

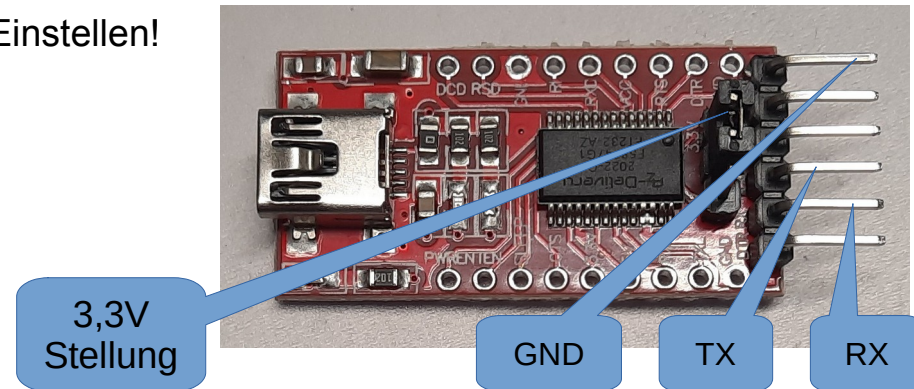


Hardware Hacking Board

Übung und Challenge

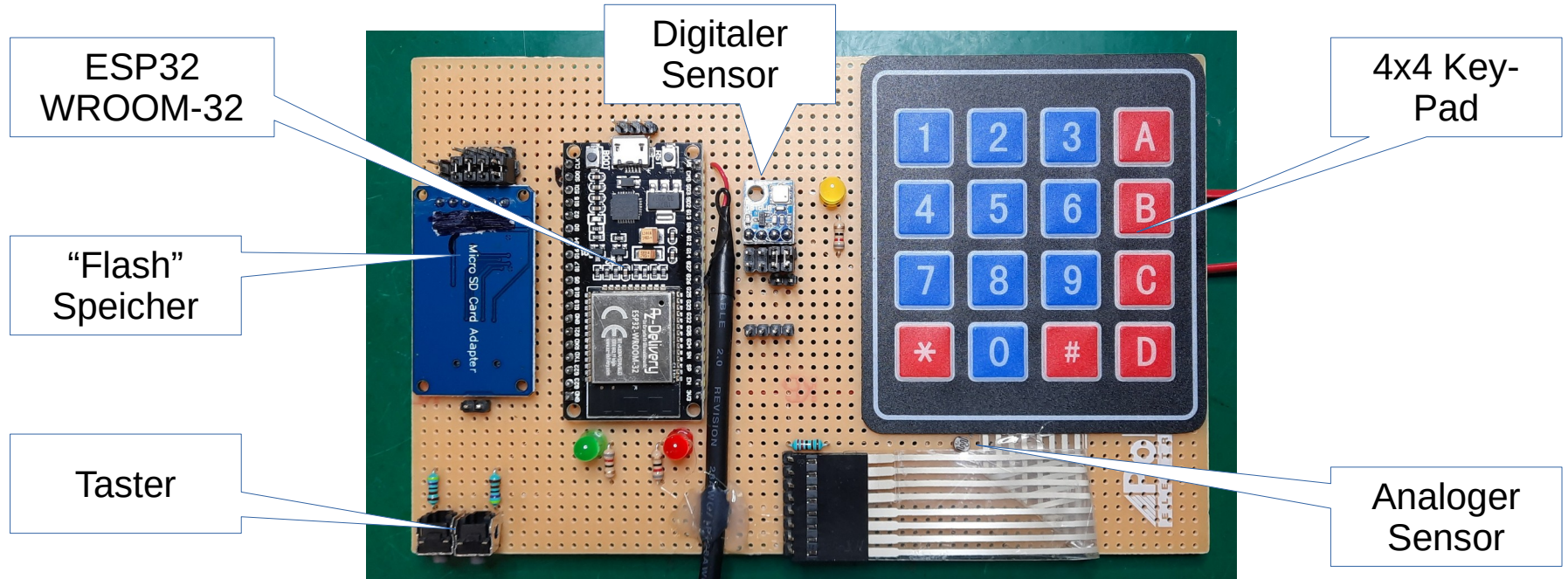
Wichtig Infos

- Außer die Jumper Header darf nichts direkt kurzgeschlossen oder mit Vcc bzw GND verbunden werden. Für die Challenges ist dies NICHT notwendig.
- Spannungsversorgung der Test-Hardware über das USB Kabel und separate USB-Netzteil.
Anschluss an Ihr Laptop ausschließlich auf Ihr eigenes Risiko!
- Unbedingt den USB TTY Adapter auf 3,3V Einstellen!
 - Anschluss an Serielle Konsole:
TX→RX und RX→TX
- Wenn mal Jumper fehlen => die Kabel des Logic-Analyzer gehen auch :-)

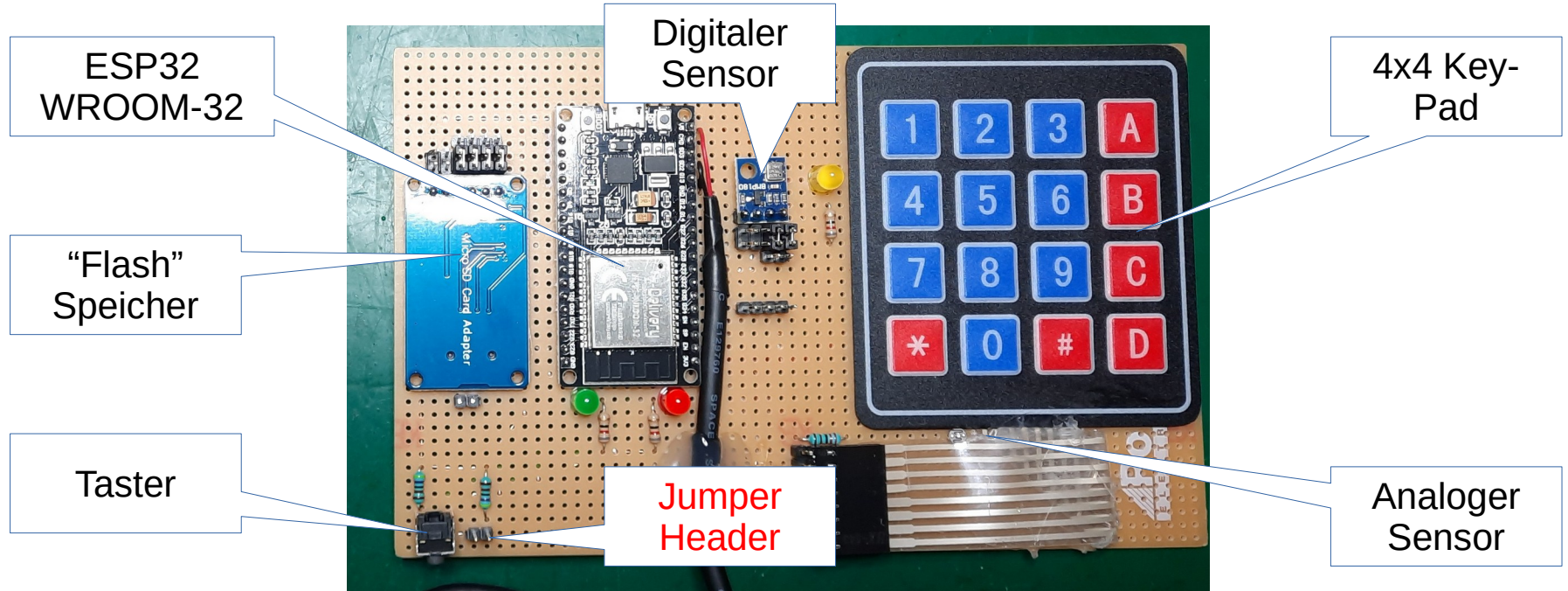


Reminder: Vorstellung des Testsystems

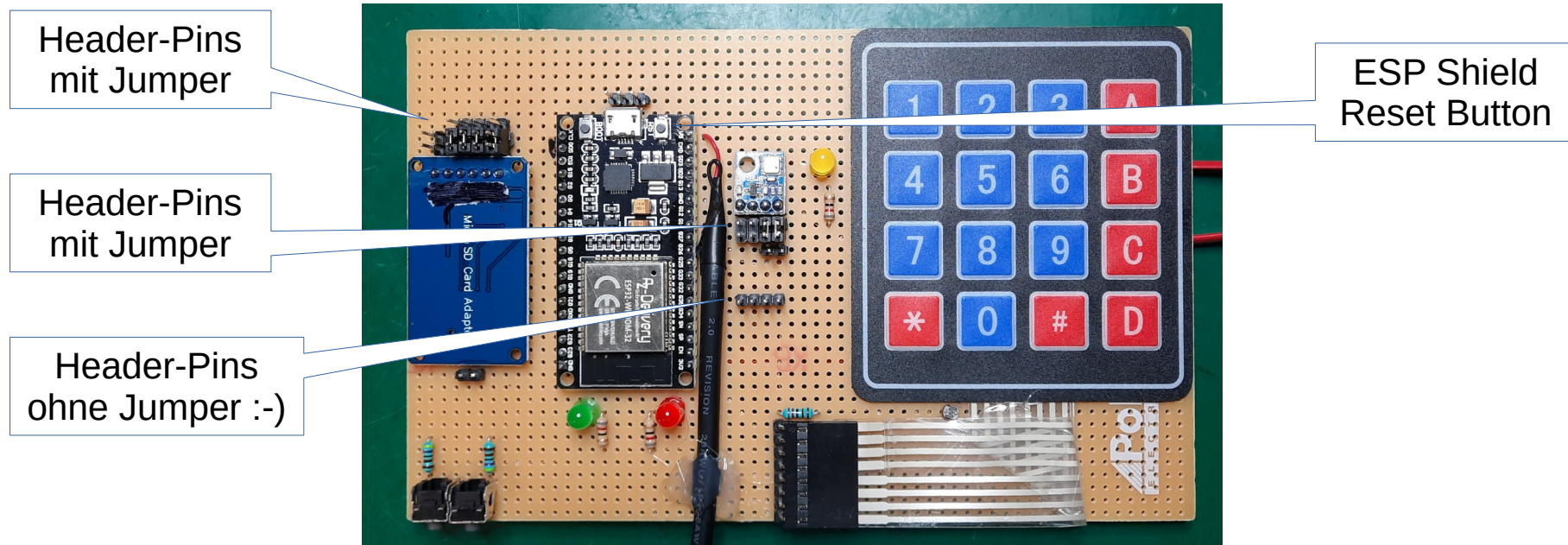
Das Test-Board und seine Komponenten



Kleine Planänderung...



Das Test-Board und seine Komponenten



Die Challenges



Challenge: HW und Funktionsanalyse

- Ermitteln der Pins und deren Funktion mit Hilfe von
 - Multimeter
 - Logic-Analyzer => welche Funktion haben die verschiedenen Pins?
 - Erstellen Sie sich eine Skizze mit den Pins und deren Funktion/Belegung.
 - TTY USB Adapter => Welche Details liefert die Serielle Schnittstelle?
- Welches Verhalten kann beim Ziehen einzelner Jumper identifiziert werden?
- Welche Funktionen haben die verschiedenen Sensoren und Taster?
 - Welches Verhalten können Sie erkennen?



Challenge: Key-Pad und die PIN

- Finden Sie einen Weg, um das Key-Pad zu aktivieren.
- Finden Sie einen Weg, um an die PIN zu gelangen.
- Hinweis: Achten Sie auf die Ausgabe der Seriellen Konsole.
 - Was können Sie daraus schließen, um an die PIN zu gelangen?
 - Denken Sie auch an die Übungen zur Analyse von über SPI übertragene Daten.



Challenge: Versteckte Funktion

- Der Jumper Header zeigt bisher beim Überbrücken mit z.B. einem Kabel vom Logik-Analyse keine Reaktion.
- Gibt es einen Weg, um darüber in Kombination mit einer weiteren Aktion eine versteckte Funktion auszulösen?
- Hint: Manchmal muss man in die Extreme gehen – nein, kein Feuerzeug, Lötkolben, Gummihammer usw. ;-)



Weitere Challenges

- Da RX-Data nicht mit der Seriellen Konsole verbunden ist, kann die Micropython REPL nicht genutzt werden.

Challenge: Finden Sie einen Weg, RX-Data für die Eingabe von Befehlen in der REPL Eingabe nutzen zu können

- Welche zusätzlichen Probleme im Code können Sie mit dem Konsolen-Zugriff noch identifizieren?
- Beim Starten des Anwendung existiert eine Race-Condition mit der das Programm zum Absturz gebracht werden kann und in einem undefinierten Zustand gelangt.

Challenge: Finden Sie den Race-Condition – wie kann man diese mit Hilfe der Konsolen-Ausgabe und dem SPI Mitschnitt zeitlich eingrenzen?

Fragen? Diskussion?