s

Mit Hardware wie dem ESP oder Routern kann eine MAN-IN-THE-MIDDLE Attacke durchgeführt werden und Daten geklaut oder eingeschleust werden

FRAGEN?

Los gehts

LANDWEHR
partner-netzwerk

1. Mit WLAN “NoFreeWifi” verbinden, Abcd1234
2. arduino-1.8.9-windows.exe von https://www.arduino.cc/en/main/software herunterladen & vollständig installieren
3. Arduino IDE starten
4. Datei -> Voreinstellungen -> zusätzliche URLs: https://arduino.esp8266.com/stable/package_esp8266com_index.json eintragen
5. Werkzeuge -> Board: „Arduino“ -> Boardverwalter -> esp8266 installieren
6. Werkzeuge -> Board: „Arduino“ -> Auf „NodeMCU 1.0“ stellen
7. Demosketch2 von http://webserver.schulung herunterladen und auf den ESP hochladen
8. PIN D6 (24R) mit LED+ (1L) und GND (25L) mit LED- (2L) verbinden
9. espXX. schulung im Browser aufrufen. XX durch ESP01-15 ersetzen

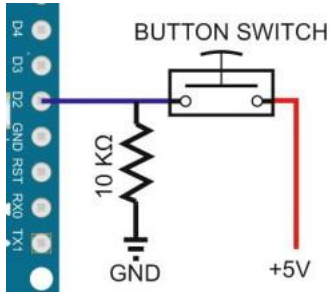
Hinweis: Ggf. muss der USB-Stecker 1-3 mal neu gesteckt werden bis

LANDWEHR
partner-netzwerk

Was haben wir gemacht?

Weitere Aufgaben

- Gruppe 1 (die mit dem Schalter)
  - Aufgabe Schalter herunterladen
  - Aufspielen
  - Schalter verkabeln
  - Schalter drücken
  - Beschreiben was passiert



- Gruppe 2 (die mit dem weißen Sensor)
  - In der Bibliotheksverwaltung: „Adafruit Unified Sensor“ und „DHT sensor library“ einspielen
  - Aufgabe Temperatursensor aufspielen
  - Sensor mit dem Board verkabeln (Hint: DHTPIN ist für den Datenkanal)
  - Werkzeuge -> Serieller Monitor starten (Baudrate 9600)

- Gruppe 3 (die mit dem Funkmodul)
  - rc-switch-2.6.2.zip von http://webserver.schulung herunterladen und über Sketch -> Bibliothek einbinden -> .ZIP hinzufügen
  - Aufgabe Funkschalter herunterladen
  - Aufspielen
    Sensor mit dem Board verkabeln (Hint: D4 ist der Datenkanal)
  - Wofür könnte die Kombi 1111 und 01000 bzw. 10000 stehen?

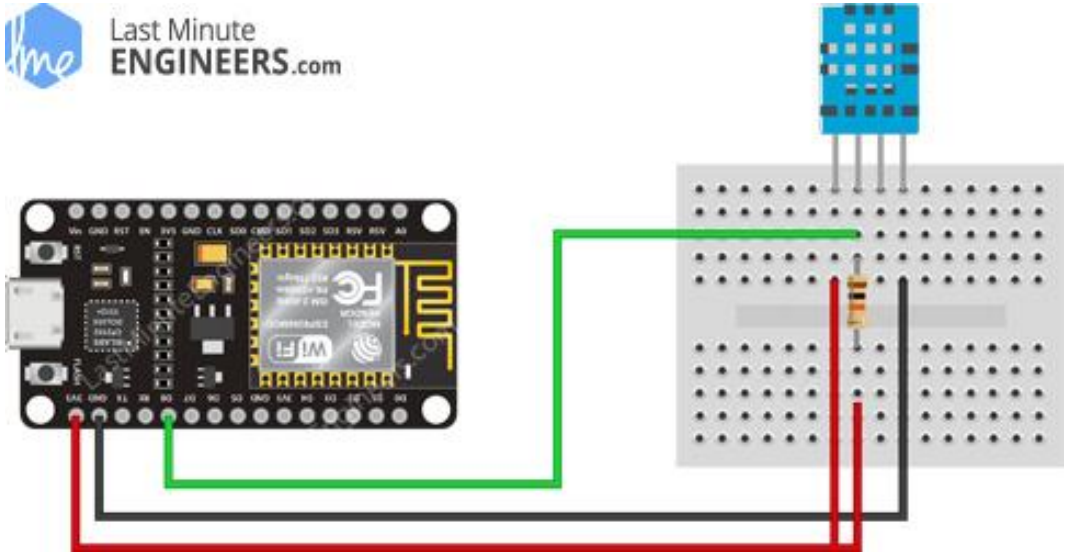
Weitere Aufgaben

- Gruppe 1 (die mit dem Schalter)
  - Nutzt HTTP Client um eine Anfrage an http://webserver.schulung/api.php?host=espXX&push=onoff zu senden
  - Schaut auf dem Webserver, dort erscheint ein Log-File
  - Schaltet zusätzlich über den Schalter die LED aus Übung 1

- Gruppe 3 (die mit dem Funkmodul)
  - Baut einen Webserver wie in Aufgabe 1 & steuert die Steckdose über den Webserver

- Gruppe 2 (die mit dem weißen Sensor)
  - Nutzt HTTP Client um eine Anfrage an http://webserver.schulung/api.php?host=espXX&temperatur=YY zu senden
  - Schaut auf dem Webserver, dort erscheint ein Log

Weitere Aufgaben



LANDWEHR
software

Haben Sie noch Fragen?