MUNI
FI

PA192: Communication buses

Jan Kral

jan.kral@fi.muni.cz

Home Preparation - Review

- Digital buses UART, SPI, I2C
  - Electrical properties of individual signals
  - Message format, waveform in time
  - Frequencies, data throughput, usage

UART communication speeds

- Typical baudrates:
  - 4800
  - 9600
  - 19200
  - 38400
  - 57600
  - 115200
  - 230400
  - 460800
  - 921600
- Note: Historically they used oscillators f = 1.8432 MHz.

SPI communication speeds

- Typical bit rates:
  - 100 kHz – 999 kHz (rare)
  - 1 MHz – 10 MHz (often)
  - 10 MHz – 50 MHz (rare)
  - > 50 MHz (very rare)

I2C communication speeds

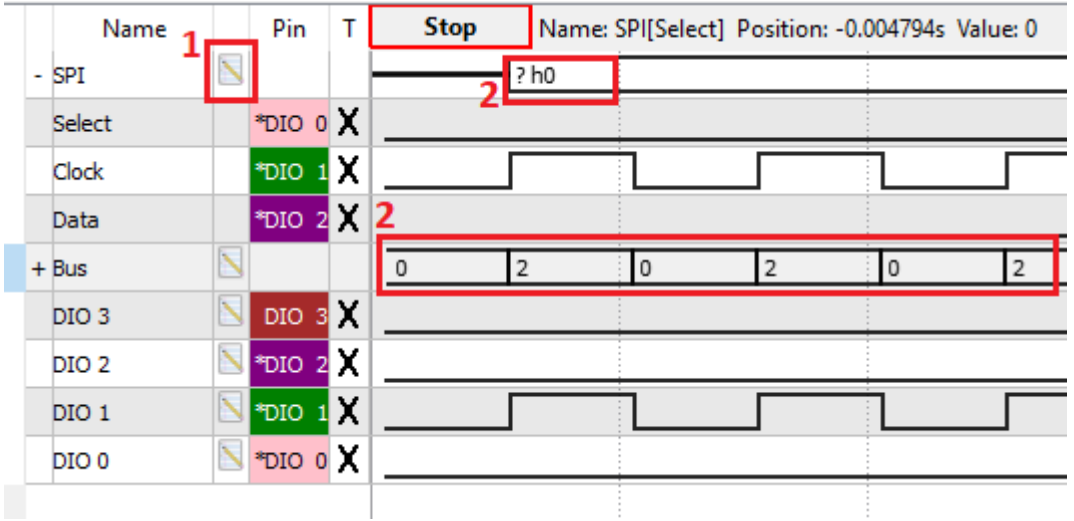
- Typical baud rates:
  - 100 kHz – standard mode
  - 400 kHz – fast mode
  - 1 MHz – high-speed mode (rare)
  - 3.4 MHz – ultra-fast mode (very rare)

Attacking on the hardware level

- Why do we care about UART, SPI, I2C?
  - Might be a weak point of a device
  - UART might give us unsecured console access (for Linux/UNIX devices)
  - I2C or SPI might give us access to unsecured flash or other memory type
- Example: Kindle hacking
  - https://kb.taktpraha.cz/projects/kindlepw5
- Example: WiFi router hacking
  - https://riverloopsecurity.com/blog/2020/01/hw-101-uart/

Logic Analyzer Demo

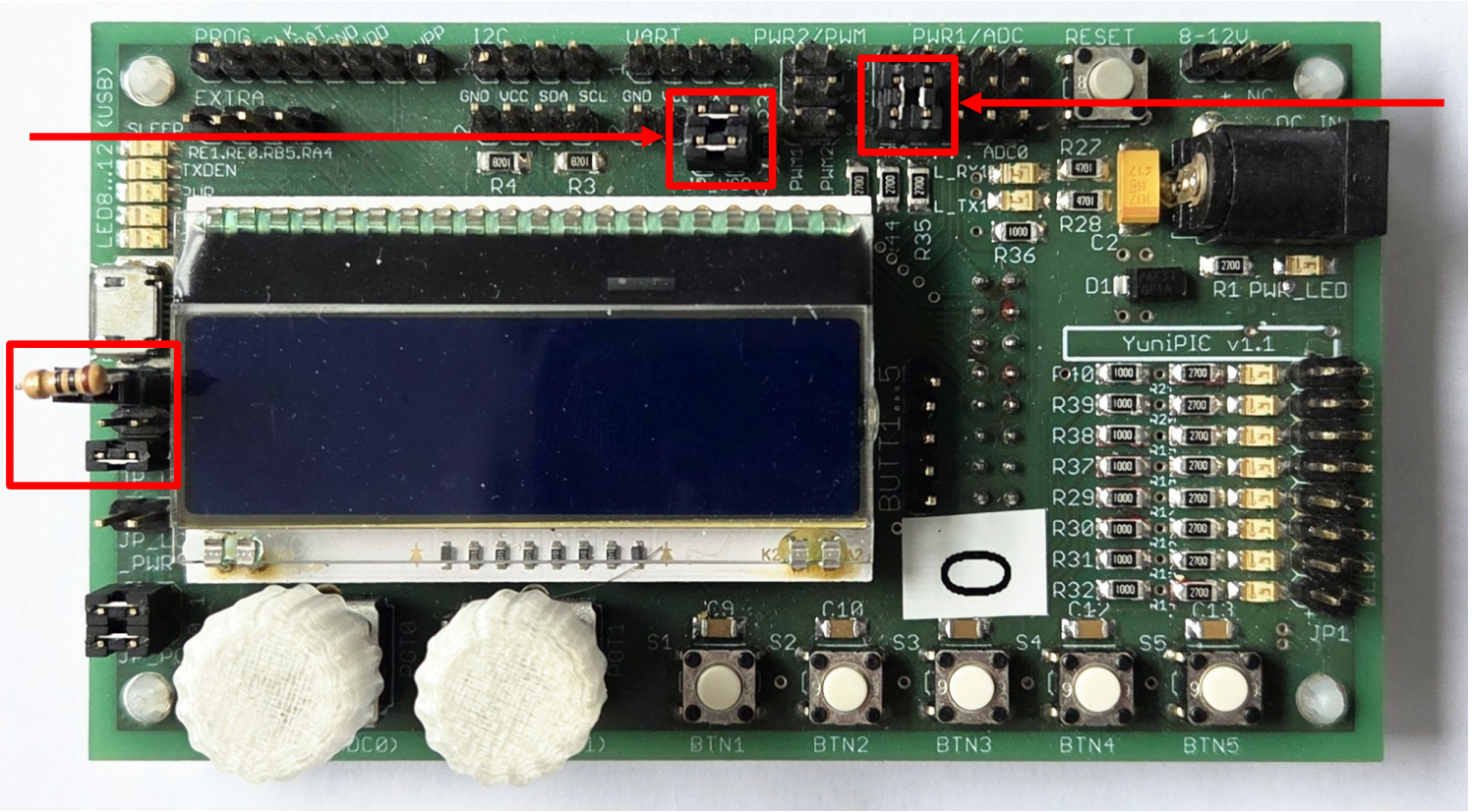
- Connect logic analyzer
- Launch in terminal: Logic-2.4.36-linux-x64.AppImage
- Tutorial: https://support.saleae.com/user-guide/using-logic/navigating-the-software



Jumper Configuration

- Unsure the correct configuration of jumpers

Two horizontal jumpers

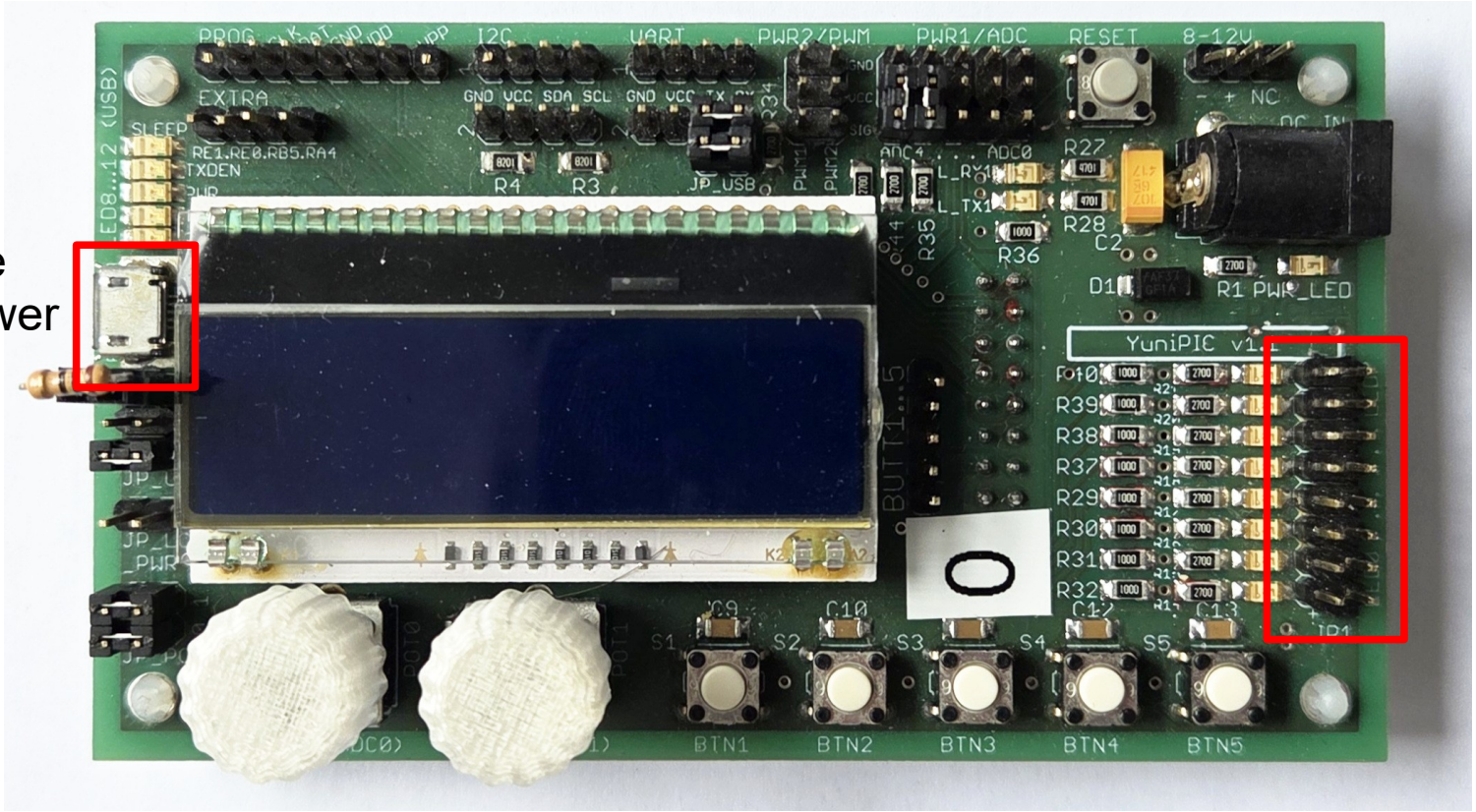


Two vertical jumpers

System Description

- Victim system

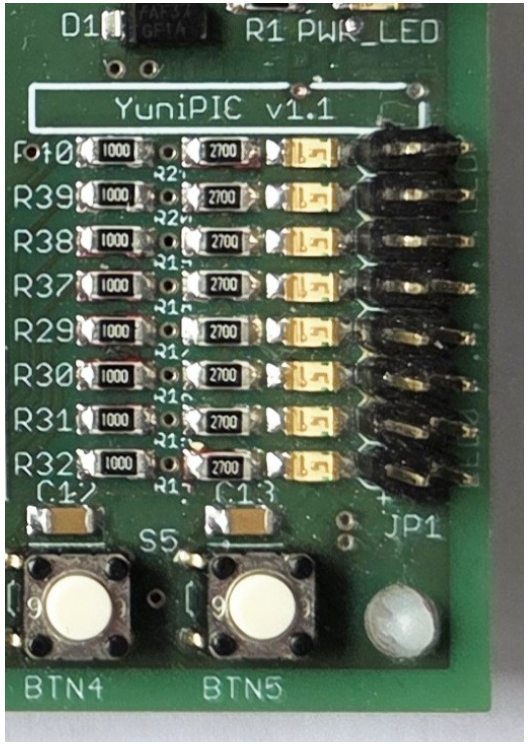
Connect the USB for power

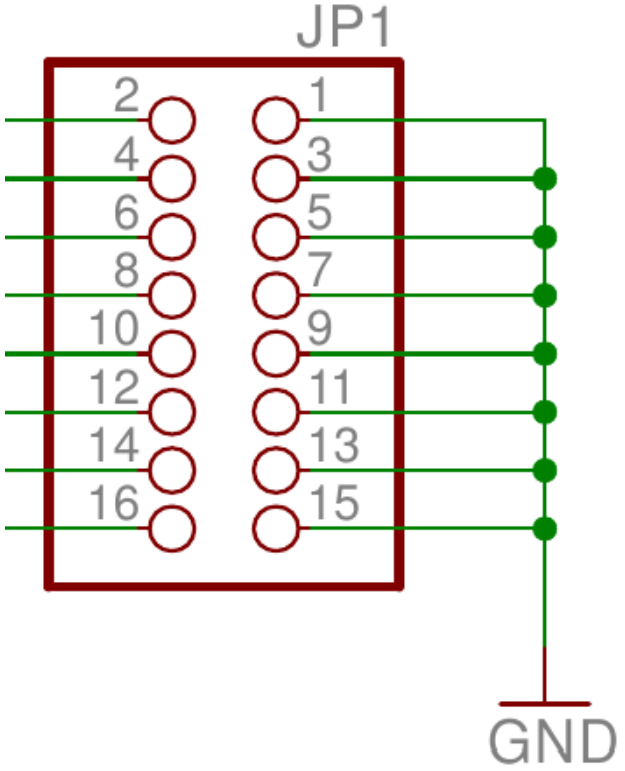


Connector with digital buses

System Description

- Connector pinout





Task 1 (0.5 pt)

- Using the oscilloscopes:
  - Find the individual signals of UART and SPI
  - Get the communication speed of UART and SPI
  - What is signaling voltage for UART and SPI?
  - Decode a single character on UART bus.
    - Present the result and the scope screen to your lecturer.
  - Decode a single character on SPI bus.
    - Present the result and the scope screen to your lecturer.

Task 2 (1 pt)

- Using the logic analyzer:
  - Get the communication speed of UART and SPI
  - Decode a password on UART bus
  - Decode a password on SPI bus
    - Message on SPI bus is valid only when CSn is active.
- Tip: You can use Digital Bus Analyzer in Logic software.

Submission

- Download w03_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/182489950/182489987/

Home Preparation for Week 04

- Microcontrollers
  - Architecture, usage (e.g. ATtiny13, STM32G0, ...)
  - Power glitch attack
    - What is it, how it is done, what can be achieved
    - Try to find at least one real-life example
  - Clock glitch attack
    - What is it, how it is done, what can be achieved
    - Try to find at least one real-life example