

**SMART POWER METER**

**Technical Report**

Gergely Levai

03.08.2023

Assignment for

E.ON FUTURE LAB

Table of Contents

[1. Project Goal 2](#_Toc141714573)

[2. Calculations and Simulations 2](#_Toc141714574)

[2.1 Calculations for necessary transformer windings 2](#_Toc141714575)

[2.2 Running electrical simulation to ensure correct calculation 2](#_Toc141714576)

[3. Selection of Micro-Controller/Processor 3](#_Toc141714577)

[3.1 Ultra-low power 3](#_Toc141714578)

[3.2 Cryptography 3](#_Toc141714579)

[3.3 Communication peripherals 4](#_Toc141714580)

[4. Communication modules 4](#_Toc141714581)

[4.1 Ethernet 4](#_Toc141714582)

[4.2 Bluetooth and modularity 4](#_Toc141714583)

[4.2.1 Bluetooth 4](#_Toc141714584)

[4.2.2 Modularity 5](#_Toc141714585)

[5. Cyber Security 5](#_Toc141714586)

[5.1 HSM 5](#_Toc141714587)

[5.2 AES encryption 5](#_Toc141714588)

[5.2.1 AES keys and product signature 5](#_Toc141714589)

[6. Addendum 6](#_Toc141714590)

# Project Goal

The goal of the project was to develop a smart certification tool that measures power flow through a wall socket of a residential home. The following requirements had to be fulfilled to achieve project success:

(1) The product must be able to measure power consumption

(2) It should have wire and wireless communication interfaces

(3) It should support pre-trained AI models

(4) It should be able to sign power consumption data using AES

During market research and competitor analysis the following extra requirements were put in place:

(5) It should have extra functionalities beside being a simple power meter

(6) Having a screen is not necessary

(7) It should work with different power mains (e.g.: 230/50, 115/60)

# Calculations and Simulations

## Calculations for necessary transformer windings

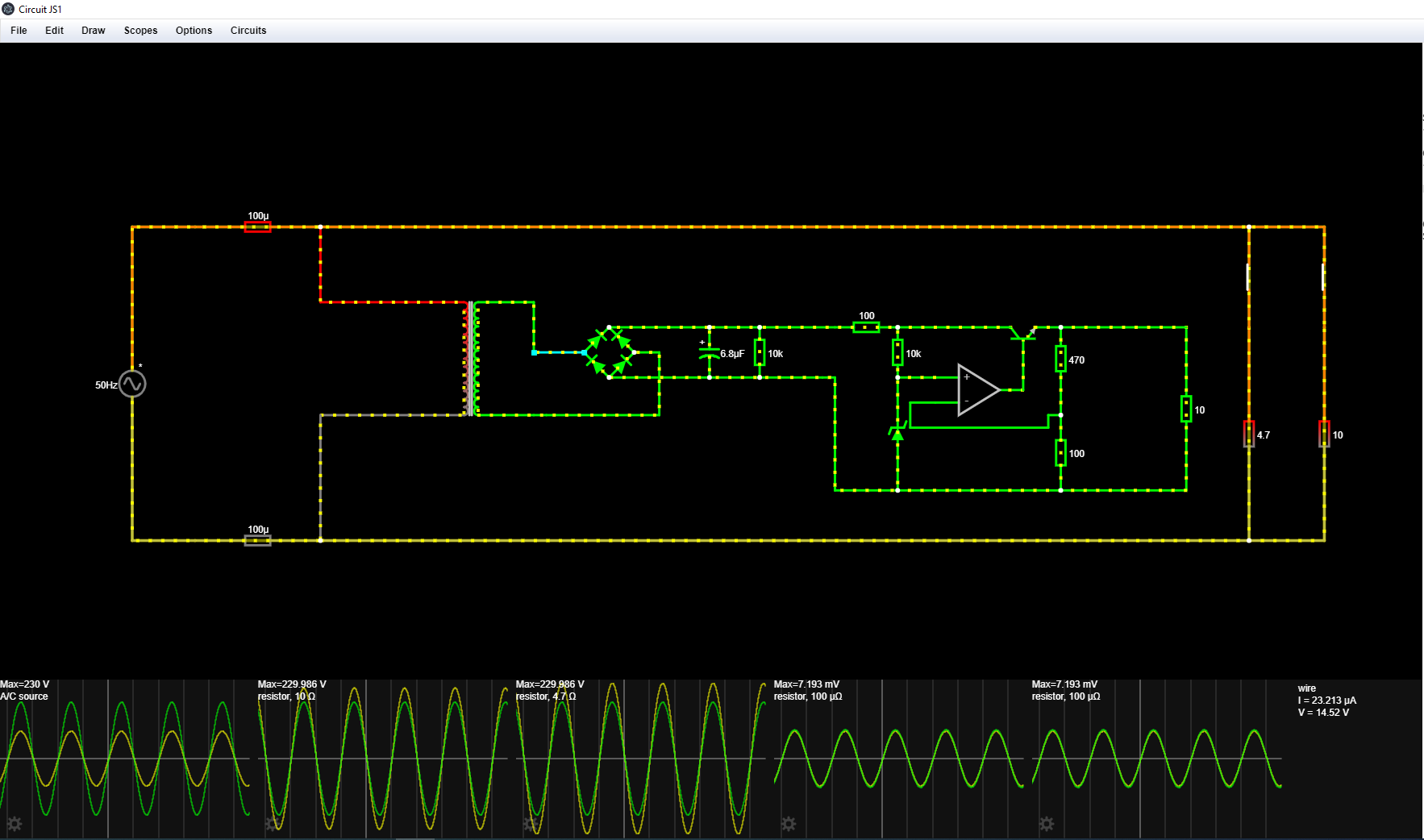
Calculating, with ideal transformer, the voltage in the secondary winding (Vs) of the transformer equals to the voltage in the primary winding (Vp) divided by the ratio of windings (T.R=Np/Ns).

The typical necessary voltage to run most digital circuits is 5V therefore a minimum of 5V is required to be present in the secondary winding of the transformer. The lowest value of power mains around the world is 100V therefore that is used to calculate the minimum required turns.

**= 20**

## Running electrical simulation to ensure correct calculation

A simplified electrical simulation model (Figure 1.) has been created using falstad to check correct transformer selection.



Figure

Slight overvoltage can be observed on the simulation model since it is taking other factors into consideration (e.g.: inductance) when running the simulation that are not present in the ideal transformer equation. This results in ~14-15 V in the secondary winding in case of 230V/50Hz and ~9 V in case of 100V/60Hz which is sufficient.

# Selection of Micro-Controller/Processor

Multiple requirements had to be taken into consideration while selecting the uC for the project such as: low power consumption, ability to AES encryption and support for wide variety of communication protocols.

The selection fell onto the STM32U545 (LQFP64 package)

## Ultra-low power

The STM32U545 is an ultra-low power microcontroller that operates on 3.3V while providing sufficient calculation capacity to support AI model interactions.

## Cryptography

The uC comes with 2 AES CoProcessors with DPA (Differential Power analysis) resistance which makes it sufficient from security point of view.

STM also provides a SmartCard that can be used together with a SmartCard-reader to achieve HSM signing of software to be flashed onto the uC.

## Communication peripherals

STM32U545 is equipped with multiple communication methods that can fit the requirements. The communication protocols include but not limited to UART, SPI, I2C and CANFD.

# Communication modules

Two communication modules have been implemented during the development of the product, one being Ethernet using a standard RJ45 connector the other is a Bluetooth module that can be removed to provide modularity to the system. For more info see 4.1.

## Ethernet

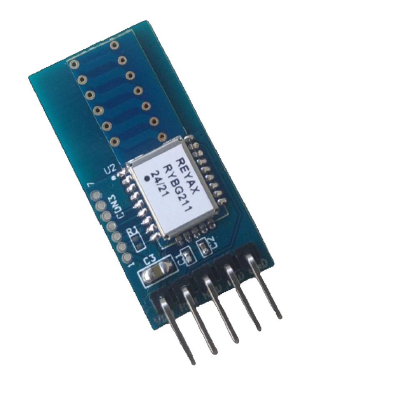
A standard RJ45 connector receives internet cable connected directly to a router or server to provide connection to the IoT and bring the product online.

The ENC28J60 ethernet controller connects via SPI to the uC to provide communication through the RJ45 connector.

## Bluetooth and modularity

### Bluetooth

The RYBG211\_Lite (Picture 1.) Bluetooth communication module selected for the project has a large range and can host up to 8 Host-Clients at a time making it suitable for being embedded into any home appliance.



Picture 1.

### Modularity

The Bluetooth module is connected via a standard 5-pin connector header meaning it can be removed on demand to replace it with other modules that also use UART as their communication interface. This opens up the possibility of later upgrades or changes to the product without actually having to change the PCB layout or Schematic.

# Cyber Security

Data protection is necessary to ensure maximum trust in the product from the consumers and to protect company data. Therefore, two security features are to be implemented:

HSM signing of software to avoid software counterfeiting and AES encryption of communication to ensure data protection.

## HSM

STM32 provides STM32HSM-V1 that is a SmartCard based Hardware Security Module used to install Secure Firmware on STM products and can be used to sign software products using public and private keys.

Once secure boot is installed on the uC only software signed with the HSM can be installed on it.

## AES encryption

Asymmetric Encryption Standard is used to encrypt data sent to and from the uC. 256-bit long AES encryption keys are used to ensure maximum security. The usage of universal (static) keys do no provide the necessary security therefore unique keys are selected.

### AES keys and product signature

The STM32Uxx series comes with a built-in real-random number generator that can be used to generate unique AES keys for each product at the production stand. Once a random number is generated the randomly generated AES key would be uploaded onto a secure server together in pair with the unique ID of the uC.

This way each and every product will have their own unique AES keys and will be able to communicate with the servers while preserving data security.

# Addendum

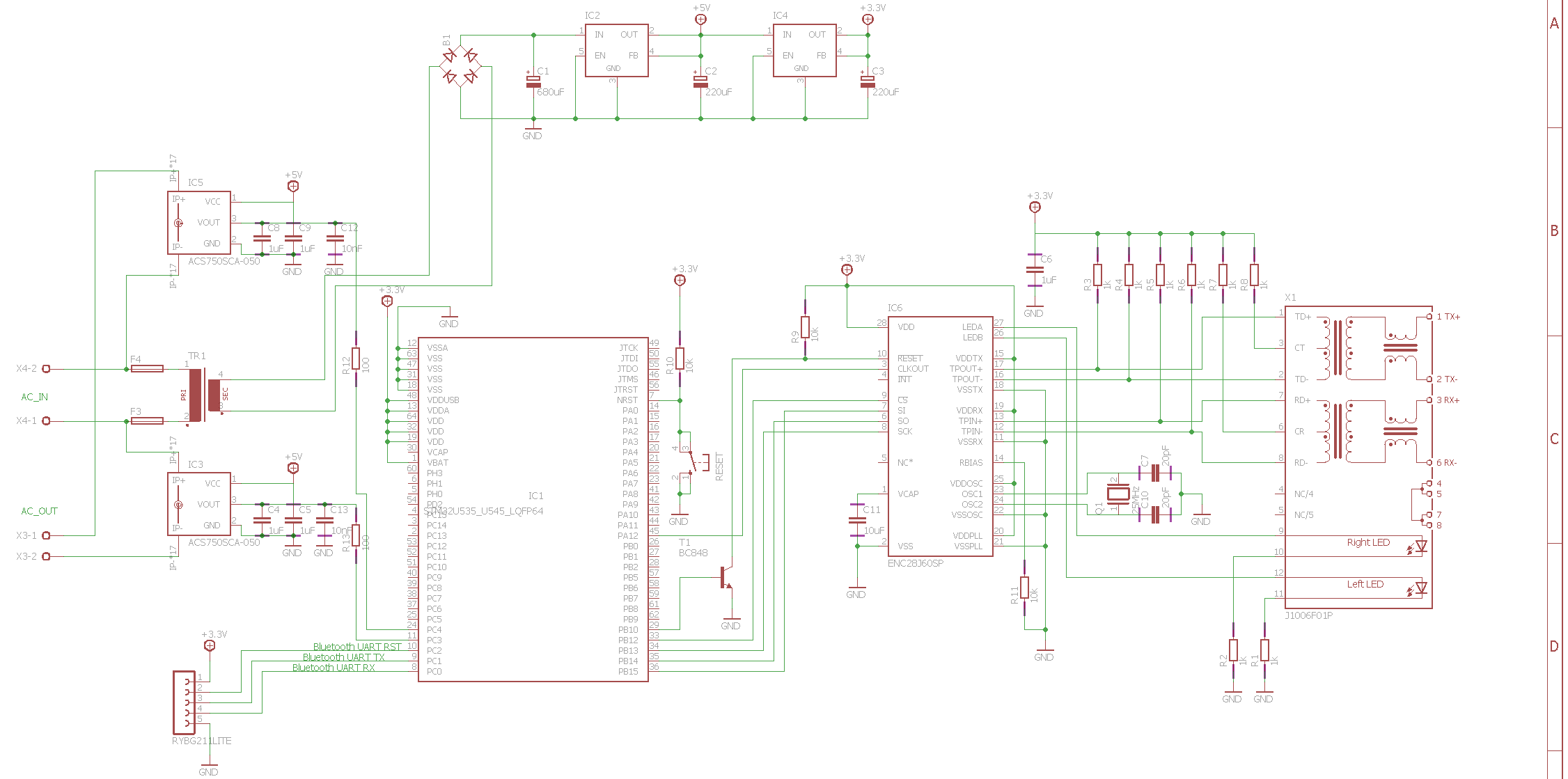


Figure – Schematic

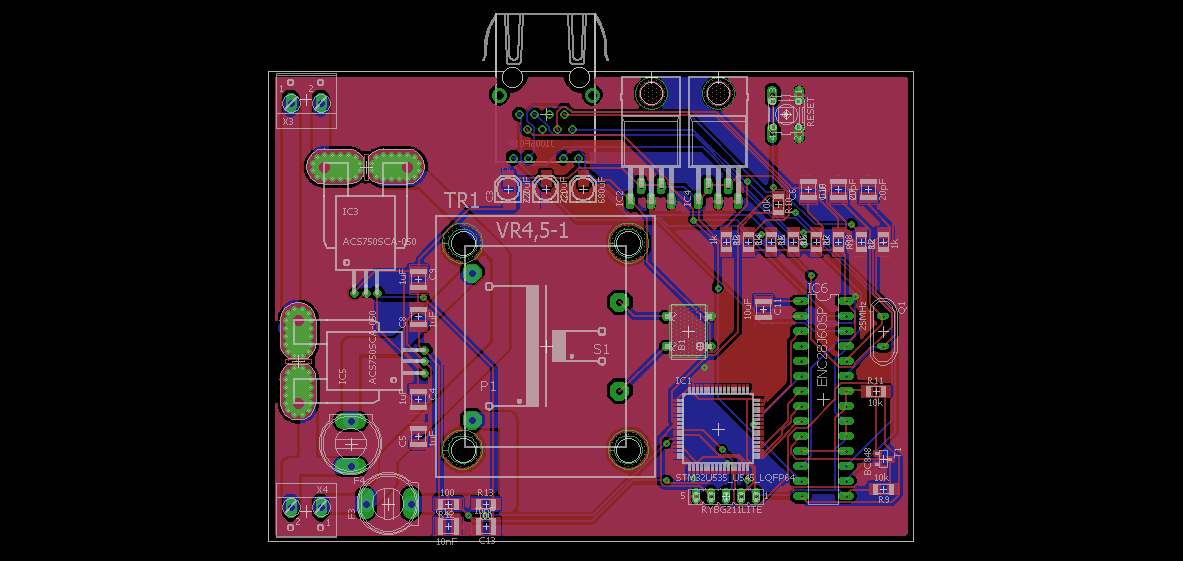


Figure – Layout