

MUNI
FI

PA192: Attacking a Safe Lock

Jan Kral

Attacks on Embedded Systems

- Electronic Safe Lock is typical representation of an embedded system where the physical access to the electronics is limited.
- Keyboard and the LED indicator are user accessible.
- Also, battery can be replaced even if the safe is locked.



Attacks on Embedded Systems

- Goal: Retrieve the password without brute force attack.
- Idea: Use every possible way to minimize number of attempts.
- Try to find a different behavior for correct and incorrect character.
 - Measuring power consumption in time – higher consumption or delays before going to sleep.
 - Identifying time discrepancies on accessible signals (e.g. keyboard readout).

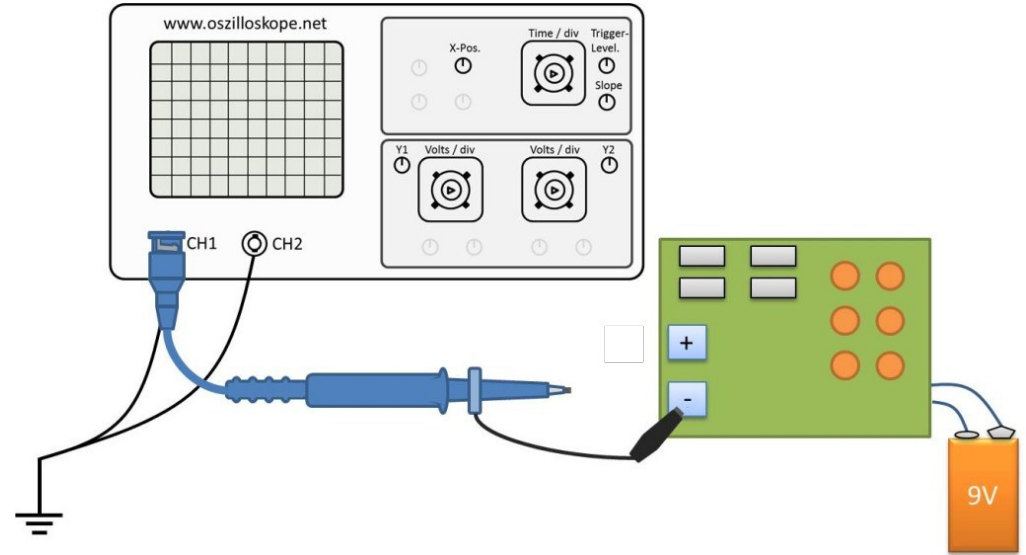
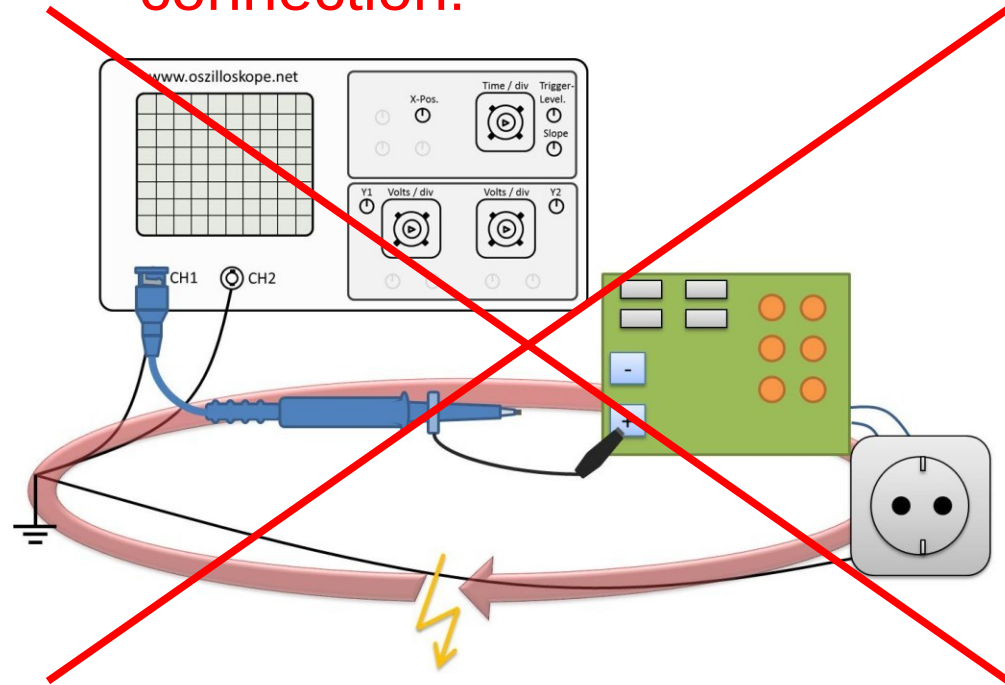


Measurements

- Communication
 - Logic Analyzer
 - Oscilloscopes
- Power Consumption
 - Oscilloscopes
- Radio Emissions (not today)
 - Radio Spectrum Analyzer
 - SDR (Software Defined Radio)

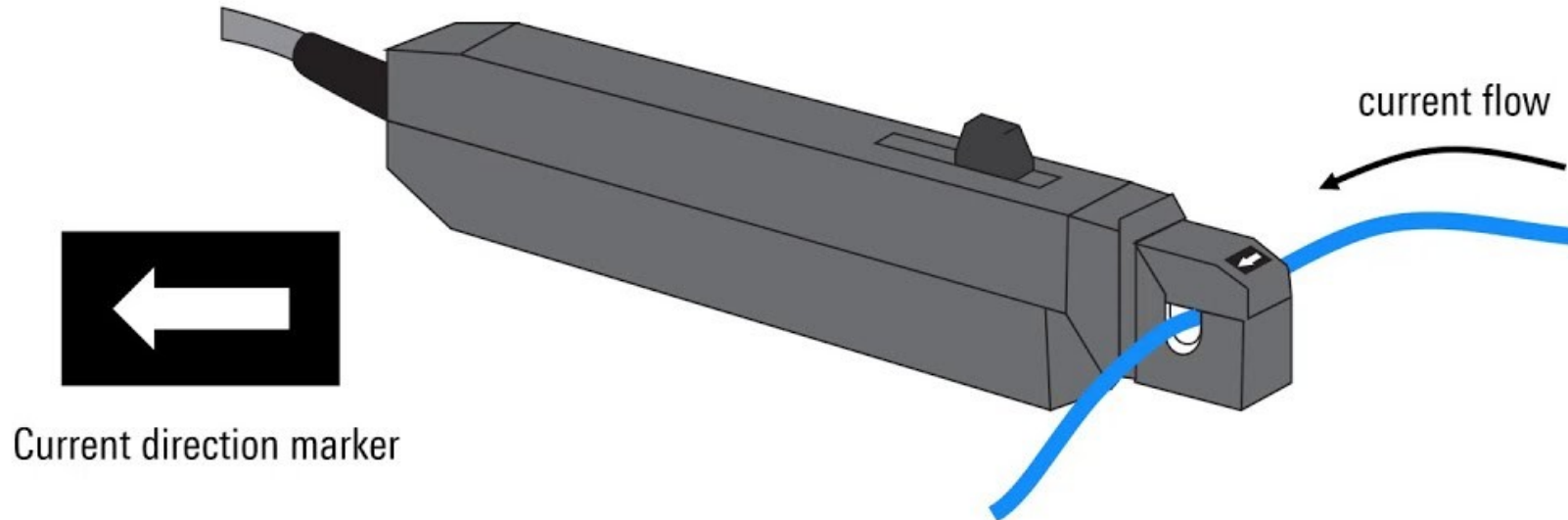
Oscilloscope Grounding

- Be careful about your oscilloscope grounding:
- You can damage your circuit or the oscilloscope by incorrect ground connection!



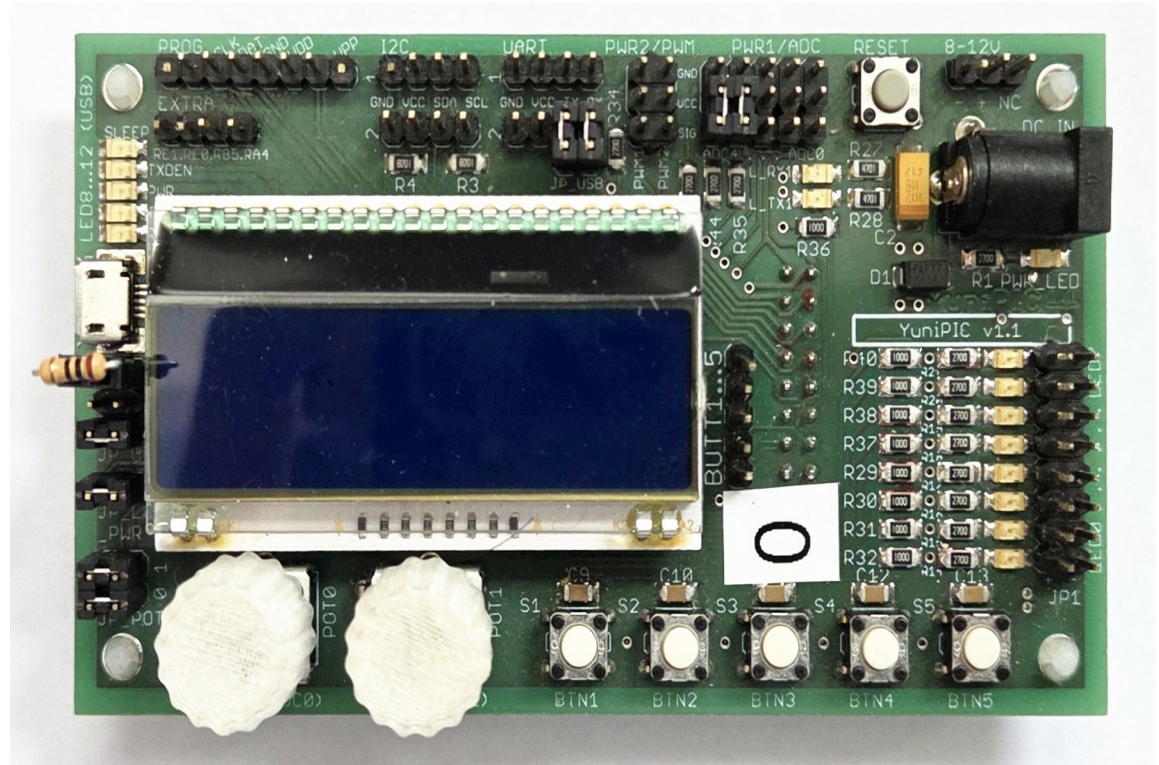
Current Measurement by Oscilloscope

- Indirect
- Direct



Our Safe Lock Emulator

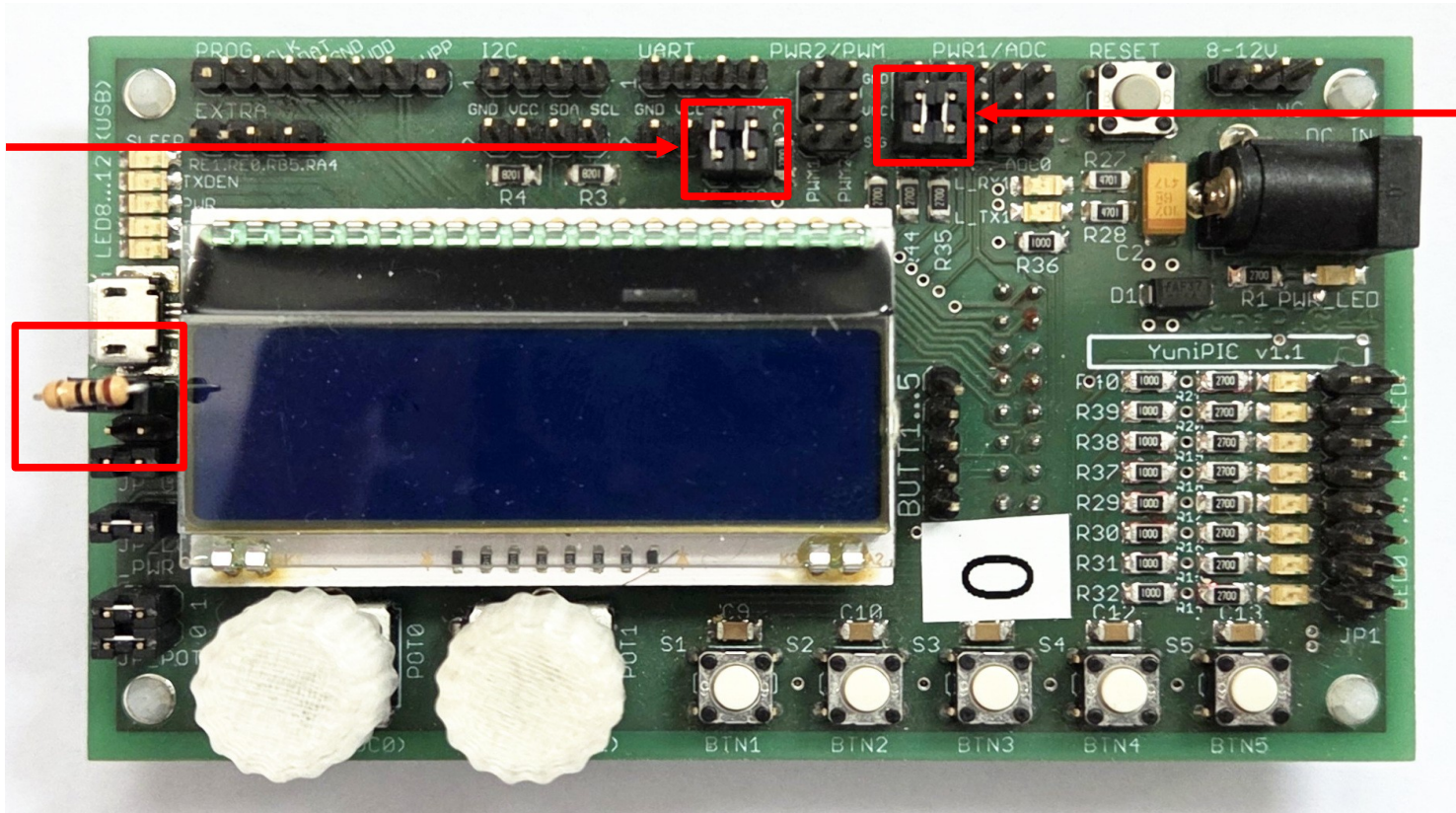
- UART on Micro USB port:
 - Baudrate:
9600 / 115200 ?
 - 1 stop bit
 - No parity
 - No flow control



Jumper Configuration

- Unsure the correct configuration of jumpers

Two
vertical
jumpers



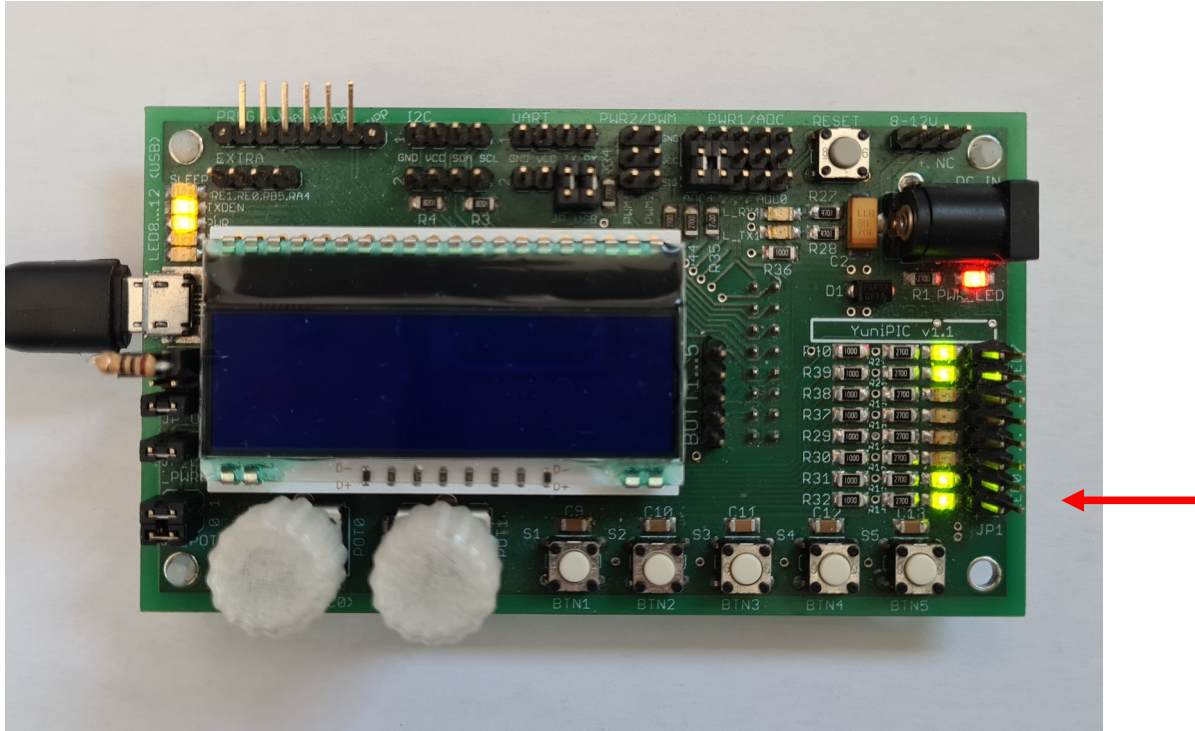
Two
vertical
jumpers

Tasks

- Connect to your board with a terminal application (of your choice, e.g. Putty, Realterm, Terminal by Bray..., on Windows,)
- There are 3 different PIN numbers (4 numeric characters) preprogrammed.
- Find all and unlock the safe (0.5 pt per PIN).

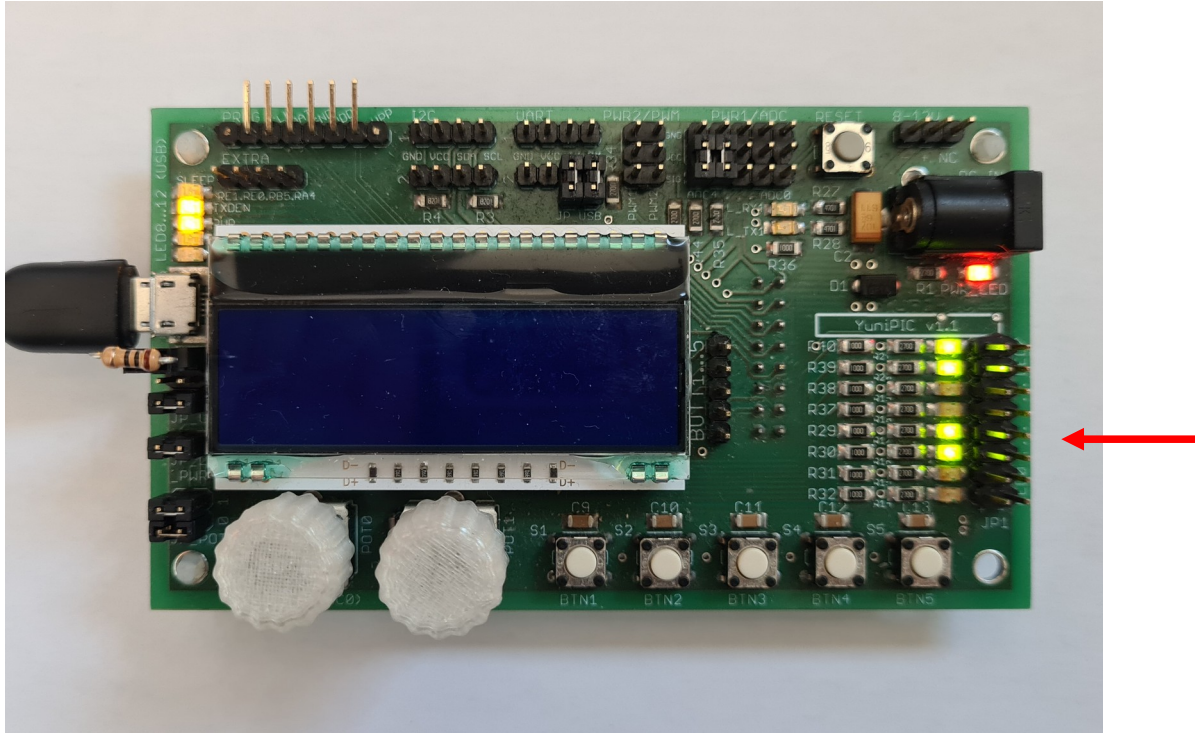
Safe 1 Unlocked

- Message:
== Bingo! Safe 1 Unlocked. ==



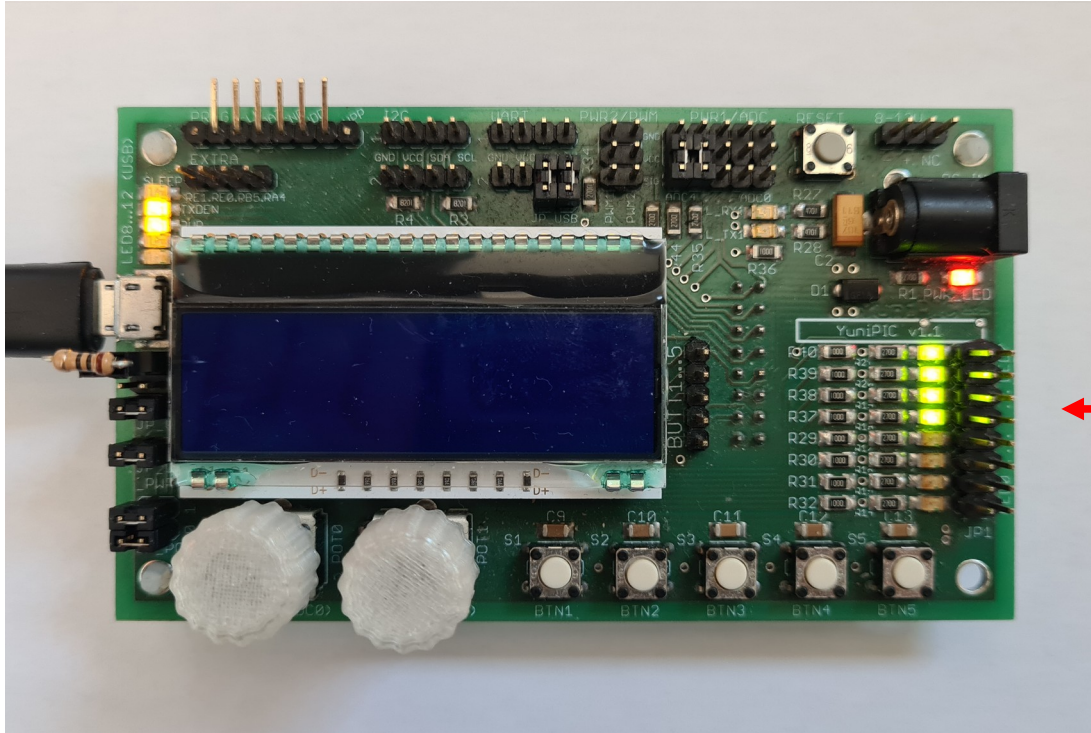
Safe 2 Unlocked

- Message:
== Bingo! Safe 2 Unlocked. ==



Safe 3 Unlocked

- Message:
== Bingo! Safe 3 Unlocked. ==

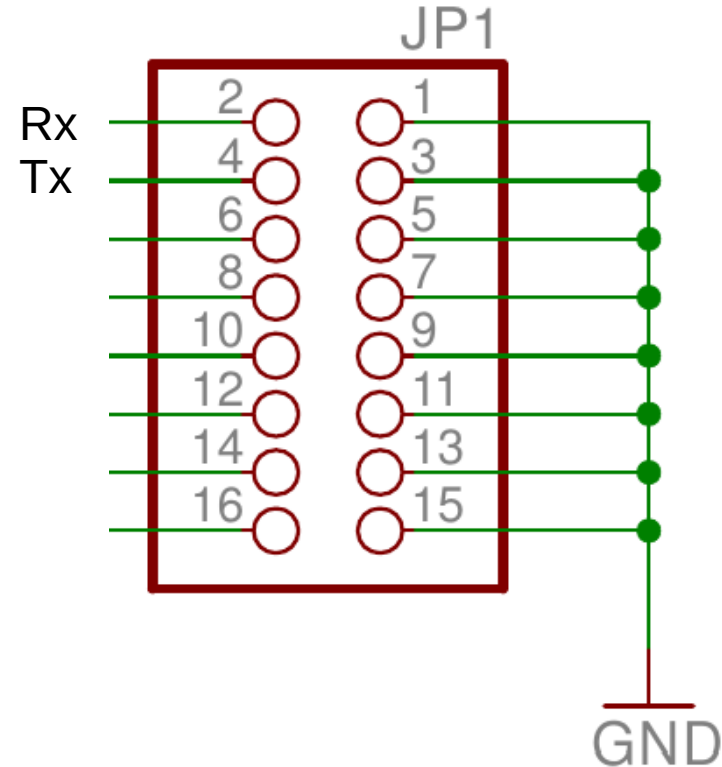
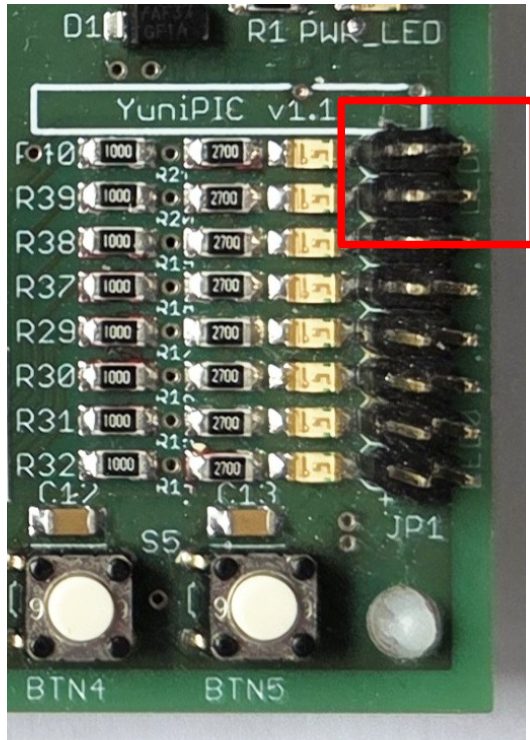


Hints: Safe 1

- Connect the Logic Analyzer or Oscilloscope to UART pins
- Measure the delay between the Rx and Tx echo
- Is the delay always the same?

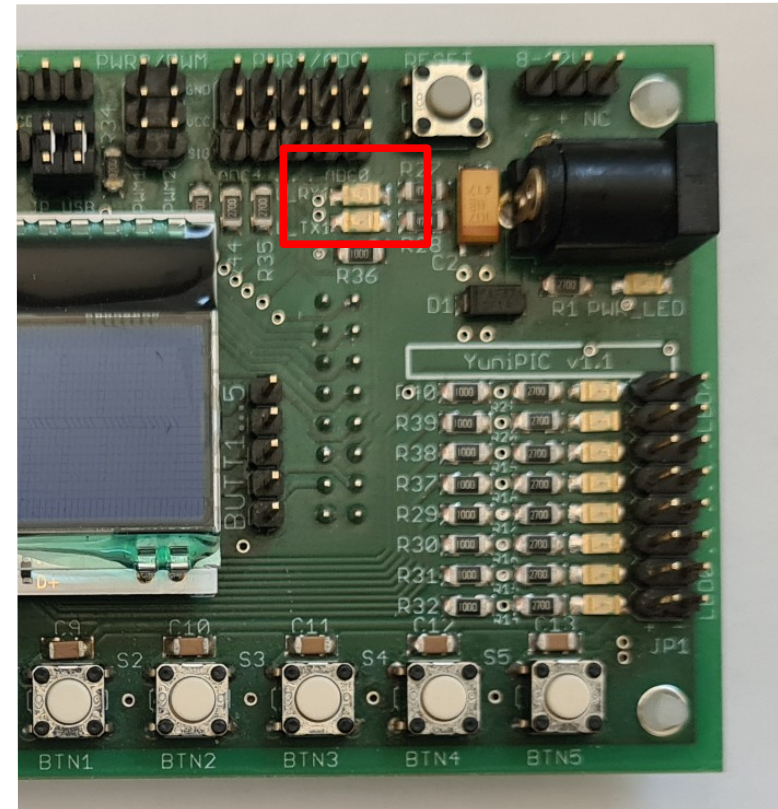
UART Communication

- Connector pinout



Hints: Safe 2

- The marked LED blinks every time when character is received.
- Measure the impulse length.
- Is the impulse length always the same?



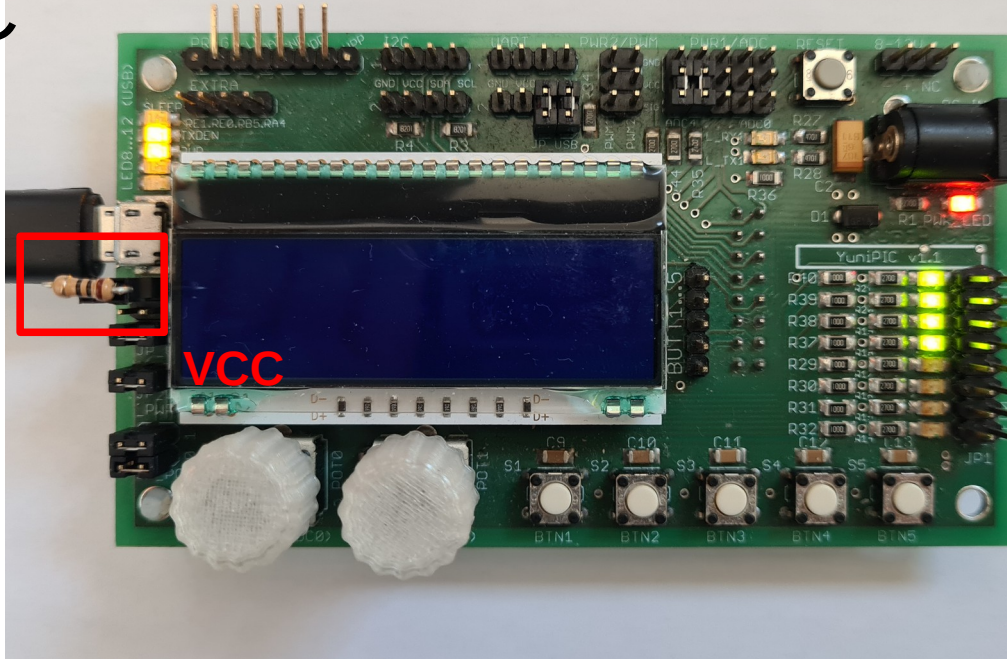
Current Consumption Measurement

- Observe the current consumption in time.
- Current Sensing Resistor is connected in series with VCC

Sensing Resistor

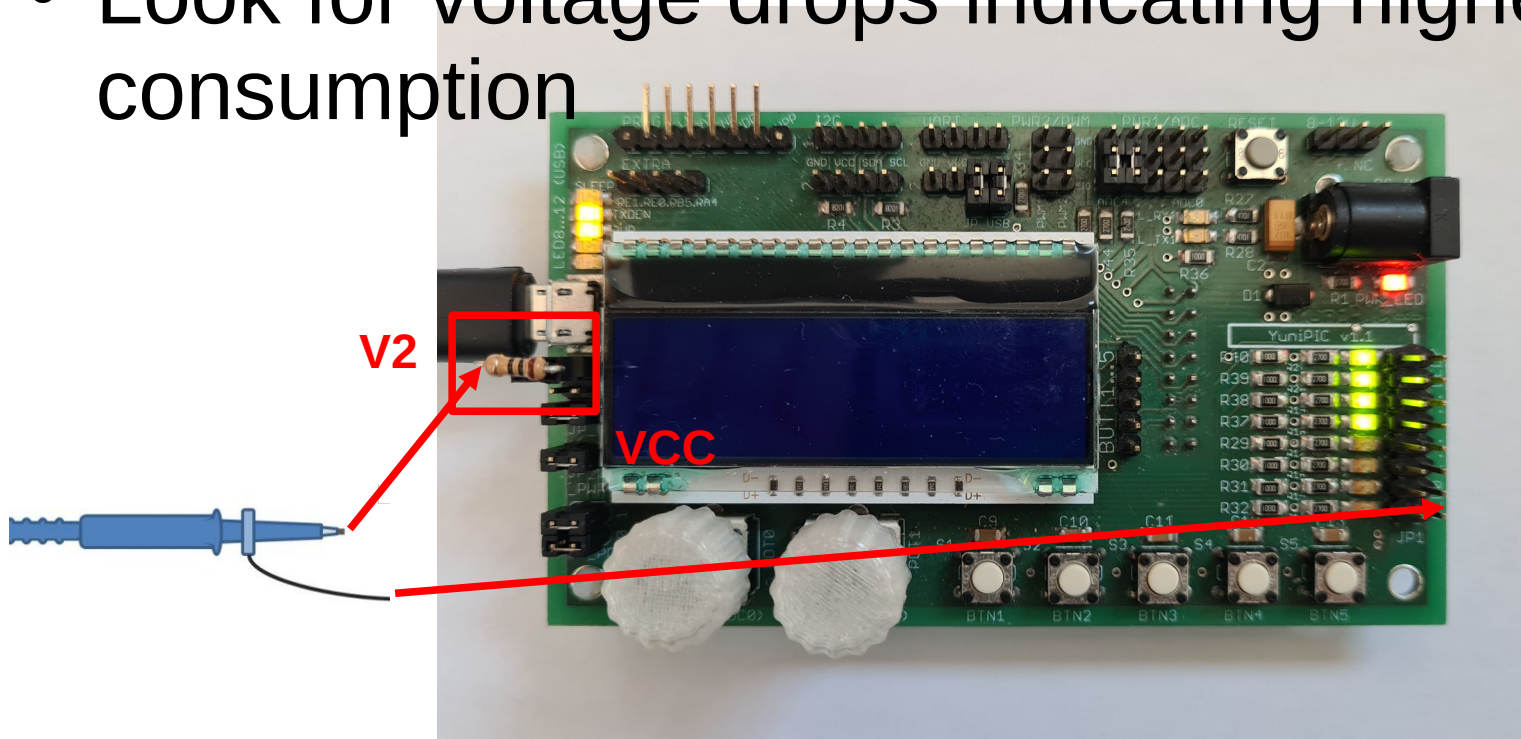
V2

VCC



Current Consumption Measurement

- Observe the current consumption in time.
- Look for voltage drops indicating higher power consumption



Submission

- Download w04_results.txt
- Fill in all the results that you have found
 - Pins are numbered with respect to slide 10
- Remember to fill in:
 - Your student IDs (uco)
 - your board ID (otherwise 0 pt)
(from the white label on your PICKIT)
- Submit your file into:

<https://is.muni.cz/auth/el/fi/podzim2025/PA192/ode/182489950/182873031>

Submission Dates

- Deadline for w03_digital_buses
 - 15.10.2025
- Deadline for w04_safe_lock
 - 22.10.2025
- W05: Whole seminar is reserved for solving a safe lock PINs