Assignment 3A: Ports & Protocols

Objectives for this assignment:

- get familiar with a logic analyzer.
- learn to decode UART signals.
- learn to decode SPI signals.

Bill of Materials

To complete this lab you will need:

- STM32 NUCLEOL152RE evaluation board
- AZ-Delivery Logic Analyzer
- A breadboard
- Some jumper wires
- 2x USB cable Type-A to type-B mini
- A computer that is running a Linux distribution. All the assignments were tested on a machine running Ubuntu 20.04. In case you don't have one, simply create a Virtual Machine and forward the USB devices. The tasks that you will perform are very lightweight so it's not necessary to have a beefy machine.

WARNING

You are going to deal with electric components that can be damaged if you don't pay attention. The given hardware has many protection circuits, so nothing bad should happen. However, follow these simple rules to avoid any inconvenience:

- NEVER connect pins at 3.3V or 5V to ground. This will cause a so called short-circuit and it can damage your device permanently.
- NEVER leave dangling wires, you may inadvertently create a short-circuit.

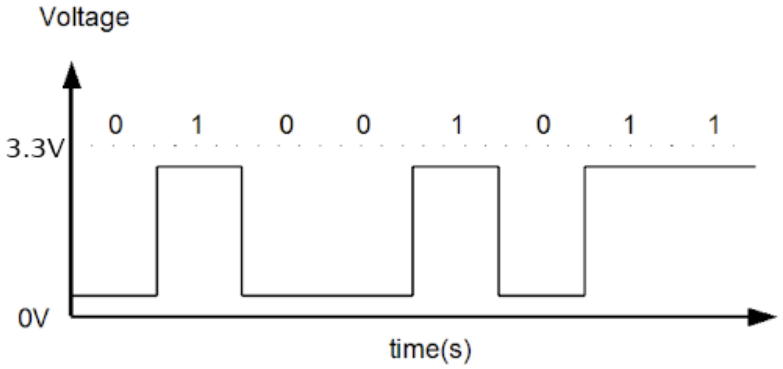
Please, pay extra care this year since, as you may not be able to complete the assignments with broken hardware. However, in case something breaks, please reach out to us *immediately*, so that we can find a solution.

Background: Logic Analyzer

Logic Analyzer 101

A logic analyzer is the debugger of the electric world. It allows you to observe electric signals over time. When things don't work it's your best friend!
A logic analyzer allows you to probe digital signals, i.e. signals that over time are either 0 or 1. In our setup 0 is represented by 0 Volts and 1 is represented by 3.3 Volts.

A digital signal looks something like this:



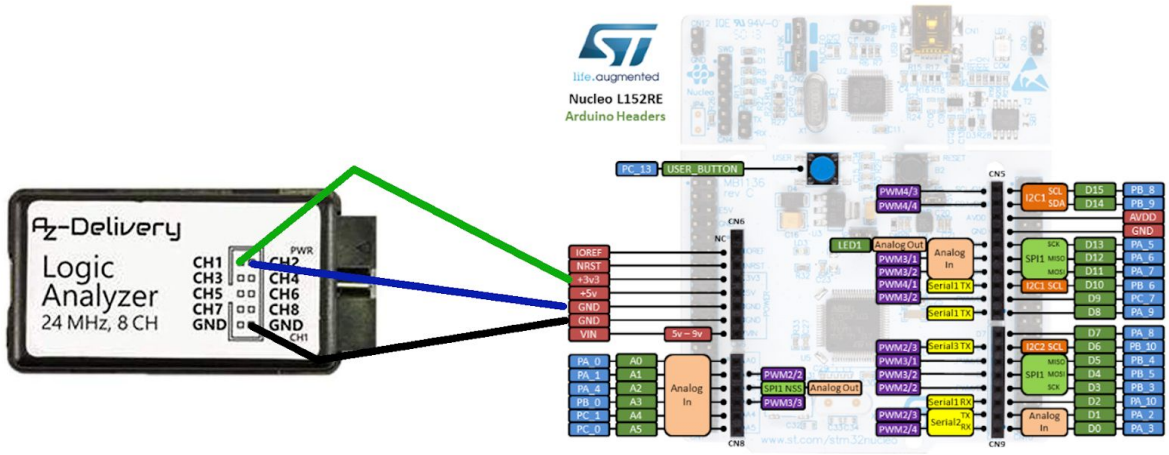
A logic analyzer is simply a tool that allows visualizing such signals.
Your AZ-Delivery Logic Analyzer can sample a signal up to 24 million of times per second (24 MegaSample/s or MS/s) and the Logic software will plot the captured signal.
The AZ-Delivery Logic Analyzer provides 8 channels, so you can sample in parallel 8 signals. This is extremely useful since the majority of digital protocols don't use a single wire/signal.

Setup

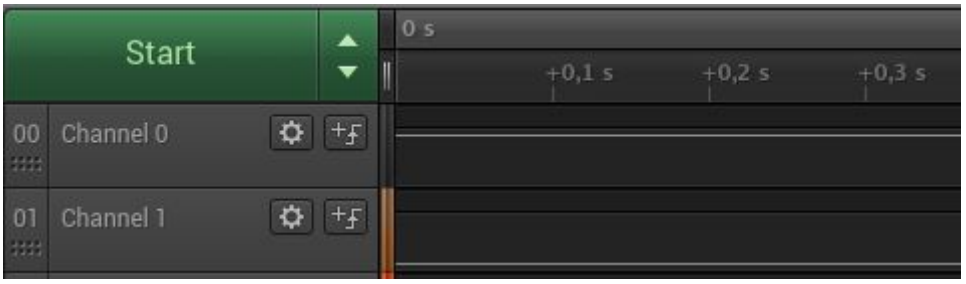
For this assignment, you need to install the Logic software to interface with your analyzer.
"Surprisingly", the AZ-Delivery Logic Analyzer is compatible with the Saleae© software.
Please visit Logic analyzer software from Saleae and download **Logic 1.2.18**.
It is available for Linux, Mac, and Windows.
Once the software is installed, connect the Logic Analyzer via its USB cable and start Logic.
If everything is fine, you should be able to press the "Start" green button on the top left.

As a simple test to verify that you are correctly capturing, connect as follow the Nucleo board and the logic analyzer:

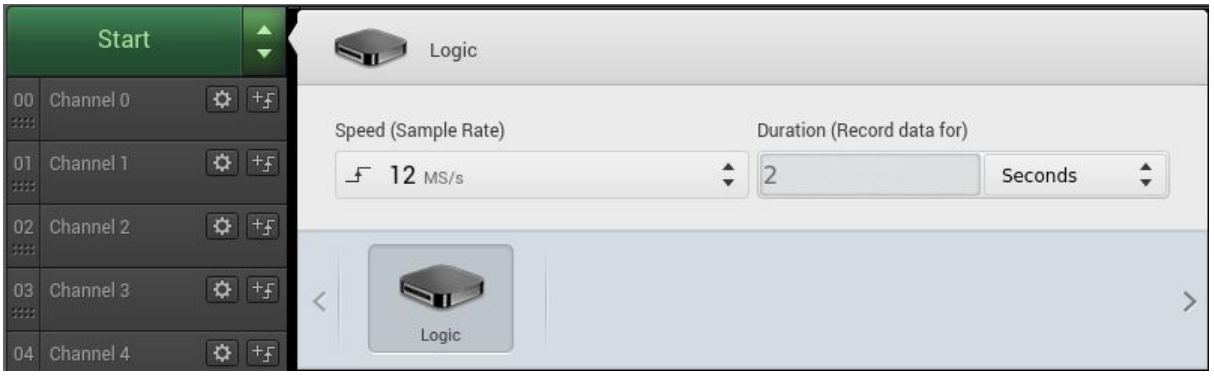
- GND to GND
- CH1 to 3.3V
- CH2 to GND



By pressing capture, you should see that for the entire duration of the sampling, CH1 is fixed at a logic level 1/High, while CH2 is fixed at 0/Low.



You can change the sampling rate and sampling duration by pressing the arrows button next to the “Start” button. For this assignment anything more than 8 MS/s is fine.



Troubleshooting:

- **A Logic device was found, but there was a problem connecting to it.**
  Try the following guide: https://schou.dk/linux/saleae/
  Alternatively, run Logic as root-user (not recommended).

- **The measured signal is unstable or it doesn’t make sense.**
  Double check that the GND of your Logic Analyzer is connected to the GND of the NUCLEO board.

Part 0: Interfacing with the Nucleo

All the assignments are already flashed and ready on your board. To select assignment 3A, connect your Nucleo board to your computer via the provided USB cable.
After this type into your terminal:

```
screen /dev/ttyACM0 9600
```

You should be welcomed by the following message after you press the reset button (the black one) on the board:

```
============================
==== HWSEC ASSIGNMENTS ====
============================
[1] Assignment 3A: UART and SPI decoding
[2] Assignment 4A: RE-HOSTING
[3] Assignment 4B: ARM ROP
Enter choice (1/2/3):
```

To start this assignment press 1 followed by Enter.

Troubleshooting:

- **/usr/bin/screen: No such file or directory?**
  Install screen: `sudo apt install screen`

- **Why does screen immediately exit?**
  You may miss permission to access the serial port. Try adding yourself to the dialout group, or run screen as root user. Alternatively, there may be already a screen process attached to the serial port, in this case, try `screen -rd`

- **How can I exit screen?**
  Press **CTRL+A** then \, and confirm with **y.** To scroll text press **CTRL+]**

- **I cannot find my device!**
  Unplug your device and type `ls /dev/tty*`, then press enter. Plug your device and repeat. The now present device should be the nucleo, typically `/dev/ttyACMx`.

- **Really, I cannot find my device!**
  Double-check that your USB cable is not a cheap one where the data lines are not present. Run `dmesg -wH` while plugging your device and observe the output.

- **Am I missing the drivers?**
  No, if you are using an Ubuntu 20.04 distribution.

- **I can see something but the text doesn't make sense!**
  Ensure that you specified 9600 as baudrate. Reconnect the Nucleo to your computer.

Part 1: UART decoding (2 pts)

As suggested by the welcome message of this assignment, use your Logic Analyzer to probe pin PA9. Your goal for this part is to decode the UART signal present on this pin.

Where is pin PA9? Have a look at the appendix or use the info card present in the Nucleo board package.

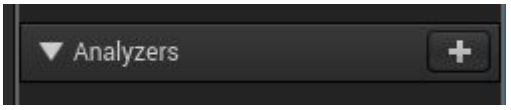
Deliverable:

- A picture of the logic analyzer connected to the board
- A text file or screenshot containing the correct UART setting
- A text file containing the decoded UART message

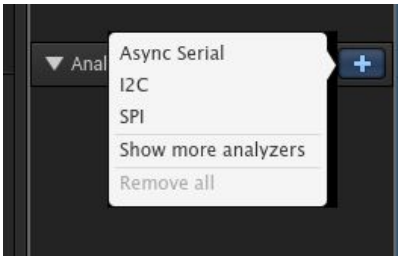
Hints:

- Decoding signals by hand is boring! Use the logic analyzer to automate this task:

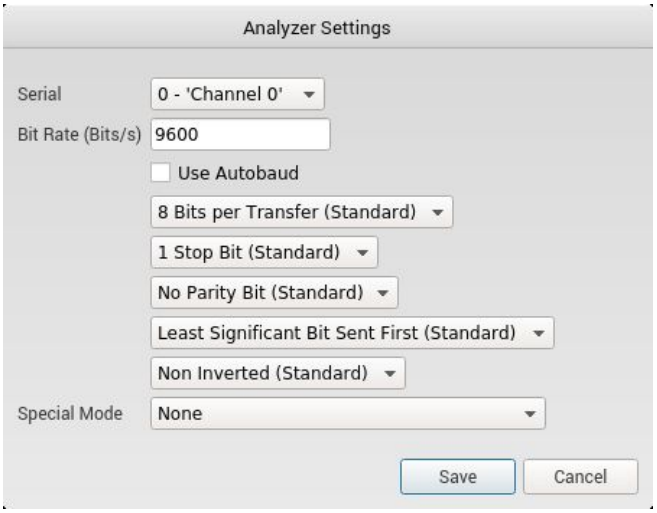
1. Add an analyzer by clicking the “+” button



2. Select Async Serial



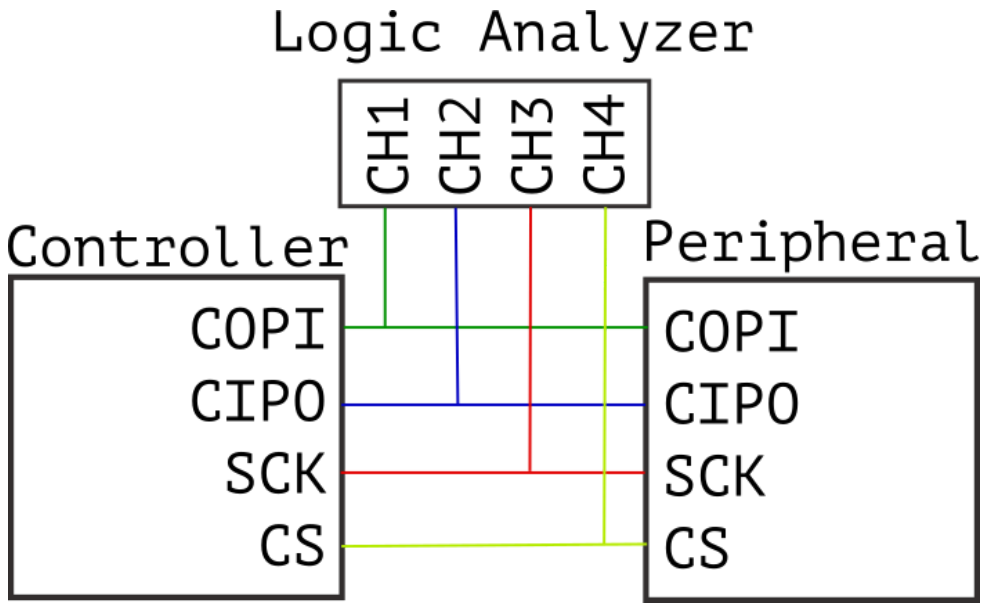
3. Find the correct settings by looking at the trace, then press save (the image below are default settings, and not the solution)



Part 2: SPI decoding (3 pts)

IMPORTANT: you cannot start this part if you haven't decoded the UART signal!

Your goal for this part is to connect the pins as below and to sniff the communication between the SPI controller and peripheral with your logic analyzer. If you manage to decode correctly the exchanged messages between the devices, you will get a flag in the format `hwsec{...}`.



For this wiring, you will need to use a breadboard to make "T connections".
In the appendix, you can find how the holes in the breadboard are connected to each other (lines indicate a connection between holes).

Deliverable:

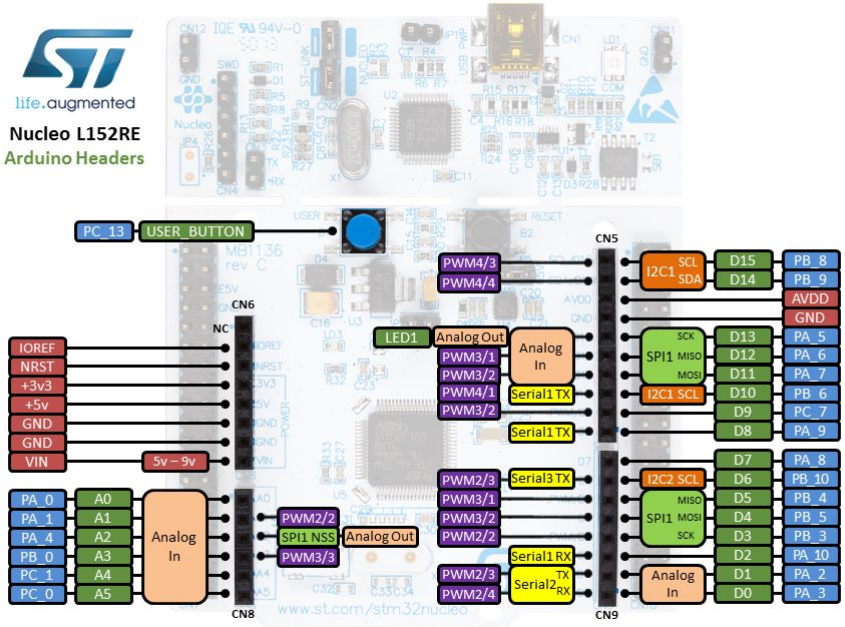
- A picture of the connections between logic analyzer, breadboard, and nucleo.
- A text file or screenshot containing the correct SPI settings
- A text file containing the flag

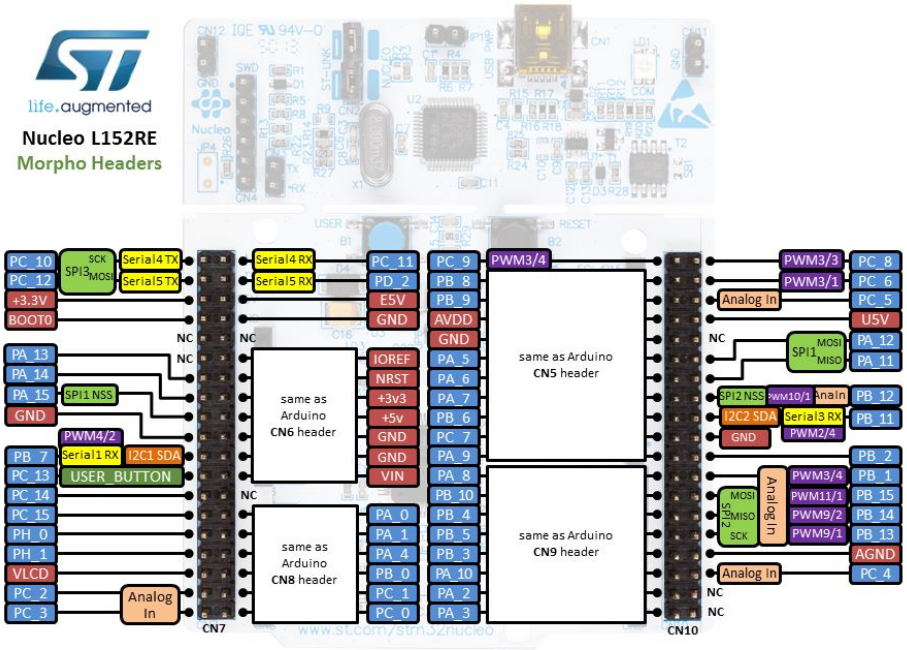
Hints:

- the Saleae software contains also an SPI analyzer
- the controller uses the command **0x5A** to query the peripheral for the next character of the flag.
- In case you are confident that you wired up everything correctly, but things are not working, try to replace single jumper wires. Some of them may have loose contacts!

Appendix

Nucleo L152RE Pin assignment

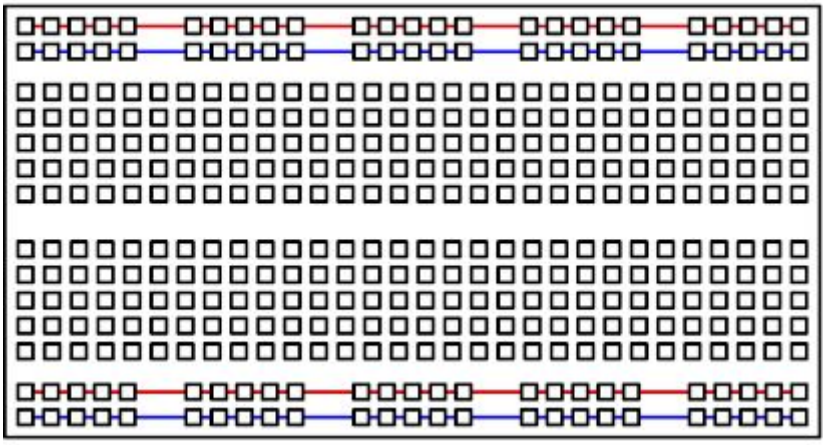




+

Breadboard interconnections

Top View of Breadboard



Interconnect View of Breadboard