Neo900 SIM Switch

Jörg Reisenweber*, Werner Almesberger†

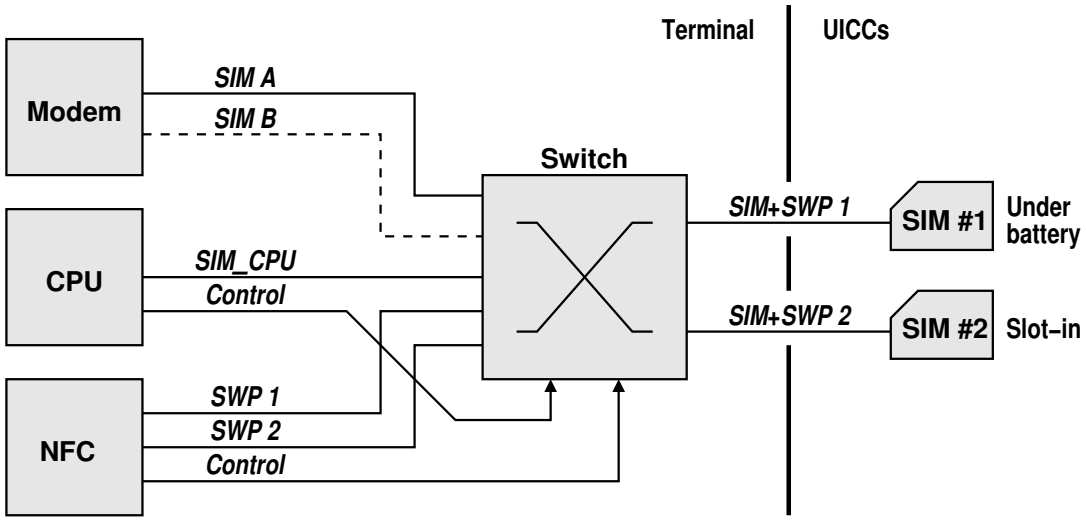
June 14, 2016

Neo900 supports up to two SIM cards, one under the battery and one in a slot-in holder accessible from the outside. The hardware supports the following operations:

- The modem accessing either SIM, under CPU control,[1]
- generic smart card reader mode by the CPU, and
- independent access of NFC (through SWP) to a secure element contained in the SIM.

This document specifies how access to these two cards is implemented in the Neo900 hardware.

The following drawing illustrates the general situation: we have modem, CPU, and NFC that each may need to access one of the SIM cards, be it for communication, for supplying power, or both.



We use A/B for the buses that are affected by the switch, and 1/2 for the SIM side and for signals or buses that are not affected by the switch.

*Concept and design requirements.

†Specification details and illustrations.

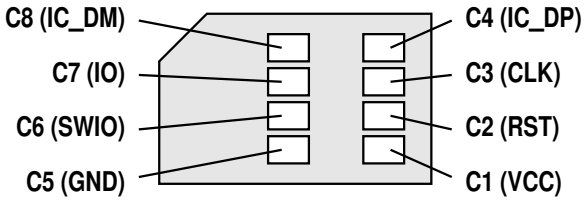
[1] To the modem, this looks like the user removing one SIM and inserting another. Depending on the availability of modem variants natively supporting two SIMs, details of which are not yet available at the time of writing, additional functionality may be available.

Depending the module version, the modem may have one or two SIM interfaces. The system is designed such that no invalid configurations occur even if the systems involved should fail to coordinate their activities.

Please note that connections that are shown as going to the CPU may in fact be handled through an IO expander. Furthermore, signal or bus names used in this document have been assigned somewhat arbitrarily, and may be harmonized with the naming chosen for the Neo900 schematics at a later point in time.

1 Connections

The following drawing shows the eight contacts of a typical SIM card:



We discuss the characteristics of the various signals and how they relate to the Neo900 hardware design in the next sections.

1.1 Power (C1, C5)

The SIM card is powered by the terminal. Of the supply voltage classes specified in section 6.2.1 of [1], we support class B (nominally 3 V) and class C (1.8 V).

1.2 Card detection

Access to a SIM card must be stopped before it can be safely removed or swapped. In order to ensure that the entity controlling a card can perform a clean shutdown, a card detection signal may warn of imminent card removal.

Of the two SIM holders in Neo900, SIM #2 is equipped with a card detection switch. SIM #1 has no such switch but its location ensures that the SIM can only be released after battery removal.

We may introduce an added safeguard in the form of a battery detection signal that acts as card detection for SIM #1.

1.3 SIM data interface (C2, C3, C7)

This is the principal communication interface of a SIM card. It is used by the modem to perform all the authentication, storage, etc., operations that are used in mobile telephony. For lack of a better term, we call this the “SIM data interface”.

This interface can also be accessed by the CPU for generic smart card reader purposes. In this case, card removal is signaled to the modem and both SIMs are then disconnected from it.

The voltage levels on these signals are defined in section 5 of [1] as functions of the supply voltage. Therefore, level shifting is required when the CPU accesses a class B (3 V) card.

1.4 SWIO (C6)

SWP (Single Wire Protocol) provides a channel that operates in parallel with and that is largely independent from the principal SIM data interface. It is used by NFC for communication with a Secure Element that is (optionally) contained in the SIM card.

SWP is specified in [2]. We discuss various implementation considerations in section 6 of [3].

While there are small differences between class B (3 V) and class C (1.8 V),[2] SWP basically operates in the 1.8 V domain in either case. It connects only to the NFC subsystem which also operates at 1.8 V. Therefore, no level shifting is required for SWP. The one signal SWP uses (in addition to power) is named SWIO. We use the terms SWP and SWIO largely interchangeably in this document.

1.5 Unused contacts (C4, C8)

Contacts C4 and C8 are reserved for the USB interface specified in [4]. We do not support this functionality and leave these contacts (if present) unconnected.

[2] See section 6.1 of [3].

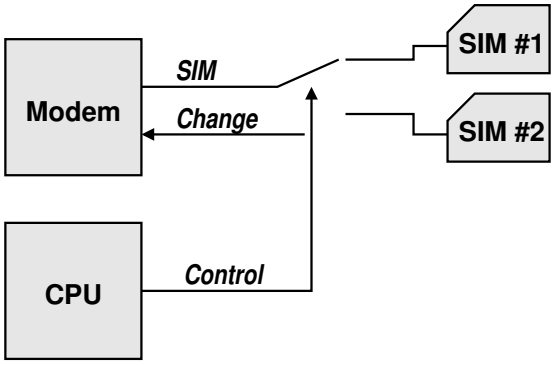
2 Terminal

While the Neo900 appears as a single terminal to a SIM card, the entity that speaks to the SIM card may be the modem, the CPU, or NFC – the latter either alone or concurrently with modem or CPU.

2.1 Modem

The modem connects to all the contacts described in the section 1, except for SWP and the USB interface. I.e., there is power, the SIM data interface, and card detection.

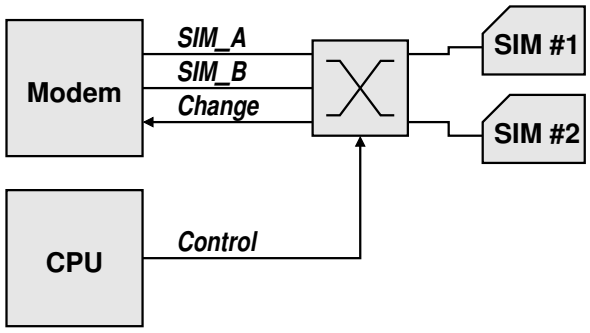
Depending on which modem version will be available at the time the design is implemented, the modem may have one or two SIM interfaces. If the modem has only one interface, the CPU will coordinate access to the SIM cards, and a card switch will appear to the modem like the removal of the old card followed by the insertion of the new card:



In addition to the card change signals from the SIM cards, the hardware generates a card change indication before the switch is operated.

In case the modem supports two SIM interfaces, the switch can still be used to swap the SIMs, should such functionality be desired. Also in this case a card removal indication is generated before any switch configuration changes are carried out: [3]

[3] At the time of writing, it is not clear whether the modem would use only one SIM at a time in this case, i.e., similar to the functionality we provide if the modem has only a single SIM interface, or whether it would be able to use both SIMs in parallel. It will also be necessary to determine, when using a modem module that is not dual-SIM capable, whether the pads used for the second SIM bus can be safely connected to the SIM switch or whether the signals will have to be isolated.



2.2 CPU

Like the modem, the CPU connects to the SIM data interface (as defined in section 1.3), to card detection, and it can request power to be provided to the SIM (see section 2.2.1).

CPU access is mutually exclusive with the modem. This gets ensured on a hardware level by giving only one of these two subsystems access to the SIMs at a time. Further details regarding the implementation can be found in section 3.1.

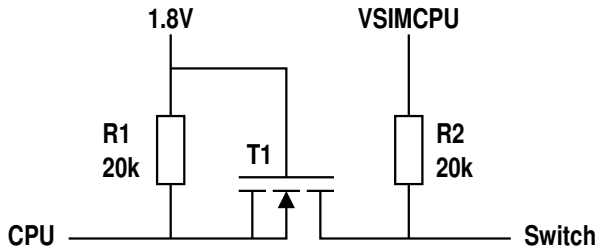
In the following sections, we discuss each type of connection and the circuits needed before going to the main switch.

2.2.1 CPU-controlled power

The CPU requests power delivery to the SIM from the power selection logic described in section 3.2.

2.2.2 CPU data

Since the SIM data interface may operate at either 1.8 or 3 V while the CPU always operates at 1.8 V, we need to provide level shifting. Tables 5.8 and 5.12 in sections 5.2.4 and 5.3.4 of [1], respectively, consider the use of a 20 kΩ pull-up resistor on the IO contact. We can therefore use the bi-directional level shifting circuit described in [5]:



For simplicity, we can also use the same type of level shifter for RST and CLK, given that they use the same voltage levels and operate at the same or a lower frequency.

In order to reduce the circuit footprint and the number of components, integrated level shifters from the TI LSF family [6] could be used instead of the discrete circuit shown above. The programmable pull-up resistors built into the CPU can be used for R1, further reducing the component count.

Section 3.4 describes how to obtain VSIMCPU.

2.2.3 CPU card detect

In order to ensure that the CPU can properly shut down any SIM card it is accessing when that card is being removed, the CPU needs to have access to the card detect signals.

Since the CPU controls the state of the switch, software can simply decide which card detect signal belongs to which SIM card, and no hardware selection is necessary.

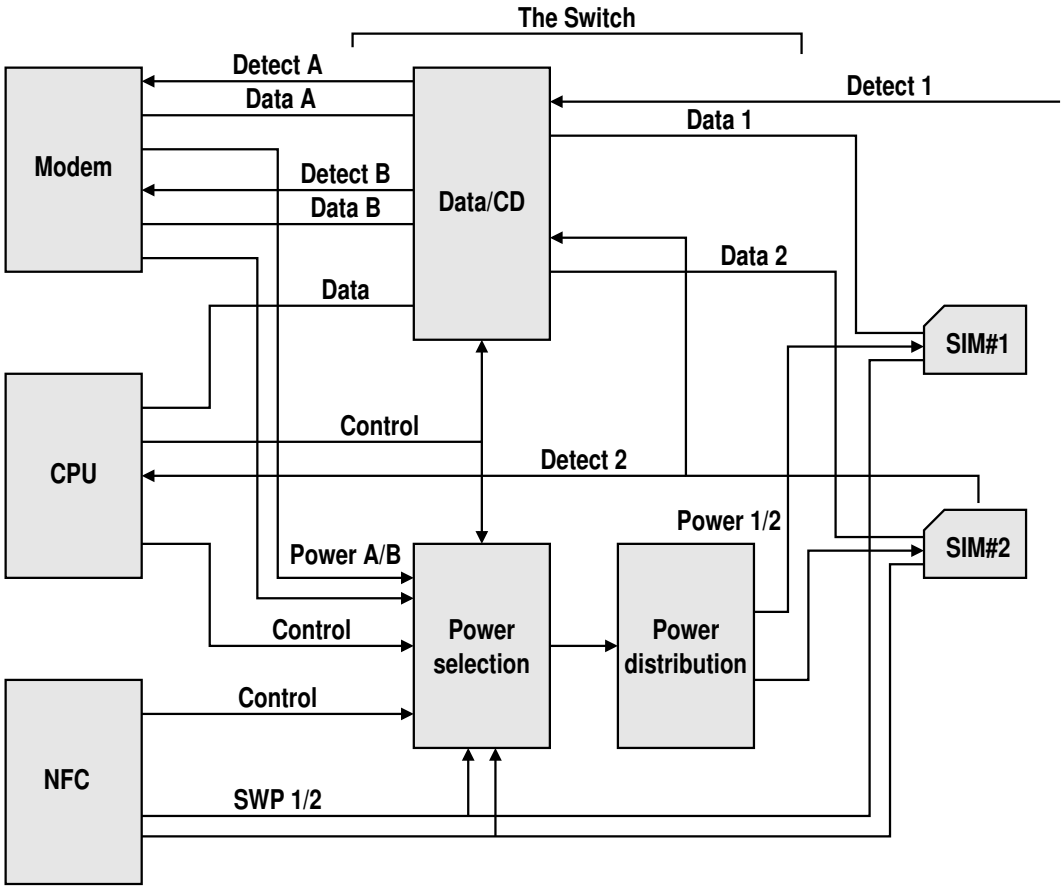
2.3 NFC

Since the NFC subsystem provides two separate SWP channels and SWP is not used by anything else, it can simply connect to both SIM cards and let software select which channel to use.

The power management subsystem monitors the two SWP lines and supplies power (if not already present) if detecting activity. This power supply remains active until explicitly reset by a signal from the NFC subsystem. This is explained in more detail in section 3.2.

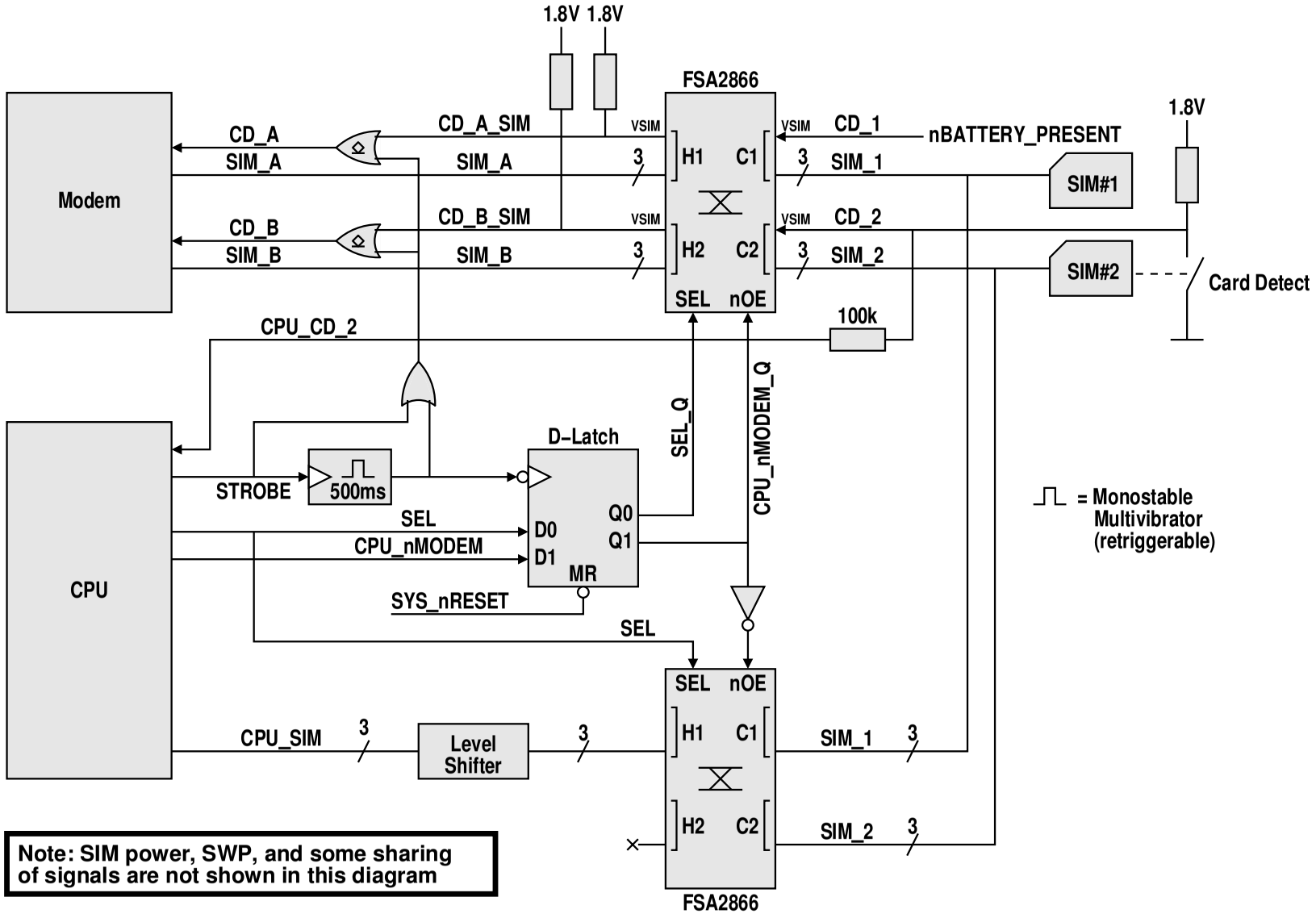
3 The switch

The switch consists of three parts: a pair of analog switches for the SIM data interface and the card detection signals, the power selection logic, and the power distribution circuit. The following diagram refines the overview from the introduction and shows how the various elements are related.



3.1 Data switching and card detection

The following diagram shows the switching of data and card detection signals. A pair of Fairchild FSA2866 analog switches [7] performs the actual switching.


1.8V 1.8V
FSA2866
Modem
CD_A
SIM_A
CD_A_SIM
SIM_A
VSIM
3
H1
C1
CD_1
nBATTERY_PRESENT
SIM_1
SIM#1
1.8V
CD_B
SIM_B
CD_B_SIM
SIM_B
H2
C2
CD_2
SIM_2
SIM#2
Card Detect
SEL
nOE
CPU_CD_2
100k
CPU
STROBE
500ms
D-Latch
SEL_Q
CPU_nMODEM_Q
SEL
CPU_nMODEM
D0
D1
Q0
Q1
MR
SYS_nRESET
= Monostable Multivibrator (retriggerable)
CPU_SIM
Level Shifter
Note: SIM power, SWP, and some sharing of signals are not shown in this diagram

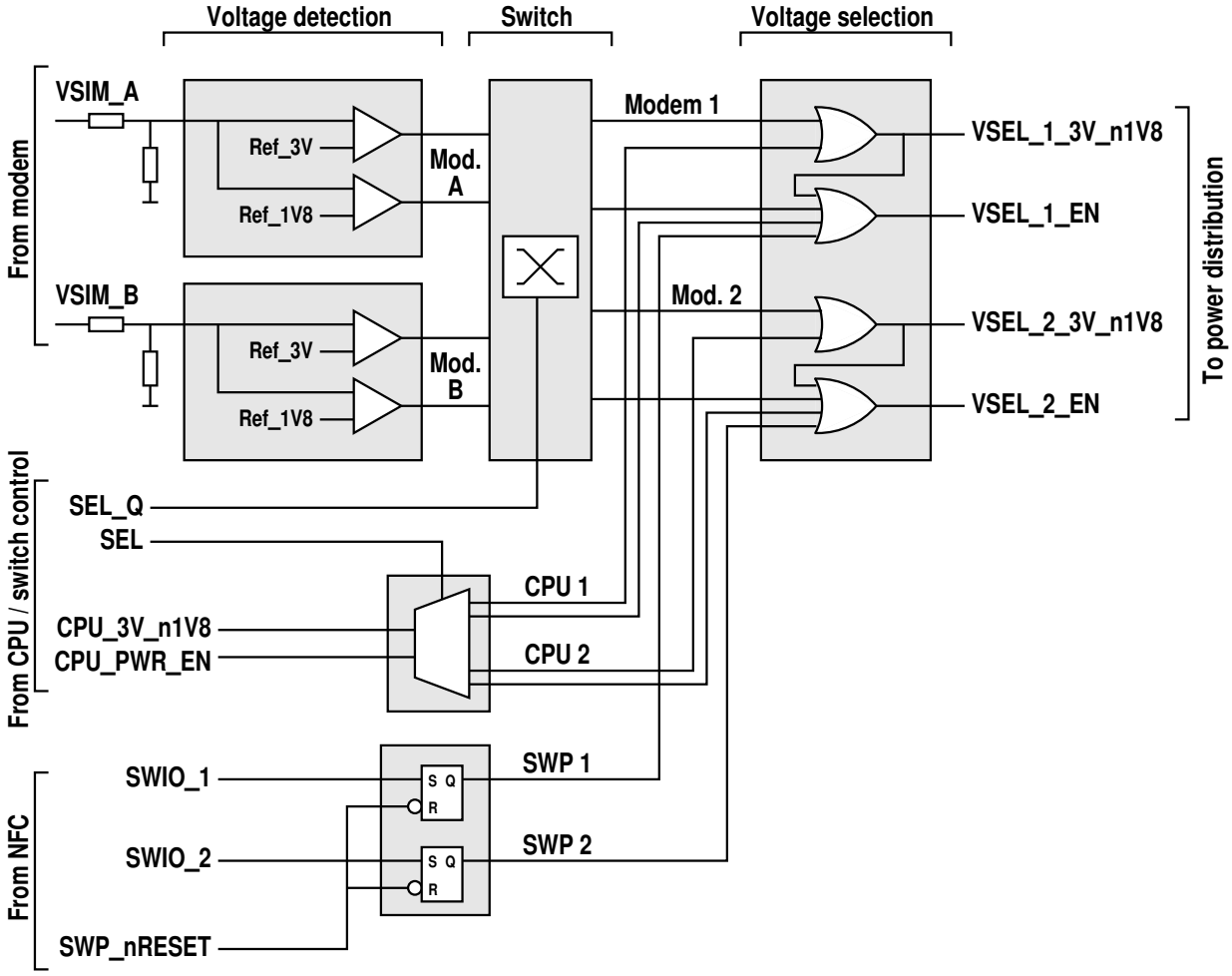
The control logic ensures that a card change is signaled to the modem during at least 500 ms before the switch configuration is changed. For regulatory considerations, this logic should be implemented with discrete logic.

The level shifters for CPU_SIM are discussed in section 2.2.2.

Please note that, in the FSA2866 serving the modem, we use the lines intended for switching power for the card detection signal instead. This is to ensure that the switching of data and of card detection can never disagree.

3.2 Power selection

The following diagram shows the power selection logic. The entire circuit can be implemented with a single Silego SLG46721 mixed-signal array [8].



Since power can be requested by various entities, we do not route modem power directly through the switch but instead measure the voltage the modem outputs and request the corresponding voltage from the following stages. (Block “Voltage detection”.)

Since the analog input voltage must not be greater than VDD, the voltages output by the modem must be divided by at least ÷2.

The resulting request signals, corresponding to the modem's SIM buses A and B, are then routed (block "Switch") towards the respective SIM, according to the setting of the data switch (SEL_Q).

The per-SIM request signals from the modem are then merged with the request signals from CPU and NFC, and for each SIM, the highest selected voltage is requested from the power distribution subsystem. (Block "Voltage selection".)

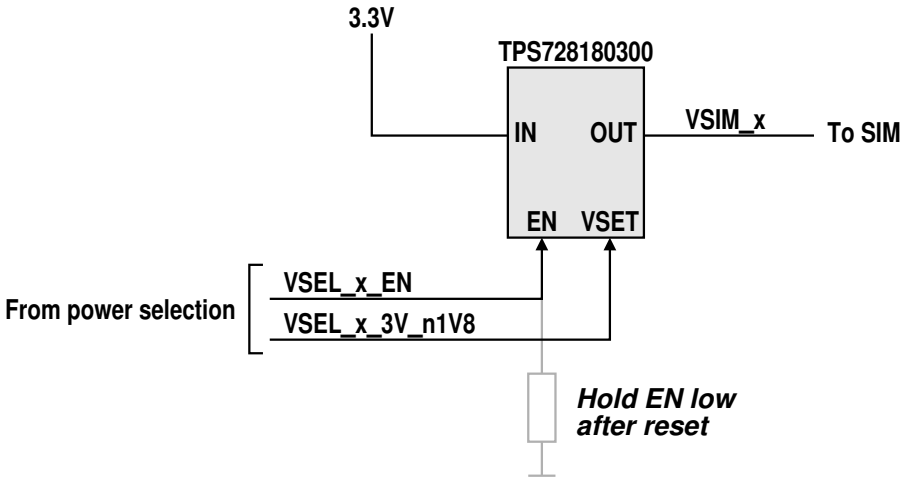
The CPU simply indicates whether it wants to request SIM power, and which voltage. This information is then routed to the corresponding SIM according to the switch setting (SEL). The CPU must keep CPU_PWR_EN low while CPU_nMODEM_Q is low.

NFC is not affected by the switch setting, and activity on the respective SWIO line generates an 1.8 V request for the respective SIM. This request remains active until explicitly reset by asserting SWP_nRESET.

Regarding the outputs, we show a configuration where each channel has an enable signal and a voltage selection signal, suitable for interfacing with the circuit described in section 3.3. Alternatively, one could use one enable signal for each voltage, e.g., to control individual switches.

3.3 Power distribution

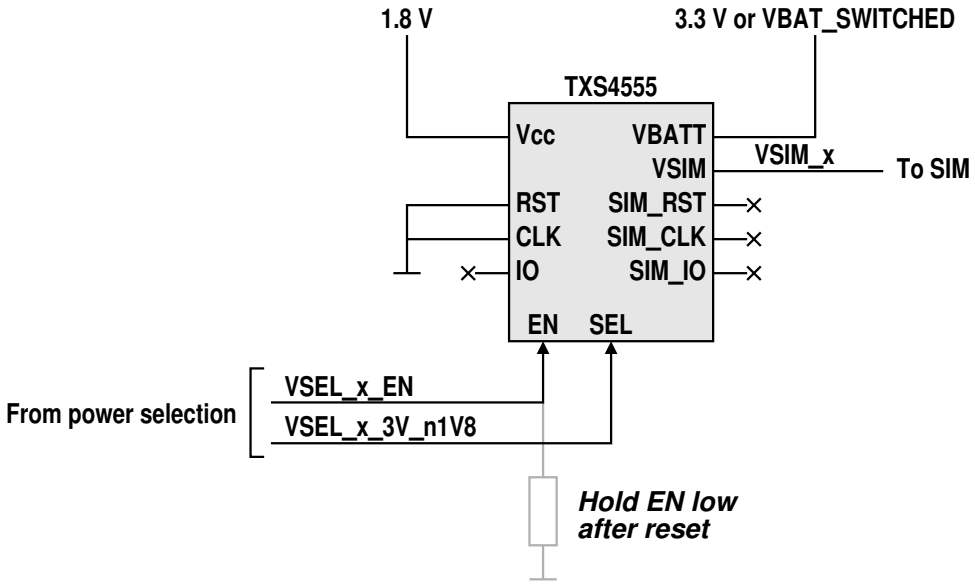
SIM power is provided by voltage regulators – one for each SIM – that are configured according to what the power selection subsystem requests. As an example, the Texas Instruments TPS728180300 [9], available in a 1.4 mm^2 5-BGA package, could be used:



This regulator outputs either 1.8 V or 3.0 V. When disabled, it discharges its output through a 60 Ω resistor.

There are also similar dual-voltage regulators specifically designed for use with SIM cards, with enhanced ESD protection, and that also include level shifters, e.g., the Texas Instruments TXS4555 [10].[4]

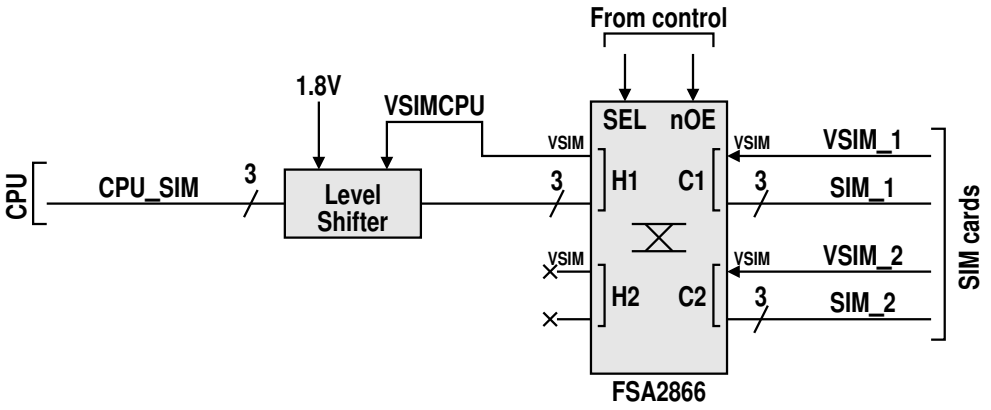
We will use this regulator with built-in level shifters, but since our design is more complex than the type of SIM applications this chip is designed for, the level shifting capabilities are of no use and are ignored.



3.4 Level shifter voltage

The last missing piece is the high-side voltage for the level shifters between CPU and the switch. Since this voltage has to match the supply voltage of the currently selected SIM, we can simply pass the SIM supply voltage back through the analog switch that also selects the data signals.

The analog switch serving the CPU shown in section 3.1 can therefore be completed as follows:



[4] Many other companies offer 4555 chips as well. However, most use a 9 mm^2 16-QFN footprint while – for space reasons – we use the 3.4 mm^2 12-QFN package only offered by Texas Instruments.

Note: to keep things clear and simple, these power connections are not shown in the overview diagram in section 3.

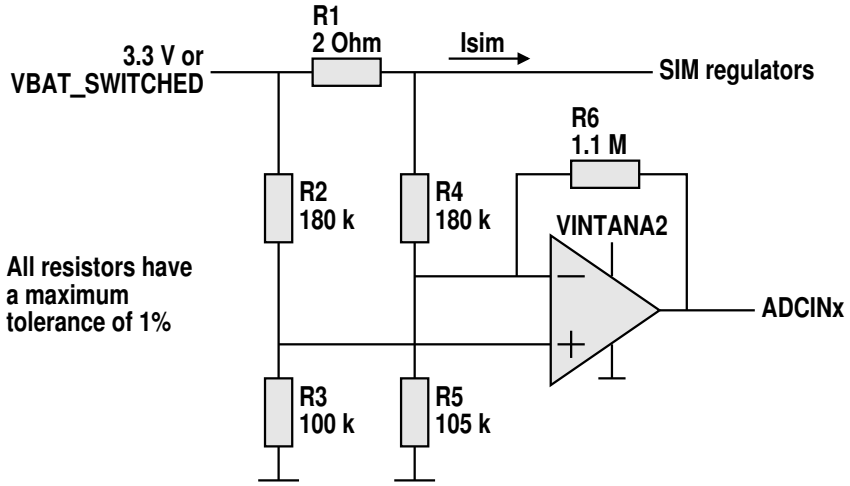
4 SIM monitoring

In order to monitor SIM activity, be it commanded from an outside source or initiated by the SIM itself, we monitor the current consumption of the SIM cards. The circuit consists of a differential amplifier whose output is sampled by the monitoring ADC (MADC) in the companion chip.

For simplicity, we measure the total current for both SIMs. To monitor a single SIM, the other should be powered down or removed.[5]

4.1 Current measuring circuit

The basic idea is to measure the voltage drop the SIM current produces across a shunt resistor. The maximum supply current is 50 mA per SIM,[6] yielding a total of 100 mA for both SIMs. Assuming the SIM regulators are supplied from the 3.3 V rail, the shunt resistor can drop up to 200 mV given the 100 mV dropout voltage of the regulator itself.[7] The maximum value for the shunt resistor is therefore 2 Ω.



To match the allowed voltage range of the MADC input,[8] we operate the opamp at the VINTANA2 voltage.[9] Given that VINTANA2 may be as low as 2.5 V, and the regulator input is either 4.30 V

[5] PCB space and available ADC inputs permitting, a variant of the same circuit could also be used to monitor each SIM individually. We briefly discuss this in section 4.6.

[6] Table 6.3 in section 6.2.3 of [1]: 50 mA for class B (3.0 V), 30 mA for class C (1.8 V). Sections 5.2.1 and 5.3.1 allow for spikes of up to 60 mA for either class, with a maximum duration of 400 ns. We consider accurate measurement of such such short spikes well beyond the design objectives for this circuit. (See also section 4.2.)

[7] Parameter V_{DO} on page 6 of [10].

[8] Table 5-75 in section 5.6.2 of [12] specifies the maximum input voltage of the MADC as 2.5 V. According to section 4.1, the absolute maximum rating for an input is given by the voltage of the corresponding power supply. In the case of to ADCIN2 to ADCIN7, the supply is VINTANA2 (table 3-1 in section 3.2), with a software-selectable voltage of 2.5 or 2.75 V (section 4.6). We designed the SIM current sensing circuit such that it is safe to use with 2.5 V.

[9] Supplying the opamp from VINTANA2 also ensures that the ADC input is grounded when VINTANA2 is turned off, as required in note (1) on table 5-76 in section 5.6.3 of [12]. The VINTANA2 regulator provides up to 250 mA (section 4.6).

(maximum battery voltage) or 3.3 V, we use voltage dividers to lower the voltage at the opamp inputs to a maximum of 1.54 V.

We designed the circuit for opamps with "rail-to-rail" outputs, corresponding to the characteristics of the ADC input. The 2 Ω and 1.1 MΩ resistor values were selected from the E24 scale, and 105 kΩ is from the E48 scale. Resistors for all these values are expected to have good availability at 1% tolerance.

4.2 Measurement resolution and sample rate

The MADC has a resolution of 10 bits[10] over the input range 0–2.5 V, giving us a resolution of 2.44 mV. The opamp circuit has a current-to-voltage conversion ratio of 7.28 V/A. The smallest current difference the ADC can distinguish is therefore 335 μA.

We note in passing that the actual power consumption of an active SIM card may be well below the 30 to 50 mA allowed by [1]. While we could not find any publicly accessible document specifying the current consumption of SIM cards, one example of a Java Card employing similar technology is specified with an idle current of 100 μA and an active current of 10 mA.[11]

The MADC can sample all 16 channels in 288–529 μs and a single channel in 18–33 μs.[12]

4.3 Leakage

The supply-to-ground resistance across R1 to R6 is 139 kΩ. The Leakage current is therefore 24 μA at 3.3 V or 31 μA at the 4.3 V battery.

Each regulator consumes at most 35 μA when enabled and idle, 3.5 μA when disabled.[13]

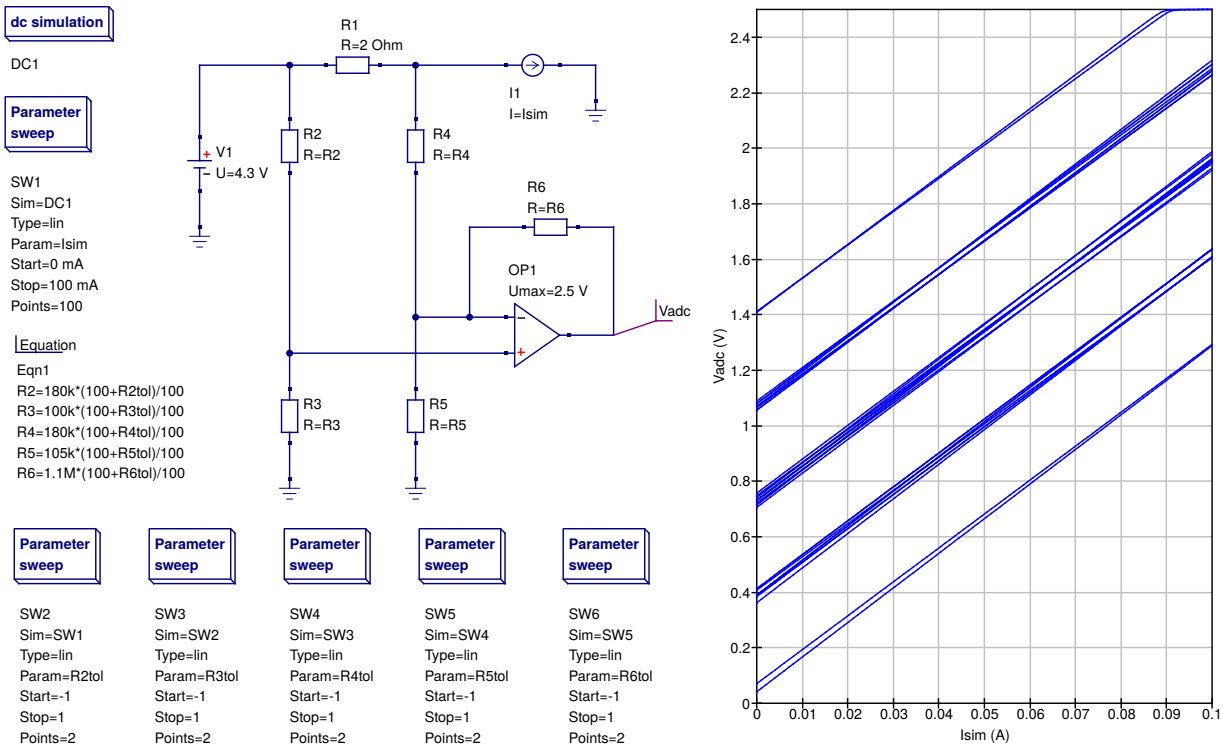
Current consumption of the opamp is expected to be significantly below 1 mA. We discuss opamp characteristics in section 4.5.

When VINTANA2 is turned off, the inputs of the opamp draw 24 μA each through the clamp diodes in the opamp.

4.4 Simulation

We analyzed the performance of the circuit and the effect of component tolerances on its characteristics with the following simulation:

[10] Table 5-75 in section 5.6.2 of [12].
[11] `http://www.smart-ecard.com/pdf/7400021F_CLXSU512KJ3-DIJ_TechBrief.pdf`
[12] Table 5-77 in section 5.6.3.1 of [12].
[13] I_{GND} and I_{SHDN} on page 6 of [10].



The plot on the right side shows the output voltage as a function of the current across the shunt resistor R1, for all combinations of the resistors R2 to R6 each being at either the minimum or maximum allowed resistance value, given a 1% tolerance.

Due to the large common mode voltage on the sense inputs, even small component tolerances have a large effect on the resulting output. This results in a DC offset on the output signal that will differ from device to device. This offset can be trivially compensated by measuring the voltage when the regulator is turned off.

4.5 Opamp selection

The most important selection criteria for the opamp are:

- operating voltage includes the 2.5–2.75 V range,
- lowest output voltage $\leq$ 40 mV (see below),
- compact package,
- low idle current, and
- reasonable price and availability.

The 40 mV output voltage minimum of our circuit is obtained from the simulation, where the ideal opamp produces this voltage for a load current of 0 A, given worst-case resistor tolerances. A real-life opamp introduces the following limitations:

- The minimum output voltage $V_{OL}(\max)$ is typically a few mV to a few dozen mV above 0 V, even if the opamp is "rail-to-rail", and
- the output can be shifted up or down by the maximum input offset voltage (V_{OS}) multiplied by the loop gain of the opamp circuit.

We therefore need an opamp that fulfills the following criteria, in addition to the operating voltage range of 2.5–2.75 V: $V_{OL}(\max) \leq 40$ mV and $|V_{OS}(\max)| \cdot \beta \leq 40$ mV, with a loop gain of $\beta = {}^{R6}/_{R5} = 10.5$.

Furthermore, since inputs of the opamp can raise above its supply voltage when VINTANA2 is disabled, the inputs must be clamped to the positive supply voltage.[14]

The Analog Devices ADA4505-1 [13] fulfills all the above criteria, draws only 10 μA, and is available in a space-saving $1.4 \times 0.9 \times 0.6$ mm^3 chip scale package.

4.6 Individual monitoring of each SIM

As mentioned above, the circuit could be extended to monitor each SIM individually. To do so, a second opamp is needed (e.g., by replacing the ADA4505-1 with the dual-channel ADA4505-2), and R1 and R4 to R6 have to be duplicated for the second channel. R2 and R3 can be shared. Since the maximum load current is then 50 mA instead of 100 mA, R1 should be increased to 4 Ω. To avoid clipping at the maximum current, R6 may be reduced to 1 MΩ.

[14] Some opamps (e.g., the microchip MCP6071 series) only clamp their inputs to ground and rely on a Zener diode (or similar) to suppress excursions above the positive supply voltage. Such a chip would be unsuitable for our purposes.

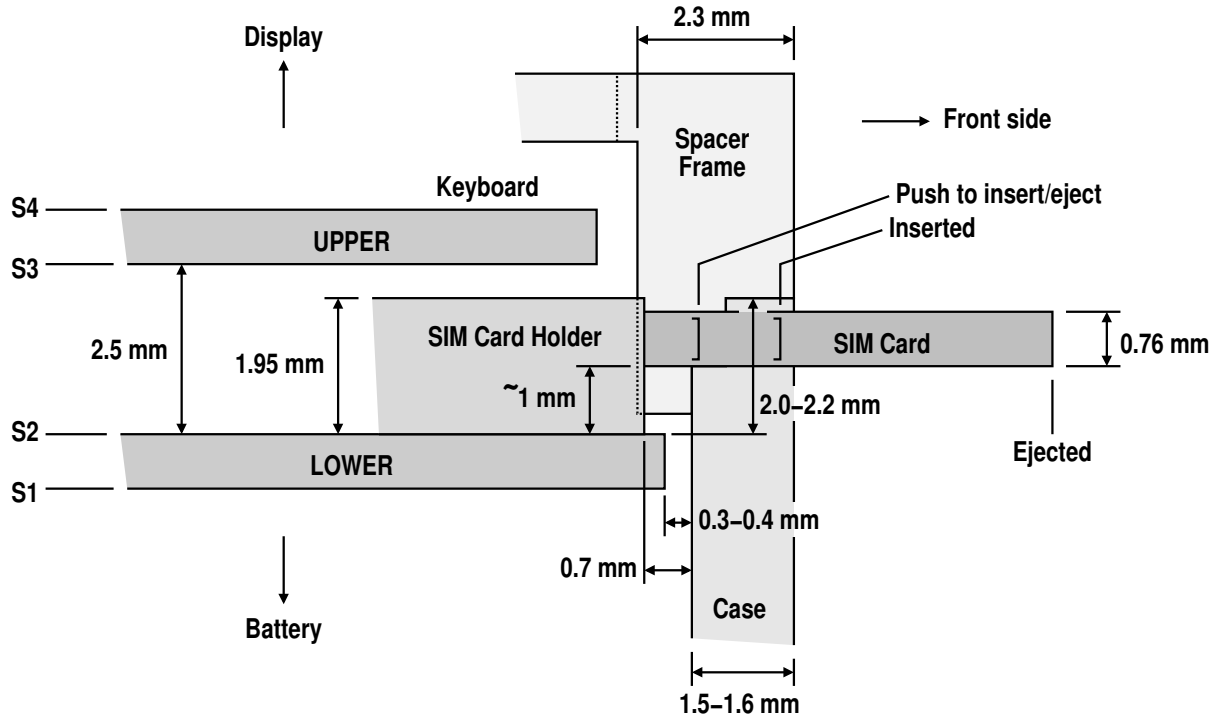
A Placement of second SIM holder

We use the Amphenol 10100271 [14] SIM card holder with an overall thickness of 1.95 mm, for standard Mini-SIM of 25 mm × 15 mm × 0.76 mm. The card is pushed in to insert and pushed again to eject.

A.1 Vertical stacking

The card holder is placed such that the opening for the SIM card consists of one or two U-shaped cut-outs in the (former) N900 case and/or the spacer frame. It would be preferable to have the cut-out only in the spacer frame, over which we have full design and manufacturing control, but no suitable location is available.

We therefore place it on the S2 surface, i.e., the top side of the LOWER PCB, as shown in the following drawing:



Additional dimensions and the underlying measurement data can be found on the "Stacking and measurements" page at `https://neo900.org/stuff/werner/stacking/`

A.2 Distance to wall

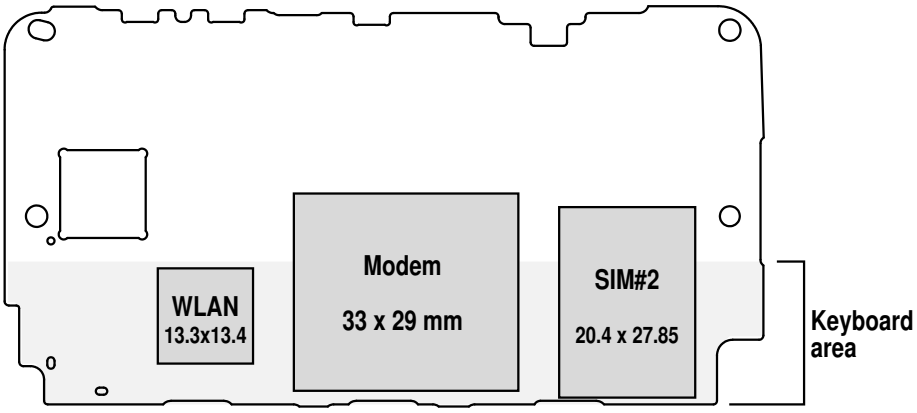
The card holder is placed such that its edge is 0.7 mm from the inside of the case wall. The following table shows the nominal positions relative to card holder and either side of the wall for different card states:

State	Position of card edge (mm) relative to ...		
	Card holder	Case wall Inside	Outside
Ejected	6.0	5.3	3.8
Inserted	2.0	1.3	−0.2
Pushed	0.8	0.1	−1.4

Ensuring that the position relative to the inside of the wall never becomes negative prevents the card from sliding up inside the case, and getting stuck.

A.3 X placement

The placement of the second SIM card holder along the Y and Z axes is determined by clearly defined mechanical constraints. We have more leeway on the X axis. The following drawing suggests an approximate placement of the three tall components that are located on S2:



The basic idea is to place these components under the keyboard area. When typing on the keyboard, the PCB flexes a little. This causes mechanical stress on chips mounted on the other side of the PCB, and on their solder joints. Such stress may eventually lead to device failure. We therefore want to avoid placing components under the keyboard on S3, especially no large chips.

Meanwhile, the modem and WLAN modules and the second SIM card holder are too tall to leave much room for other components on the PCB above them. We should therefore try to overlap the area where we do not wish to place large components as much as possible with the area where we can only place very thin (if any) components.

The above placement is merely a suggestion. Layout will encounter further constraints and therefore has the final say.

A.4 Case cut-out

To Do

B References

[1] ETSI TS 102 221 V11.1.0 (2013-11). *Smart Cards; UICC-Terminal interface; Physical and logical characteristics (Release 11)*, http://www.etsi.org/deliver/etsi_ts/102200_102299/102221/11.01.00_60/ts_102221v110100p.pdf

[2] ETSI TS 102 613 V11.0.0 (2012-09). *Smart Cards; UICC - Contactless Front-end (CLF) Interface; Part 1: Physical and data link layer characteristics (Release 11)*, http://www.etsi.org/deliver/etsi_ts/102600_102699/102613/11.00.00_60/ts_102613v110000p.pdf

[3] Almesberger, Werner. *Neo900 NFC Subsystem*, Draft, December 2015. https://neo900.org/stuff/papers/nfc-draft.pdf

[4] ETSI TS 102 600 V7.5.0 (2009-04). *Smart Cards; UICC-Terminal interface; Characteristics of the USB interface (Release 7)*, http://www.etsi.org/deliver/etsi_ts/102600_102699/102600/07.05.00_60/ts_102600v070500p.pdf

[5] NXP Semiconductors. *Level shifting techniques in I^2C-bus design*, AN10441, Rev. 01, June 2007. http://www.nxp.com/documents/application_note/AN10441.pdf

[6] Texas Instruments Incorporated. *Voltage-Level Translation With the LSF Family*, SLVA675B, March 2015. http://www.ti.com/lit/an/slva675b/slva675b.pdf

[7] Fairchild Semiconductor. *FSA2866 - Dual-Host / Dual-SIM Card Crosspoint Analog Switch*, May 2011. https://www.fairchildsemi.com/datasheets/FS/FSA2866.pdf

[8] Silego Technology, Inc. *SLG46721 - GreenPAK 3 Programmable Mixed Signal Array*, Rev 1.10, October, 2015. http://www.silego.com/uploads/Products/product_243/SLG46721r110_10282015.pdf

[9] Texas Instruments Incorporated. *TPS728xx Series - 200mA Low-Dropout Linear Regulator with Pin-Selectable Dual-Voltage Level Output*, SBVS095, August 2007. http://www.ti.com/lit/ds/symlink/tps728.pdf

[10] Texas Instruments Incorporated. *TXS4555 - 1.8V/3V SIM Card Power Supply With Level Translator*, SBOS550B, August 2013. http://www.ti.com/lit/ds/symlink/txs4555.pdf

[11] Fairchild Semiconductor. *FPF1320 / FPF1321 - IntelliMAX^{TM} Dual-Input Single-Output Advanced Power Switch with True Reverse-Current Blocking*, September 2013. https://www.fairchildsemi.com/datasheets/FP/FPF1321.pdf

[12] Texas Instruments Incorporated. *TPS65950 Integrated Power Management and Audio Codec*, SWCS032F, Silicon Revision 1.2, July 2014. http://www.ti.com/lit/ds/symlink/tps65950.pdf

[13] Analog Devices. *ADA4505-1/ADA4505-2/ADA4505-4 - 10 μA, Rail-to-Rail I/O, Zero Input Crossover Distortion Amplifiers*, Rev. D, 2010. http://www.analog.com/media/en/technical-documentation/data-sheets/ADA4505-1_4505-2_4505-4.pdf

[14] Amphenol 10100271. *SIM Card Reader 8Pin (Push/Push) With Switch*, April 2009. http://media.digikey.com/pdf/Data%20Sheets/Amphenol%20PDFs/101-00271.pdf