Michael Fuchs, BSc.

Development of an UWB Radio Platform with Hardware Components and System Software

MASTER THESIS

to achieve the university degree of

Master of Science

Master's degree programme:
Electrical Engineering and Audio Engineering

Submitted to

Graz University of Technology

Supervisor
Ass.Prof. Dipl.-Ing. Dr.techn. Peter Söser

Institute of Electronics

Second Supervisor
Dipl.-Ing Thomas Baier

Graz, February 2016

AFFIDAVIT

I declare that I have authored this thesis independently, that I have not used other than the declared sources/resources, and that I have explicitly indicated all material which has been quoted either literally or by content from the sources used. The text document uploaded to TUGRAZonline is identical to the present master's thesis dissertation.

Date

Signature

Abstract

English

The aim of this thesis is to develop a car key incorporating an IC featuring UWB IR radio and another low power IC used as wake up device (via LF communication or simply trigged by pressing a button). To power the two ICs by a single coin cell (CR2032), a power management system also has to be developed.

The UWB IC is used to measure the distance between the car key and the car. Furthermore, two software versions should be developed for two different purposes:

The first version should perform a single ranging measurement as soon as the key is triggered by the press of a button or by the detection of a low frequency field. It should then put the device into a low-power state and wait for the next trigger to wake up and perform another measurement.

The second version should be able to localize the key by *two- dimensional triangulation* at least twice a second, assuming the driver always approaches the car from the driver's side. For this second application, the device should be powered by a Lithium-ion-polymer accumulator to account for the higher current consumption that goes along with the ongoing ranging measurements.

Deutsch

Ziel dieser Arbeit ist die Entwicklung eines Autoschlüssels, der einen Ultrawideband-IC mit einem bestehenden Low-power-IC, welcher als Wakeup-Device dient, verbindet. Dazu ist eine Stromversorgung zu entwickeln um den Schlüssel mit einer einzelnen Knopfzelle (CR2032) zu betreiben.

Der UWB-IC wird dazu benutzt die Distanz zwischen Auto und Schlüssel zu bestimmen. Zudem sind zwei Softwareversionen für zwei verschiedene Anwendungsfälle zu entwickeln.

Die erste Version soll eine einzelne Distanzmessung vornehmen sobald ein Knopf gedrückt wird oder der Schlüssel einen Wakeup von einem LF-Feld detektiert. Danach soll das Gerät in einen stromsparenden Modus umschalten, woraus es nur durch einen erneuten Trigger (LF-Feld, oder Knopfdruck) erwacht.

Die zweite Version soll mithilfe einer zweidimensionalen Triangulation mindestens zwei mal pro Sekunde den Schlüssel detektieren können, wenn davon ausgegangen wird, dass sich der Fahrer dem Auto ausschließlich auf der Fahrerseite nähert. In dieser zweiten Applikation wird der Schlüssel von einem Lithium-Ionen-Polymer-Akkumulator versorgt, der den benötigten, höheren Strom für diese Messung zur Verfügung stellen kann.

Special Thanks

I want to thank all my friends for the support they have given me over the years. You were always there guiding my way and supporting me in good times as in bad. I could not have done this without you.

In addition, I want to thank my family for making it possible to achieve this goal. You took the time to let me make my own decisions, even if this was not the fastest way to get there.

I also want to thank the University of Graz for the great time during which I was allowed to study here. I also had the pleasure to work as a student assistant for a few years and I can honestly say that this was one of the best jobs I have had so far.

Finally, yet importantly, I want to thank NXP for giving me the opportunity to write this thesis. A special thank goes out to my mentor Thomas Baier for all the advice and patience.

Contents

Figures

Tables

1   Passive Keyless Entry（PKE）Systems and Security

1.1   Introduction to PKE

More and more car manufacturers are gradually moving towards using passive entry systems. With these systems, the car owner does not have to use mechanical car keys or operate any buttons on remote controls to open the car. The pure presence of the car key (or key fob) itself in the immediate vicinity of the car is sufficient to unlock the car simply by touching the door handle. Also, operating the start button inside the car is sufficient to start it, as long as the key fob can be detected inside the car.

The system consists of a low frequency (LF) 125 kHz or 22 kHz magnetic induction wake up system, a VHF or UHF wireless remote control communication system and a passive NFC based immobilizer communications system as fallback solution in case the battery of the car key has run out of energy.

The LF system can detect a wake up pattern from the car when the key is in the vicinity. Figure 1 shows the area of LF signal coverage areas around the vehicle. The typical range of the magnetic induction field is about 2 meters. Beyond this distance, the field deteriorates quickly and makes it impossible for the key fob to detect the car. If the fob is somewhere in the marked areas 'inside' or 'outside' the LF signal will wake up the key to establish VHF or UHF communication. The key will then authenticate itself as a valid car key and the car in return will accept commands from it or react properly for instance if the driver touches the door handle or presses the start button.
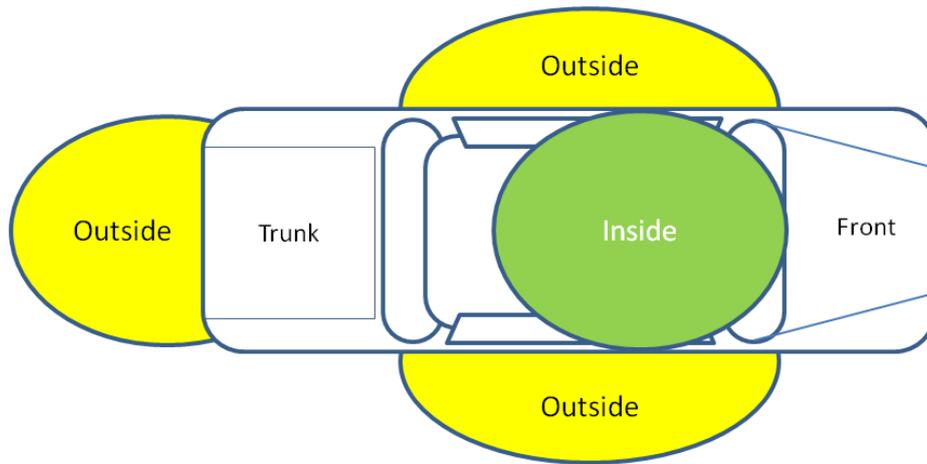
Figure 1 - LF Signal Coverage Areas of a Vehicle [1]

After receiving the LF wake up pattern there are two common implementations for the following protocol exchange. The flow of messages in these two implementations is outlined in Figure 2.
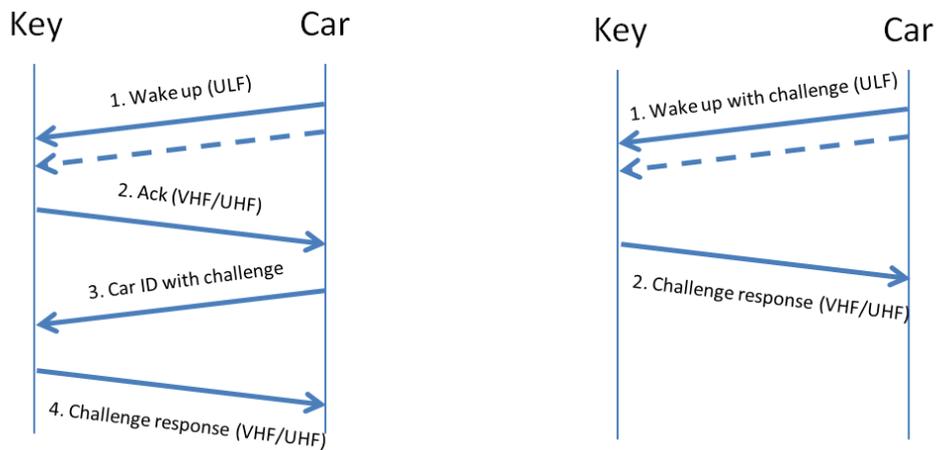
Figure 2 - Message Flow of PKE Systems [1]

In the first case (Figure 2 on the left) the LF message is only a wake up pattern, which contains either some basic information about the make and model of the car or even no content at all. If the key detects the LF message, it sends an acknowledgment message using the VHF/UHF channel. The car then again responds with an encrypted challenge

12

message, and the key responds to it with an equally encrypted response message. Finally, the car recognizes the key as valid and executes the desired action, like opening the door. The second implementation on the right shows another approach where the wake up signal already includes the challenge and the key responds directly by sending a challenge response via VHF or UHF.

As one can imagine the timing of such a PKE-system is critical. If the driver touches the door handle, for instance, the car has a very small time frame to verify that a registered key is in the vicinity and to execute the mechanism to unlock the door. As will be discussed in detail later, the total time allowed can be as short as 150 ms.

1.2   Security Aspects

In every PKE system, there are a number of security aspects implemented in the car as well as in the car key. A detailed discussion of those aspects however would exceed the scope of this master thesis and is therefore only mentioned on the margin.

The car and the car key typically offer some features regarding security issues, like the ability to generate random challenges from a pool of challenges to the effect that they are very hard if not impossible to predict. In addition, the key needs to be able to generate a cryptographically relevant response to the challenge received. Further, the car has to store keys and identifiers so that they cannot be tampered with or be read out. Also, there has to be a unique identifier of sufficient length to identify the car or the key. The car and the key also need to support a process through which a car key can be registered for a specific car. The programming must exclusively be conducted in a secure environment and the secret information stored inside the car key must only be available after authorization by the manufacturer.

1.3 Relay Attacks

This section gives a short overview of the most common relay attacks. Relay attacks are a special form of man-in-the-middle attacks. This is an attack where the attacker can secretly relay and possibly alter the communication between two parties, who themselves believe they are communicating directly with each other. The basic idea of this form of attack is depicted in Figure 3.
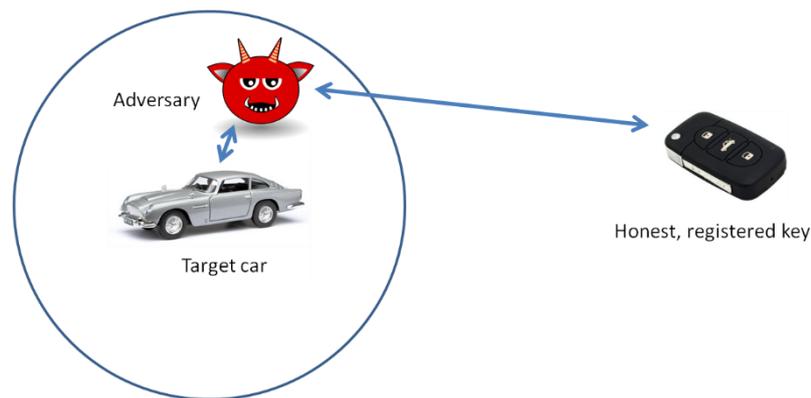
Figure 3 - Constellation for a Typical Relay Attack with PKE Systems [1]

These attacks can succeed because of current PKE systems, which allow for relatively long delays when the key communicates back to the car.[1]

In such a relay- or man-in-the-middle attack, the attacker is trying to make the car believe that an honest car key is in the vicinity of the car, even if the key is actually further away. In order for the attack to succeed, only one adversary has to be in the vicinity of the car. In addition, they must have wireless remote control of a legitimate key, which can be outside of the vicinity of the car.

The attack succeeds if the adversary manages to transmit the messages between the car key and the car over a long distance via cable or wireless connection. In the end, both the car and the car key think that they have been talking directly to each other. The attacker does not even have to have knowledge about the protocol data being actually sent between car and key, nor about the challenge presented by the car to the key. Also, the owner of the key does not have to press any buttons of the key, since

---

[1] Relay Attacks on Passive Keyless Entry and Start Systems in Modern Cars.

this is generally not necessary with PKE systems. Typically, the owner of the key is totally unaware that an attack has been executed.

The same principle can also be used in a more sophisticated way if there are two attackers, as can be seen in Figure 4.
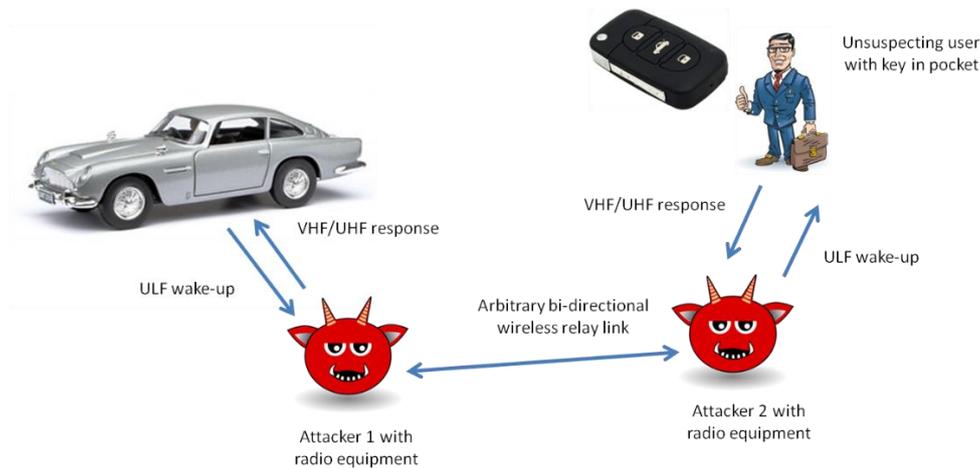
Figure 4 - Principle of a Man-In-The-Middle Attack [1]

For this implementation of the relay attack, two attackers employ a bi-directional wireless connection between them in order to complete the attack. This can work over even longer distances. Practical scenarios of such an attack include restaurants, elevators in parking garages or the driveway scenario, where the car is parked outside of the house and the key is kept inside the jacket hanging in the hallway behind the front door.

To avoid such man-in-the-middle attacks it is necessary that the car is able to determine the exact distance between itself and the key before sending any challenges to the key. This additional measurement would have to be initiated by the key after receiving an LF wake up pattern. Only after the car confirms the key being in the vicinity of the car it is safe to send any encrypted data, at which time a challenge should be sent to the key, and car and key follow the standard PKE procedure to unlock the car. Otherwise, the car will refuse to open or execute any other PKE related functions such as autonomous parking. Nevertheless, the distance-bounding measurement should not affect the overall wireless remote control functionality, e.g. pressing buttons on the key to unlock the car should still be possible.

1.4 Future Use of PKE System

If the car key is far away from the car (up to 100 m) the key must only support some basic functions. In general, it only operates as a classical wireless remote control system. Some manufacturers however are planning to offer a new feature, namley 'approaching', which is activated once the car key can be identified to be located within 10 m of the car. The car then will perform a predefined action, e.g. turn some lights on to 'welcome' the driver. Any other functions would still need to be triggered by the driver, like pressing a button to unlock the doors.

Another future use is the accurate detection of the driver inside the car. The idea is that the driver can only start the engine by pushing the start button when the car localizes the key within the passenger compartment. This is meant to prevent a child from starting the engine while the owner is leaning against the car. This feature would require a very accurate localization within the range of 5 - 10 cm, which does not work with an LF signal, but is a possible future application of the UWB distance measurement.

Autonomous parking is another use case to be supported in the future. The use case itself is described by the user leaving the car and letting it park autonomously. The driver has to remain within 7 m of the vehicle while it is parking itself. If the car cannot detect the driver, it should abort the parking process and should not move any further.

1.5 Technical Requirements of a Distance–Bounding Functionality

1.5.1 Distance to be Covered

For all soon-to-be used functions like the autonomous parking feature or a 'welcome light', which activates some predefined lights when the driver approaches the car, it can be assumed that the driver needs to be in sight of the car. For all those purposes the minimum distance which the distance-bounding sub-system needs to be able to support even under worst conditions, shall be no less than 10 m. At this range a body attenuation of up to 20 dBm already needs to be taken into account. Beyond this distance, neither a welcome light function is reasonable nor must the car be allowed to park autonomously without the driver watching it. For the second purpose, it might even be required that the consumer holds the car key in his or her hand while the car is parking to abort the process by pressing a button if necessary. In addition, autonomous parking should be aborted automatically as soon as the driver leaves the vicinity (in this case 10 m) of the car.

1.5.2 System Latency

The latency requirements concerning the ranging process for the cases 'approaching' and 'autonomous parking' are for further discussion, since there are no laws yet for the latter. It can safely be expected that the most important case concerning the maximum latency is the PKE case. In this case, the maximum latency for the entire process – including the mechanical unlocking of the door – should not take longer than 150 ms upon the user starting to pull the door handle of the car.
It can be assumed that the mechanical unlocking process takes about 70 ms, e.g. 80 ms are left for the entire communication process associated with the PKE function including the distance bounding. The latency requirement for the engine start is also a topic for further discussion but can be assumed to be less stringent than for the PKE case.

1.5.3 Accuracy Requirements

Depending on the absolute distance between the key fob and the car, the distance-bounding method should achieve the following minimum accuracy levels shown in

Table 1[2]. In order to achieve the range 'inside the car', which is a future use of the UWB ranging system, it may be required to evaluate the results of the distance measurement from multiple sensors, not just one, or to include other distance measurement technologies to rule out that the key is not inside the car.

Range	Minimum accuracy	Preferred accuracy
Inside the car [3]	< 10 cm	< 5 cm
Within 2 m of the car, but not inside the car	< 30 cm	< 30 cm
Within 10 m of the car, but not closer than 2 m	< 1 m	< 30 cm
Further away than 10 m	< 1m	< 30 cm / 1 m (tbf)
Within 7 m of the car (Autonomous parking)	< 50 cm (tbf)	< 30 cm (tbf)

Table 1- Required Accuracy Levels for Distance Bounding

1.5.4 Electrical Specifications

The power supply of the key shall be a regular CR2032 coin cell with a nominal voltage of 3 V. The maximum peak current the battery can deliver should be assumed 20 mA. As it is discussed in detail in chapter 5, any higher current will cause the button cell to appear, as it has been short-circuited, e.g., its output voltage will drop quickly below acceptable levels. Limiting the output current to 20 mA can also extend the lifetime of the battery.
The total PKE car key solution should be designed to support a battery lifetime of at least one year.

It should be taken into account that the 125 kHz LF receiver sub-system in present PKE systems consumes an average current of 5 μA. In future, the UWB ranging system could be also used to wake up the key, and could therefore replace the LF receiver if it can achieve a comparable current consumption and thus be competitive.

---

[2] According to [1]

[3] The most important feature would be to determine if the key is inside or outside the car; the position within the car is not rated as critical.

2   Introduction to UWB

Ultra-wide-band (UWB) is a radio technology that can use a very low energy level for short-range, high-bandwidth communications over a large portion of the radio spectrum (Ultra-Wideband). It was first defined by the Defense Advanced Research Project Agency (DARPA) as any wireless transmission scheme with a fractional bandwidth of more than 25% where the fractional bandwidth is defined as the ratio of 3 dB signal bandwidth to center frequency. In 2002, the FCC updated this definition. According to the new definition a signal is considered UWB if either the -10 dB bandwidth of the signal is larger than 500 MHz or its fractional bandwidth is at least 0.2. The fractional bandwidth was defined as

$$B_f = \frac{Bandwidth(10\ dB)}{center\ frequency} = \frac{2(f_H - f_L)}{f_H + f_L}$$

(1)

where f_L and f_H are the lower und upper 10 dB frequencies of the power spectrum relative to the PSD peak. [2]
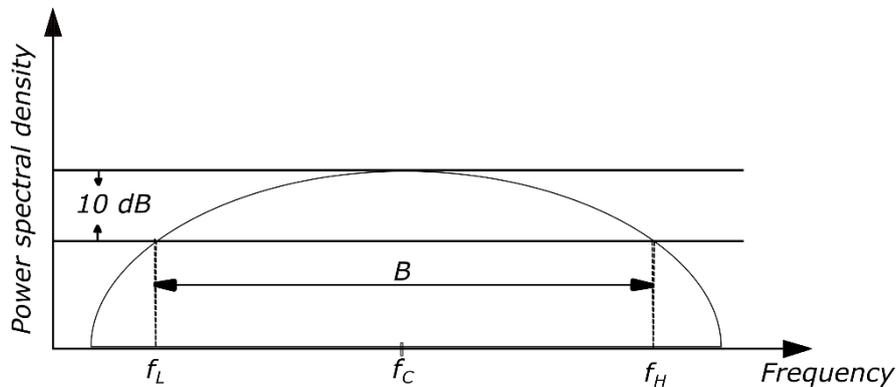
Figure 5- PSD Over Frequency for UWB [3]

UWB has many different applications from radar and sensing applications to high bandwidth communications. The technology has been around since the 1980s and has been mainly used for radar applications in its early days. Due to developments in high-speed switching technology, UWB has developed into more attractive communications applications [4]. It is therefore used in both commercial and military applications [5].

Ultra-wide-band employs a very different method of transmission than other wireless technologies. It does not use a specified carrier frequency, like traditional radio transmissions. Instead of transmitting information by varying the power level, frequency and/or phase of a sinusoid, it transmits information over a large bandwidth (>500 MHz) by generating very short pulses. Therefore UWB was formally referred to as *carrier-less radio* or *impulse radio*, but later renamed by a study panel from DARPA in 1989 [6].
The information can be modulated by encoding the polarity of the pulse, its amplitude and/or by using orthogonal pulses. Those pulses can be sent at different pulse rates, e.g. to support time or position modulation.

The most important aspect of UWB technology for this thesis is the ability to measure the 'time of flight' of the transmissions at various frequencies. This helps overcome multipath propagation in the broadest sense since some frequencies usually have a line of sight. In addition, though it is permitted to occupy low carrier frequencies, signals can more easily pass through obstacles. Another feature is that the pulses are very short (60 cm for a 500 MHz-wide pulse), so most signal reflections do not overlap with the original pulse. As a result, there is almost no multipath fading of narrowband signals. Finally yet importantly, UWB signals' shape is quite similar to noise, which makes it quite hard to detect and there is thus a lower chance of eavesdropping.

2.1 Bandwidth, Data Rate and Power Consumption

In information theory the well-known Shannon-Hartley theorem [7] describes a direct relationship between capacity and bandwidth as well as an inverse relationship between bandwidth and power consumption. Their theorem states

$$C = B \log_2 \left(1 + \frac{S}{N} \right)$$

$$(2)$$

where C describes the capacity in bits per seconds, B the bandwidth, S the average received signal power over B and N the average noise over B. The term $\frac{S}{N}$ is commonly referred to as signal to noise ratio (SNR).

Equation (2) states, that for a specific channel capacity we consume less power with a larger bandwidth. Because the SNR term is under a logarithm, it is easier to increase the capacity by increasing the bandwidth instead of the SNR. As UWB uses an enormously large bandwidth of at least 500 MHz, the theoretical channel capacity that can be achieved at low power levels can be very high and UWB is therefore a good opportunity to transmit a large amount of data. Due to restrictions of power spectral density, though, it is most commonly used over short distances. This insight and the fact that UWB has a very good time-domain resolution are the reasons for using UWB technologies in wireless sensor networks (WSN).

A WSN is simply defined as a large collection of sensor nodes. Such networks can be used for a large variety of applications where one sensor node detects environmental changes and reports them to other nodes over a flexible network architecture. Examples are networks in factories for condition-based maintenance, in homes to realize 'smart homes', or even in bodies for patient monitoring. Since a transceiver in such a network usually has to operate for several years with no battery maintenance, a key requirement is very low energy consumption.

2.2 Regulations and Standards

In 2007, the IEEE established the IEEE 802.15.4a standard, which was an amendment to IEEE 802.15.4-2006. The original standard, defined in 2003, specifies a protocol for Wireless Personal Area Networks (WPAN).

> *IEEE standard 802.15.4 intends to offer the fundamental lower network layers of a type of wireless personal area network (WPAN), which focuses on low-cost, low-speed ubiquitous communication between devices. It can be contrasted with other approaches, such as Wi-Fi, which offer more bandwidth and require more power. The emphasis is on very low cost communication of nearby devices with little to no underlying infrastructure, intending to exploit this to lower power consumption even more. The basic framework conceives a 10-meter communications range with a transfer rate of 250 kbit/s.* [8]

With the IEEE 802.15.4a amendment, additional physical layers (PHYs) were added to the original standard, one of which uses Direct Sequence

UWB, which is spectrally efficient and has precision ranging capability. This UWB PHY is designated for frequencies in three ranges (< 1 GHz, 2 GHz – 5 GHz and 6 GHz – 10 GHz). Since then, the UWB PHY also provides variable data rates (110 kb/s, 1.70 Mb/s, 6.81 Mb/s, 27.24 Mb/s). Along with the DS-UWB PHY, a second PHY, the Chirp Spread Spectrum (CSS) PHY should briefly be mentioned here. It supports communication with devices moving at high speeds at longer ranges. Both PHYs have added scalability to data rates as well as longer ranges and lower power consumption to the standard, which was originally intended with the IEEE 802.15 standard to emphasize very low cost communication systems. The IEEE 802.15.4a amendment has later been merged into and is superseded by IEEE 802.15.4-2011.

2.3 Feasibility of UWB Signals

Due to the modulation of extreme narrow pulses, UWB can deliver a large amount of data with low power spectral density. The brief duration of the pulses is the key to spreading the energy across a wide range of frequencies from near DC to several GHz. As a result, UWB signals share the frequency spectrum with other existing radio services. To most of those services, like WLAN (2.4 GHz or 5 GHz), Bluetooth (2.40 GHz – 2.48 GHz), LTE (0.7 GHz – 2.6 GHz), Cordless Phones and GSM (0.89 GHz - 1.9 GHz), GPS (1.18 GHz – 1.58 GHz) or Home RF, an UWB signal (3.1 GHz – 10.6 GHz) can be seen as random noise. Since the transmitted average power of UWB systems is extremely low, WLAN and WPAN systems can coexist in the same band. Since the power density of UWB signals is usually below the environmental noise (e.g. -41.3 dBm or 560 µW) and with direct signal spread spectrum (DSSS), which is described below, the signal energy becomes very low. As a result, the probability of detection as well as interference with other radio signals operating at the same frequency band is negligible. Figure 6 is a simplistic illustration of the overlay of UWB devices with some existing radio services.
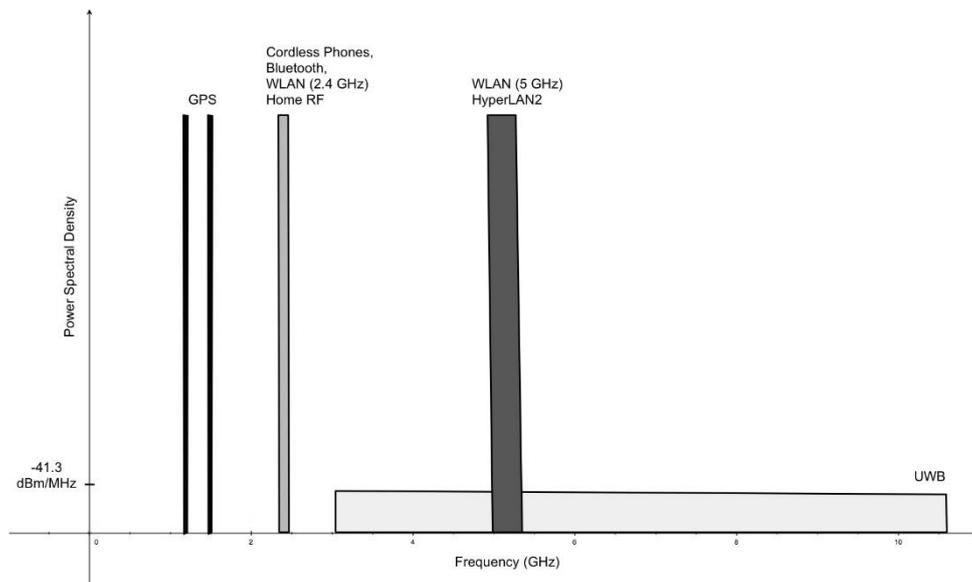
Figure 6 - PSD of Different Radio Services [9]

Table 2 shows a few standards and different technologies comparing data rate and distance. [9]

WPAN (IEEE)	Technology	Data Rate	Distance
IEEE 802.15.1	Bluetooth	1 Mbps	10 m (Class 3)
			100 m (Class 1)
IEEE 802.15.2	Coexistence Mechanisms between WLAN and WPAN		
IEEE 802.15.3	High Rate WPAN (UWB)	22, 33, 44, 55 Mbps	30 - 50 m
IEEE 802.15.3a	Alternate 15.3 PHY	> 100 Mbps	10 m
IEEE 802.15.4	Low Rate WPAN(ZigBee)	250 Kbps	1 - 100 m
IEEE 802.15.4a	Low Rate Alternative PHY of 802.15.4 (UWB)	5 Mbps	< 1000 m

Table 2 - Comparison of Different Technology Standards

2.4   UWB Implementations and Modulation Techniques

There are a number of different implementations of UWB systems such as impulse radio approaches using pulse-position modulation (PPM), pulse-amplitude modulation (PAM), binary phase-shift keying (BPSK) as well as frequency based approaches using pulsed orthogonal frequency division multiplexing (OFDM).

23

2.4.1 Spread-Spectrum Techniques

Most radio-based implementations use spread-spectrum techniques, which deliberately spread the signal in frequency domain, resulting in a wider bandwidth. The data of interest occupies a bandwidth in excess of the minimum bandwidth necessary to send the data. There are several different spread-spectrum techniques such as Frequency-Hopping Spread Spectrum (FHSS), Chip Spread Spectrum (CSS), Direct-Sequence Spread Spectrum (DSSS) and Time-Hoping Spread Spectrum (THSS), the last two of which should be described here shortly as parts of those modulation techniques that are used with UWB transmission.

2.4.2 Direct-Sequence Spread Spectrum （DSSS）

In DSSS modulation, the message signal is used to modulate a bit sequence known as the Pseudo Noise (PN) code. There are two modulation stages used in common radio systems. First the incoming data sequence is used to modulate a wideband code that transforms the narrowband data sequence into a noise like wideband signal. The spectrum spreading is accomplished by using the PN code sequence, which is independent of the data sequence. The duration of the pulse of the PN code is referred to as chip duration Tc and its inverse as chip rate Rc, which corresponds to the bandwidth of the signal.

Several chips represent a single information symbol, which adds redundancy to the signal. As a result, two positive effects are worth noting. First off, the signal is more likely to resist interference and enables secure communication. Unwanted listeners cannot easily detect the transmitted signal. Secondly, it is possible for multiple users to share a common channel without an external synchronization mechanism.
Last but not least, it should be mentioned again that spreading creates a lower power density. This allows the SNR of the signal to be below the noise floor level and the system will be less likely to interfere with other users on the same spectrum.

2.4.3 Time-Hopping Spread Spectrum （THSS）

Strictly speaking, THSS is not actually a spread spectrum technique, but can be used like DSSS to achieve a low probability of interception. For this purpose, the transmission time is changed randomly by varying the period and duty cycle of the pulse again using a pseudo random

24

sequence. The transmitted signal will then have intermittent start and stop times.

2.4.4 Pulse Shaping

The choice of the pulse is critical as its impulse response affects the PSD of the transmitted signal. In most literature, three types of pulses are employed, e.g., Gaussian pulse, Gaussian monocycle and Gaussian doublet. The latter two are the first and second derivative of the Gaussian pulse itself. (1)

The general formulas are given in (3) to (5) in which τ is a time constant. The pulses are depicted in Figure 7.

$$g_0(t) = e^{-\left(\frac{t-t_0}{\tau}\right)^2}$$

(3)

$$g_0(t) = \frac{t-t_0}{\tau}\, e^{-\left(\frac{t-t_0}{\tau}\right)^2}$$

(4)

$$g_0(t) = \left[1 - 4\pi\left(\frac{t-t_0}{\tau}\right)^2\right] e^{-\left(\frac{t-t_0}{\tau}\right)^2}$$

(5)
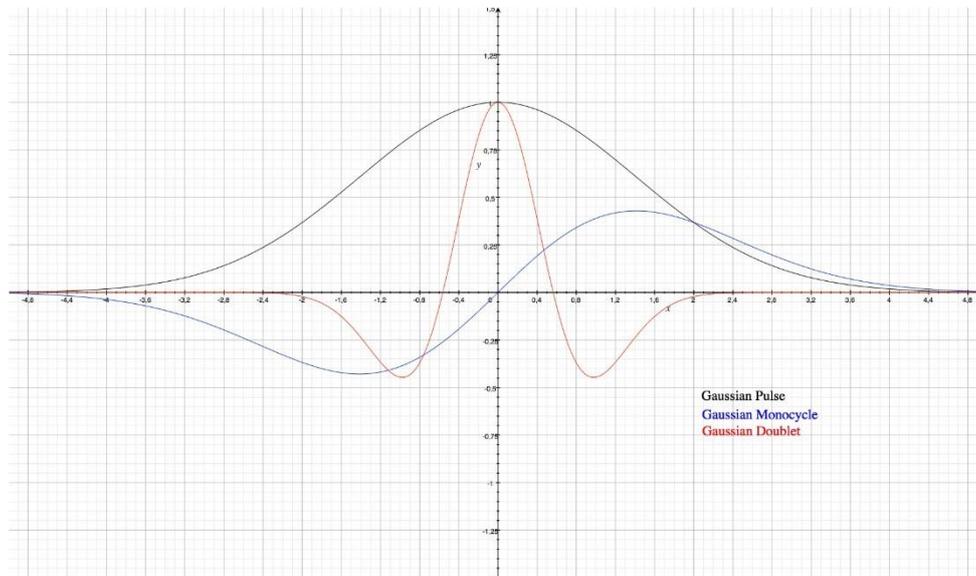
Figure 7 - Most Common Pulse Shapes for UWB [10]

There are different methods to generate such pulses e.g. simple MOSFET circuits. In addition, the pulse width depends on the circuit architecture as well as the semiconductor materials, which are used to generate the pulse. As this goes beyond the scope of this thesis, I will refer to [10] for some examples.

In the following examples the Gaussian doublet shall be used, since it is very common in a lot of UWB literature.

2.5   Example of the Discussed Modulation Techniques

The following example shows the method of binary phase-shift keying (BPSK) where the information corresponds to the polarity of the signals.

This impulse radio approach is only one method of using UWB systems. In this method, data is transmitted by low duty UWB signals and information is conveyed by position and/or polarity of the signals. Each symbol corresponds to one or more signals. [10]

In the following example, a time hopping (TH) code is used for determining the accurate position of a signal in a dedicated time frame. The TH code reduces the chance of interference with other UWB systems.

Each frame has the length Tf and consists of four IR signals. The signals are Gaussian pulses of length Tc, which is also the length of the chip-interval.

The TH codes for the symbols are {2,1}, {2,3} and {1,0} respectively, so the first and second signals are shifted by two and one chip-intervals and so on. Therefor the IR stream represents "101".
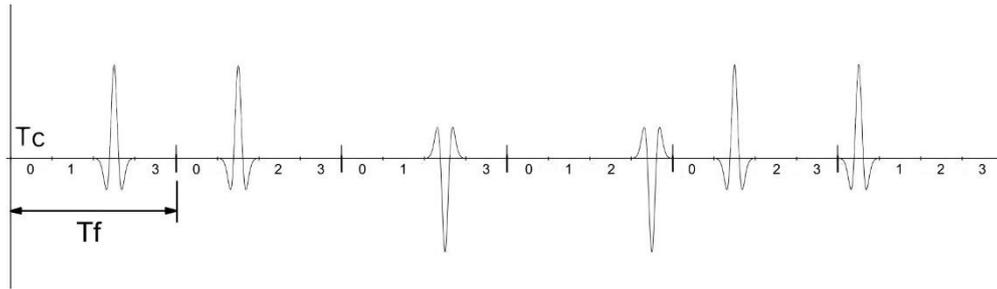
Figure 8 - BPSK with Time Hopping

While conventional narrowband and wideband systems use RF carriers to move the signal from the baseband to a carrier frequency, the UWB system can be implemented without a carrier. The data transmission with digital pulses substantially simplifies the transceiver circuitry in comparison with traditional RF radio systems.

To sum up the UWB system design Figure 9 finally shows a proposed, simplified DS-UWB transmitter. To transmit data over UWB it first has to be spread in the frequency domain. After, e.g., DSSS coding, the signal is modulated (e.g. with BPSK) and finally passes a pulse-shaping filter. The receiver does exactly the inverse of the mentioned process, which is visualizedin Figure 10 below.[4]

---

[4] Figure 9 and Figure 10 according to [9]
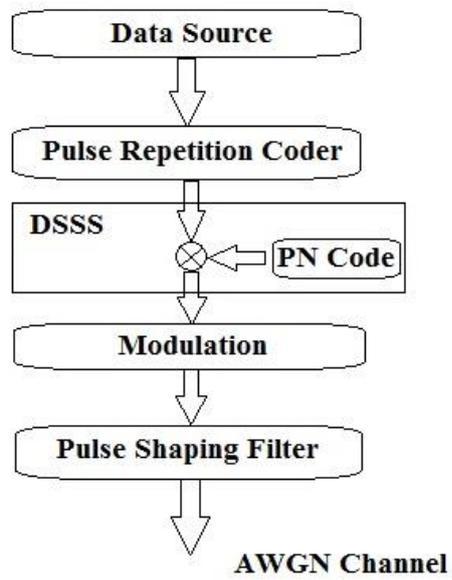
Figure 9 - Basic Concept of an UWB Transmitter
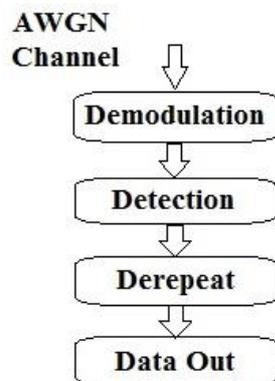
Figure 10 - Basic Concept of an UWB Receiver

3 Position- and Range-Measurements with UWB

3.1 Position Estimation

To estimate the absolute position of a target node in 2D or 3D space it is necessary to determine how far away it is from a number of known points (source nodes). For the purpose of this thesis, those known points will be referred to as *Anchor*. The target nodes will be called *Tag*.

There are two ways to determine the position of a node in general: direct and two-step. In the first approach, the signal is used for positioning itself. In the two-step approach, positioning is based on parameters extracted from the signal but not the signal itself. Since the direct approach imposes a higher complexity, while the performance stays nearly the same, the two-step approach is most commonly used and therefore more relevant in practice.

3.2 Signal Parameters

Mainly there are four signal parameters that can be used for estimating the distance between two nodes: the Received Signal Strength (RSS), and three time-based schemes, namely Time Of Arrival (TOA), Time Difference Of Arrival (TDOA) and Angle Of Arrival (AOA). All these methods shall be discussed briefly although the thesis exclusively focuses on the TOA method, since this was a company's' decision beforehand, which lead to the choice of the DW1000 microprocessor.

3.3 Received Signal Strength （RSS）

This scheme involves measuring the signal strength of an arriving radio signal at the receiver. RSS is based on the fact that the distance between transmitter and receiver is proportional to the path loss by which the signal is decreased. Formula (6) can be used to estimate the received power at distance d:

$$\bar{P}(d) = P_0 - 10n \log_{10}\left(\frac{d}{d_0}\right),$$

$$(6)$$

where n is the path loss exponent, $\bar{P}(d)$ is the received power at distance d and P_0 is the received power at reference distance d_0.

The received power can also be calculated by the following integration:

$$P(d) = \frac{1}{T} \int_0^T |r(t)|^2 \, dt$$

(7)

The path loss is mainly influenced by two phenomena. The first one is the multi-path phenomenon. This occurs because several components of one signal follow different paths to the receiver. Each component experiences different amounts of path loss. This can be easily overcome by choosing a sufficiently long integration interval in equation (7).

The second phenomenon is shadowing, which occurs because the environment over large distance propagation usually changes. There are methods to take this error into account, which will not be discussed any further as this is not part of the thesis. This scheme is perfectly adequate in certain circumstances, but generally speaking, time-based schemes using UWB can achieve a far more accurate result and involve much simpler mathematics.

3.4 Time Of Arrival（TOA）

All TOA based systems work on the basis of determining the time it takes for a radio signal to propagate from a transmitter to a receiver. In our case, the TOA method can determine the position of a tag by measuring the time of arrival of a signal sent by the tag to an anchor. We assume that the position of the anchor is known. The tag's position must hence lie on a circle of radius $d = c\tau$ around the anchor, where c is the speed of light and τ is the time of arrival.

3.4.1 Time Synchronized Transmitter and Receiver

The synchronization between tag and anchor is critical for the precision of the distance measurement. As long as this criterion can be sufficiently fulfilled, the system can reach a precision in the order of a few centimeters. There are a few methods, besides simply connecting the nodes with a cable, to achieve a good synchronization, all of which are relatively complicated. For this reason, this system is seldom used.

3.4.2 Unsynchronized Transmitter and Receiver

In this case, the tag communicates with the anchor in a so-called *two-way ranging* exchange. Tag and anchor exchange timing information so the anchor can calculate the time-of-flight of the signal from tag to anchor without the necessity for each of them to be synchronized in time. In case of several anchors, the tag has to exchange the timing information with each anchor separately. As soon as all distances to all the anchors are known, a location engine can calculate the real position of the tag.

This process requires the tag to be able to receive as well as send information. Therefore, this method generally consumes more power than the TDOA solution. On the other hand TDOA always needs at least two anchors. This is the reason why the focus of this thesis lies on the TOA scheme, since the key fob (in our case the tag) has the ability to receive and send data.

To implement a full real time location system the distance between the tag and a number of anchors in known locations must be measured. Such a system is depicted in Figure 11. The three anchors A1, A2, and A3 can each locate the Tag T on a circle. Calculating the point of intersection between these three circles gives the tag's position.
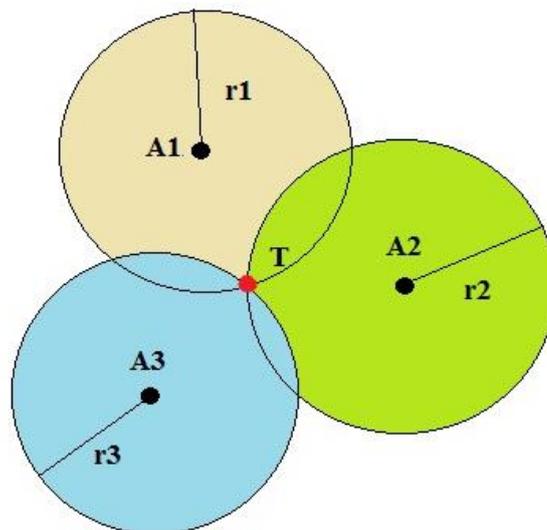
Figure 11 - 2D Positioning Scheme with 3 Anchors and 1 Tag [11]

3.5   Time Difference of Arrival （TDOA）

As the name suggests, TDOA measures the time difference of a signal sent by a tag to at least two anchors. The merit of TDOA in comparison with TOA is that only the anchors have to be synchronized. There is, however, no need for synchronization between the anchors and the tag.

There are two common methods for the estimation of the TDOA. We can simply measure the two TOAs τ_1 and τ_2 of the tag's signal at the two anchors. Consequently, the TDOA we get is:

$$\tau_{TDOA} = \tau_1 - \tau_2$$

（8）

The second approach is to measure the TDOA by using the cross correlation between the two signals. As there must be some amount of offset between the received signals, the cross-correlation will reach a maximum when one of the signals is shifted with the correct offset.

The cross correlation equation is given as

$$\phi_{1,2}(\tau) = \frac{1}{T}\int_0^T r_1(t)r_2(t+\tau)dt$$

（9）

where $r_1(t)$ and $r_2(t)$ are the received signals and T is the observation interval. We estimate TDOA by

$$\hat{\tau}_{TDOA} = \arg\max|\phi_{1,2}(\tau)|$$

（10）

The cross-correlation approach works well for white noise and single path channels but in the case of multi-path channels or colored noise its performance decreases significantly. [3]

32

3.6   Angle Of Arrival（AOA）

If we have an antenna array, we can estimate the angle ψ between the array and the tag. The angle can be calculated by the delay of arrival between the individual antennas. If we use a uniform linear array as shown in Figure 12 and we know the exact distance l between the consecutive antennas, the angle can be calculated by rearranging equation (11).

$$\tau = \frac{l\ sin\psi}{c}$$

(11)

where τ is the delay, ψ is the AOA and c is the speed of light.
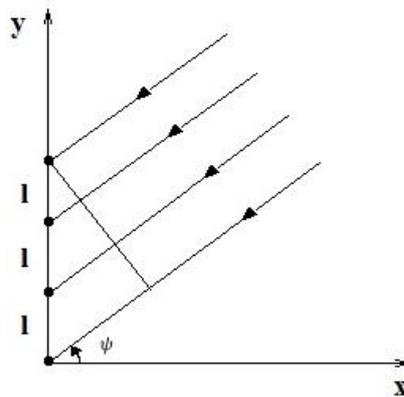
Figure 12 - Uniform, Linear Antenna Array [3]

For all of the last tree methods of estimating the position, increasing the bandwidth has a significant effect on the accuracy. With high bandwidth, we can gain high accuracy even with low SNR, which makes UWB a very good candidate for all those approaches.

33

3.7 Ranging Measurements with UWB Signals

3.7.1 Principle of Two-Way Ranging

Decawave uses the two-way ranging (TWR) scheme to calculate the distance between two objects. Thereby the time of flight (TOF) of signals traveling between two objects is measured. The absolute distance between those two objects can be determined by multiplying the TOF by the speed of light. As already mentioned in the last chapter, synchronization of the clocks is crucial to this type of measurement.

When certain things occur during the transmission and reception of radio wave signals, an UWB IC must have the ability to timestamp those events, by recording the state of the clock.

The basic TWR process can be described as follows. The initiator (usually the Tag) transmits a radio message via UWB and records its time of transmission, which is denoted as $t1$ in Figure 13 below. The responder (Anchor) receives the message and transmits a response message back to the Tag after a particular delay t_{reply}. The reply time can be predetermined either so that it is known by both Tag and Anchor, or it can be estimated by the Anchor and sent to the Tag in the message. Finally, the Tag receives this response and records another timestamp $t2$.
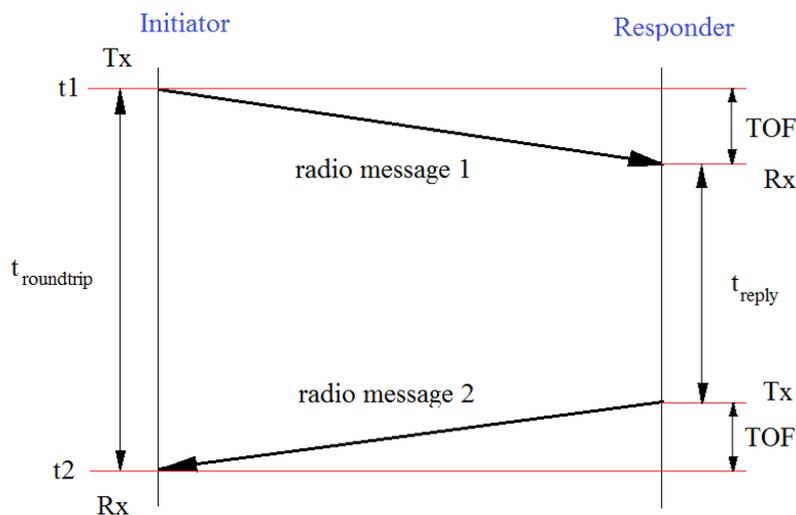
Figure 13 - Two-way ranging concept [12]

Using the two timestamps $t1$ and $t2$ the Tag can now calculate the roundtrip time $t_{roundtrip}$ and knowing the reply time in the Tag, t_{reply}, the TOF can be determined by,

$$TOF = \frac{t_2 - t_1 - t_{reply}}{2}.$$

(12)

As a result, the distance can be calculated by multiplying the result with the speed of light. Therefore, the distance d is given to

$$d = c \cdot \frac{t_2 - t_1 - t_{reply}}{2}$$

(13)

3.7.2 Error Sources of TWR

With this rather simple scheme described above, there are two major sources of error that have to be addressed:

- Errors related to clock drift
- Errors related to frequency drift

The clock drift:
If we consider two devices, each has an UWB IC with a free running oscillator and a microprocessor. We assume that each of the two devices has a fixed frequency error with respect to the nominal oscillator frequency. The frequency error of each device will give rise to a clock drift, which is directly related to the normal frequency.

The frequency drift:
A frequency drift can occur when the frequency error on any device is not stable, but changes over time. This can happen e.g. due to changes in temperature or component aging. For lowest power consumption, battery powered devices usually remain in SLEEP mode with the crystal oscillator turned off for most of the time. For every transaction, the device has to be switched on first. Especially during crystal warm-up there is usually a temperature drift, which can cause a frequency drift in the device.

In order to have a robust solution for the two-way ranging process these errors must either be controlled or eliminated. The dominant error in the ranging scheme depicted in Figure 13 can be calculated according to

$$Error = \frac{1}{2} t_{reply}(e_A - e_B)$$

(14)

where e_A is the frequency error of the initiator and e_B is the frequency error of the responder, which are both assumed constant for now. We can see that there is a strong dependency on t_{reply}.

3.7.3 Symmetric Double-Dided Two-Way Ranging (SDS-TWR)

Even with small frequency offsets, the error in ranging accuracy in a two-way ranging scheme can be very large. If we introduce another message in the ranging transaction, we can minimize the error. The new ranging scheme is called *symmetric double-sided two-way ranging* (SDS-TWR) and is depicted in Figure 14. With SDS-TWR the dominant error is given by

$$Error = \frac{1}{4} \Delta_{reply}(e_A - e_B)$$

(15)

The dependency on t_{reply} has been eliminated and the error is now only dependent on the reply delay Δ_{reply}, which is defined as

$$\Delta_{reply} = t_{resp_A} - t_{resp_B}$$

(16)

In comparison to the error calculated for a standard TWR scheme, one can see that both the primarily responsible time delay as well as the factor in front of it get smaller and as a result, the error in the ranging accuracy also decreases dramatically.

One can also see that in order to minimize the error, the response times t_{resp_A} and t_{resp_B} should be as equal as possible. This is useful to reduce the clock drift as well as the frequency drift. In addition, it is also advisable to make the two response times as short as possible to further reduce the frequency drift error. Last but not least a warm-up time of about 2 ms should be granted to ensure a stable output frequency of the crystal.
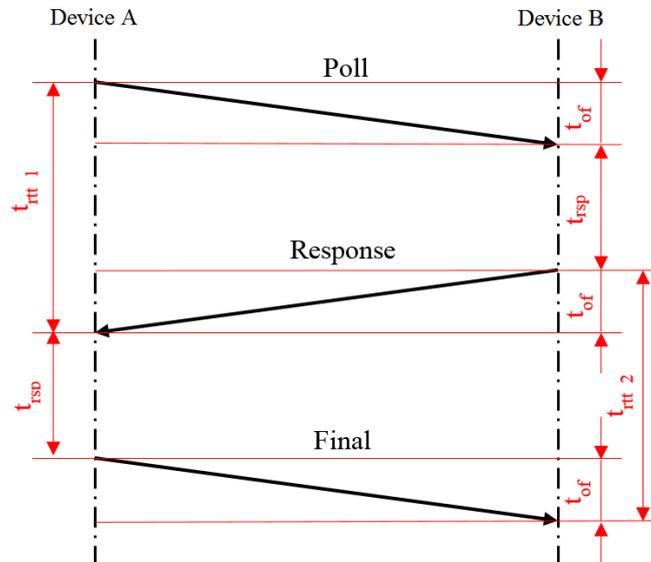
Figure 14 - Symmetric two-way ranging scheme [13]

3.7.4 Implementation of Ranging by Decawave

To understand the original idea of the ranging implementation as well as the optimization process during the development of the prototype, the approach of Decawave should first be explained.[5]

As described previously Decawave's two-way ranging demo also uses two units, one of which acts as Tag and the other as Anchor. In this approach, the Anchor constantly listens for a message from the Tag to initiate the ranging phase. For all further purposes, this initiation message shall be referred to as *Blink Message*.
Figure 15 - Decawave approach for TWR - shows the complete TWR scheme, which is described in detail below.

---

[5] Chapter according to [12]

Discovery Phase

Unpaired Anchor is in listener mode looking for Tags' blink messages

Blink

Unpaired Tag sends periodic blinks, listens for a response and sleeps

Idle

Blink

Idle

Blink

Anchor decides to pair with this tag for ranging and sends the *Ranging Init* message

Ranging Init

Tag sees the *Ranging Init* response to pair with the Anchor

Ranging Phase

Poll

Response

Anchor calculates the range and (optionally) sends a ranging report back to the Tag in the next *Response*

Final

Anchor listens for next *Poll*

Tag idles before sending another *Poll*

Figure 15 - Decawave approach for TWR [12]

The Discovery Phase

Initially, Tag and Anchor are in a discovery phase where the Anchor listens constantly for *Blink Messages.* The Tag itself sends a *Blink Message* periodically, e.g. every second. The *Blink Message* contains basically nothing more than the Tags address. After every *Blink Message,* the Tag listens for a *Ranging Init* response from the Anchor. If the Tag does not get any response, it goes to sleep before blinking again. When an Anchor is in the vicinity of the Tag and receives a *Blink Message*, it will send a *Ranging Init Message* to the Tag, which will complete the *Discovery Phase* and enter the *Ranging Phase.*

The Ranging Phase

As described above the Tag now periodically performs a double-sided two-way ranging. The Tag sends a *Poll Message*, saves the time when the *Poll* was sent ($T_{Poll\,TX}$) in a so-called *timestamp* and listens for a *Response Message*. Should the Anchor not react to the *Poll*, the Tag will get a timeout, return to the *Discovery Phase* and start blinking again.

In general, the Anchor will react to the *Poll* and send a *Response Message*. It immediately safes one timestamp when receiving the *Poll* ($T_{Poll\,RX}$), and another timestamp when sending the *Response Message*

($T_{Response\ TX}$). The difference between these two timestamps yields the time t_{resp_B}, according to Figure 14 where in this case Device A refers to the Tag and Device B refers to the Anchor.

$$t_{resp_B} = T_{Poll\ RX} - T_{Response\ TX}$$

(17)

The *Response Message* must not contain any data, but may contain a previously calculated TOF though, representing the estimated distance between the Tag and the Anchor.
As soon as the Tag receives the *Response Message* it once again saves the time when the message is received ($T_{Response\ RX}$) and calculates the first roundtrip time $t_{rtt\ 1}$ to

$$t_{rtt\ 1} = T_{Response\ RX} - T_{Poll\ TX}$$

(18)

Afterwards the Tag estimates the time when the *Final Message* will be sent ($T_{Final\ TX}$) and pre-calculates the difference between $T_{Response\ RX}$ and the estimated $T_{Final\ TX}$. Referring again to Figure 14, t_{resp_A} is calculated as the difference between those two times.

$$t_{resp_A} = T_{Final\ TX} - T_{Response\ RX}$$

(19)

Finally, the Tag sends the *Final Message*, containing both the pre-calculated time t_{resp_A} as well as the roundtrip time $r_{rtt\ 1}$. After transmitting the *Final Message,* the Tag goes to sleep and sends another Poll message as soon as it wakes up.

Once the Anchor has received the *Final Message*, the device has all the data to calculate the TOF while minimizing the error caused by the clock drift.

3.7.5 Calculating the time of flight with SDS−TWR

Figure 16 shows a Poll-Response-Final method of doing TWR. According to [14] the TOF[6] can be calculated with

$$TOF = \frac{T_{round1} \cdot T_{round2} - T_{reply1} \cdot T_{reply2}}{T_{round1} + T_{round2} + T_{reply1} + T_{reply2}}$$

$$(20)$$
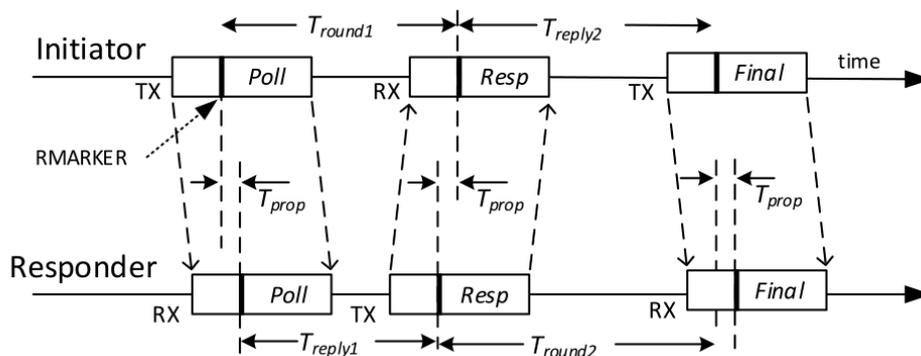
Figure 16 - TWR method using a Poll-Response-Final scheme

---

[6] The TOF is referred as propagation time T_{prop} in Figure 16

4   The DW1000 Ultra–Wideband IC by Decawave

As mentioned before, at the beginning of this thesis, NXP had already made a few specifications concerning the project. An UWB IC to work with, namely the DW1000 by Decawave, has already been picked beforehand. This chapter focuses on the peculiarities of the DW1000 IC, concerning its basic architecture and a few important functions.

4.1   Description of the DW1000

The DW1000 is a fully integrated single chip Ultra-Wideband transceiver IC compliant to IEEE802.15.4-2011. It consists of an analog front end containing a receiver, a transmitter and a digital back end that interfaces to a host controller via SPI. In addition, temperature and voltage monitors are provided on-chip.

The receiver consists of an RF front end, which amplifies the received signal before down-converting it directly to a baseband signal, which is then demodulated. The resulting received data is made available to the host controller via SPI.

The transmit pulse train is generated by applying digitally encoded transmit data to the analog pulse generator. The pulse train is up-converted by a double mixer to a carrier generated by the synthesizer and centered on one of the UWB-channels. The modulated RF waveform is amplified before transmission from the external antenna.

The IC has an on-chip One-Time Programmable (OTP) memory. This memory can be used to store calibration data such as TX power level, crystal initial frequency error adjustment, and range accuracy adjustment. An Always-On (AON) memory can be configured to retain DW1000 configuration data during the lowest power operational states.

The DW1000 clocking scheme is based around three main circuits. Firstly, there is a *Crystal Oscillator*, which is operated at a frequency of 38.4 MHz using an external crystal. This clock is used as the reference clock input to two on-chip PLLs, the *clock PLL (CLKPLL)* and the *RF PLL*. The CLKPLL generates the clock required by the digital back-end for signal processing. The RF PLL generates the down-conversion local oscillator (LO) for the receiver chain and the up-conversion LO for the transmit chain. In addition, an internal 13 kHz oscillator is provided for use in the SLEEP state.

Figure 17 shows a block diagram of the DW1000 IC including all the available pins and its functions. [15]
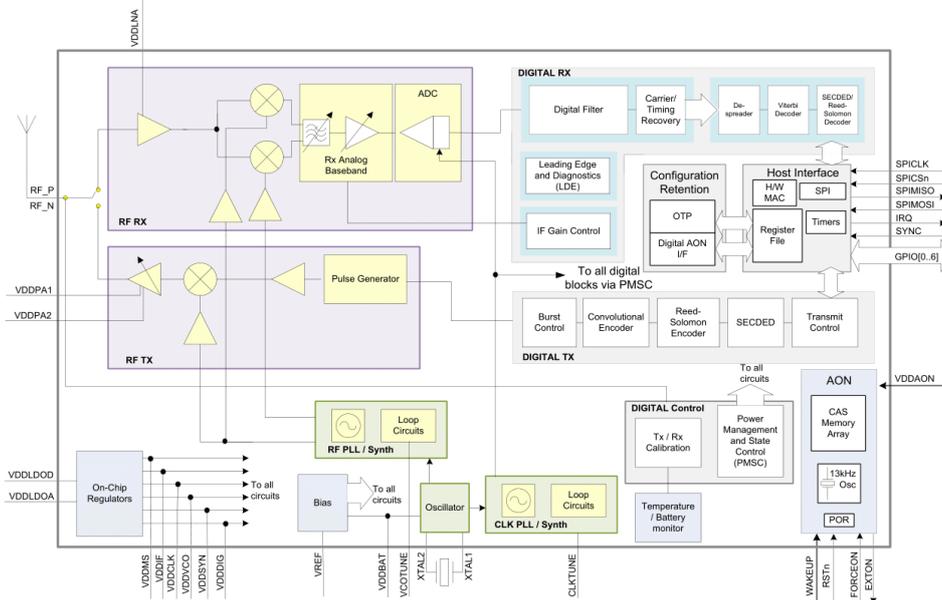
Figure 17 - DW1000 IC Block Diagram

Providing all the described functions, the DW1000 IC can be used in 2-way ranging or can do TDOA measurements to locate asserts to a precision of 10 cm. It supports 6 RF bands from 3.5 GHz to 6.5 GHz with a programmable transmitter output power. The DW1000 provides two low power consumption modes, referred to as SLEEP and DEEP SLEEP mode, with a current consumption of 2 µA or 100 nA respectively. The possible supply voltages are between 2.8 V and 3.6 V. In TX- and RX-mode, the data rate is adjustable and can be set to 110 kbps, 850 kbps or 6.8 Mbps. The maximum packet length is 1023 bytes.

4.2 Power Consumption

As will be seen in chapter 5, the power consumption of the DW1000 in different states[7] is strongly dependent on the used data rate and the preamble length. To get accurate values of the current consumption in different states when using different data rates, etc., we could not trust

---

[7] i.e. RX-, TX-, SLEPP-, DEEP SLEEP- and IDLE-state

the DC characteristics of the datasheet depicted in Figure 18. Chapter 5 therefore covers some prior measurements to get the 'real' values for which the power supply is designed.

Parameter	Min.	Typ.	Max.	Units	Condition/Note
Supply current DEEP SLEEP mode		50		nA	Total current drawn from all 3.3 V and 1.8 V supplies.
Supply current SLEEP mode		1		µA	
Supply current IDLE mode		18		mA	
Supply current INIT mode		4		mA	
TX : 3.3 V supplies (VDDBAT, VDDPA1, VDDPA2, VDDLNA, VDDAON, VDDIOA)			70	mA	Channel 5 TX Power = MAX mean (-9.3 dBm/500 MHz)
TX : 1.8 V supplies (VDDLDOA, VDDLDOD)			90*	mA	
RX : 3.3 V supplies (VDDBAT, VDDPA1, VDDPA2, VDDLNA, VDDAON, VDDIOA)			30	mA	Channel 5
RX : 1.8 V supplies (VDDLDOA, VDDLDOD)			210*	mA	
Digital input voltage high	0.7*VDDIO			V	
Digital input voltage low			0.3*VDDIO	V	
Digital output voltage high	0.7*VDDIO			V	Assumes 500 Ω load.
Digital output voltage low			0.3*VDDIO	V	Assumes 500 Ω load.
Digital Output Drive Current GPIOx, IRQ SPIMISO EXTON	4 8 3	6 10 4		mA	

* These currents are on the 1.8 V supplies, not referenced back to the 3.3 V supply

Figure 18 - DW1000 DC Characteristics

4.3   Additional Notes

4.3.1   Power Up

When power is applied to the DW1000, RSTn is driven low as part of its power up sequence. The port remains low until the XTAL oscillator has powered up and its output is stable. As soon as the supply voltage exceeds the threshold V_{ON} of 2 V, the EXTON signal goes high for the time T_{EXT_ON} before RSTn is released. The oscillator takes about 1.5 ms to start up (T_{OSC_ON}) and the whole power up process lasts for about 2 ms (T_{DIG_ON}). It is important to remember that this time has to be given to the DW1000 after every start up.
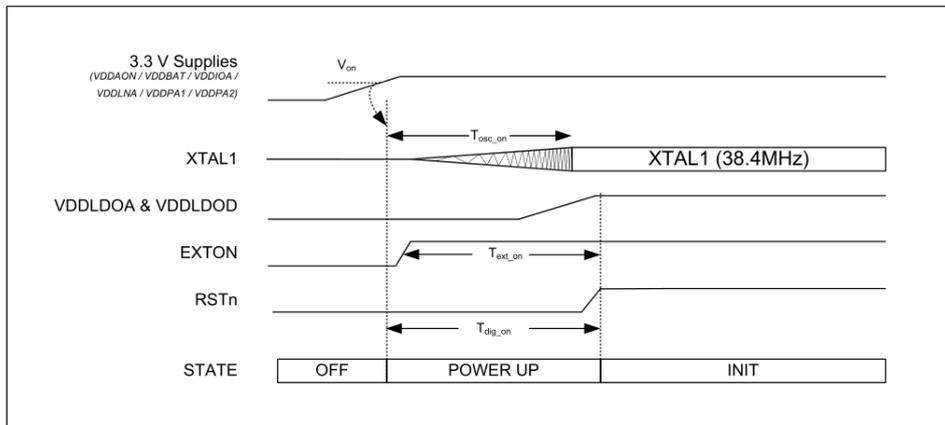
Figure 19 - DW1000 Power-Up Sequence

4.3.2   SPI Interface

The SPI interface can be configured using GPIO5 and 6, if necessary. An easier way is to configure the SPI settings of the host controller to the default settings of the DW1000. In the default mode, the data is sampled on the rising (first) edge of the clock and launched on the falling (second) edge.

4.3.3 General Purpose Input Output （GPIO）

The DW1000 provides 8 user-configurable I/O pins. The default setting on reset is input. GPIO0, 1, 2, & 3, as one of their optional functions, can drive LEDs to indicate the status of various chip operations.

4.3.4 Memory

The DW1000 includes a number of user accessible memories. Most importantly, there are receive and transmit data buffers. The TX buffer (1024 x 8 bits) contains data written by the host processor to be transmitted via the transmitter. The RX buffer (1024 x 8 x 2 bits) contains received data and can be read by the host processor via SPI. The RX buffer also supports double buffering so that the receiver can receive a second packet while the host controller is reading the first.

An accumulator memory (1016 x 32 bits) is used to store channel impulse response estimates data to be optionally read by the host controller.

Last but not least, the DW1000 also has a small OTP memory (56 x 32 bits) used for storing calibration data.

4.4 The Development Platform

I initially started experimenting with the EVK1000 demo kit by Decawave. This was a good starting point to get a basic understanding of the two-way ranging process, and was used as a development platform to develop the software for the final product. In addition, the boards were useful to measure the current consumption of the DW1000 in different states, which is why the basic functions of the EVK1000 board should be described concisely.

4.4.1 EVK1000 Operational Modes

The kit consists of a pair of EVB1000 boards, each configured to run a pre-programmed two-way ranging demonstration application. An onboard ARM processor[8] controls the DW1000 IC to exchange messages, calculate the time-of-flight, estimate the resultant distance between the two boards and display the result on the on-board display.
The boards can be powered by an external supply as well as via USB. Also, the EVK1000 kit contains a piece of software using the USB interface of the EVB1000 to connect to a PC. With this application, the onboard ARM can be bypassed and the DW1000 can be controlled directly from the PC.

Figure 20 shows the front- and backside of the EVB1000 board and specifies some of the essential components.

---

[8] *STM32 F105 RCT6 microcontroller*
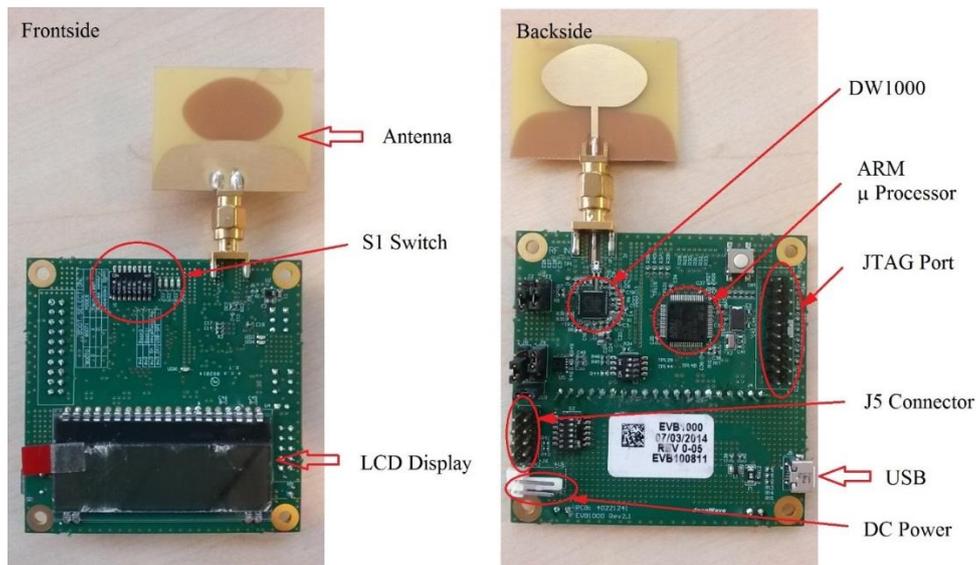
Figure 20 - Front- and Backside of the EVB1000

Some major functions of the EVB1000 boards can be controlled with the S1 switch. It controls many different pre-settings like whether the board is a Tag or an Anchor, if the DW1000 is connected to the ARM processor or to a PC over the USB port, and – most importantly – which operational mode is selected for UWB communication. These modes can be chosen to explore the DW1000's performance in e.g. high-speed short range and low speed long-range applications. A list of the possible operational modes can be found in Table 3.

A few of these modes be should used to determine the current consumption of the DW1000. The third mode is recommended by Decawave and therefore highlighted. It guarantees a high range with the drawback of a slow data rate, which has a negative impact on the power consumption. It is a good way of testing the application though, which is why the final car key should be able to use this mode eventually.

S15	S16	S17	Mode	Cha	Data Rate	PRF	Pream.	Pream. Code	Non stand. SFD
OFF	OFF	OFF	1	2	110 kbps	16	1024	3	Yes
ON	OFF	OFF	2	2	6.8 Mbps	16	128	3	No
OFF	ON	OFF	3	2	110 kbps	64	1024	9	Yes
ON	ON	OFF	4	2	6.8 Mbps	64	128	9	No
OFF	OFF	ON	5	5	110 kbps	16	1024	3	Yes
ON	OFF	ON	6	5	6.8 Mbps	16	128	3	No
OFF	ON	ON	7	5	110 kbps	64	1024	9	Yes
ON	ON	ON	8	5	6.8 Mbps	64	128	9	No

Table 3 - Operational Modes Configuration Details

The first task in order to design a power supply for the yet to be built UWB demo board is to measure the exact current consumption of the DW1000 in different modes. This can be done easily with the EVB1000 board as it features a jumper to measure the current over the DW1000 without corrupting the measurement by the additional current-flow over the ARM, Display and LEDs, etc. The basic measurements and consequential calculations for the design of the power supply shall be explained in the next chapter.

4.4.2 Chip features of the STM32 controller

The host controller of the DW1000 in the EVB1000 board is an *STM32 F105 RCT6 IC* with a 32-bit Cortex–M3 CPU, with 256 kB program memory and 64 kB general-purpose SRAM. It has an internal 8 MHz RC and a separate 32 kHz oscillator for RTC. There are 51 I/Os available and it supports many different interfaces, like I2C, USART, SPI, CAN, USB 2.0 and Ethernet.

To put it in a nutshell, the STM32F105 is a monstrosity compared to the Token IC[9], which is the host processor for the DW1000 on the final prototype. Therefore, the software, written by Decawave, cannot be used for the final implementation[10], since the final software must be simpler.

Nevertheless, the STM32F105 is a good choice to be able to explore all the features of the DW1000 and to test its maximal speed concerning e.g. SPI transmission. Of course, it needs a lot more power and would therefore not be suitable for our purposes.

---

[9] See chapter 7.1 for more information on the Token IC.
[10] The Token IC cannot even recognize *int64* or *double* data types.

5 Calculations for the Power Supply

The main technical specification of the UWB system used in the key fob, which is required by the customer, is to be able to do a ranging report over a distance of at least 12 meters. In general only one successful ranging has to be conducted to ensure that the key fob is really in the vicinity of the car.

Since the ranging measurement via UWB consumes quite a lot of energy[11], care has to be taken that the system operates most efficiently. To do so, the time the DW1000 spends in RX- or TX-mode has to be minimized. However, even if the times are kept short, the temporary current consumption during the RX- and TX phase is excessively high for a single coin cell.

To meet the requirement of a single CR2032 coin cell battery powering the whole prototype, a capacitor has to provide the energy for the peak currents. A so-called supercapacitor was chosen to account for the peak currents. The big advantage of choosing a supercapacitor over a standard electrolytic or ceramic capacitor is that it can store 10 to 100 times more energy per unit volume or mass than conventional capacitors, which makes it suitable for the small casing of a car key. In addition to this, the average supercapacitor has a vanishing low leakage current compared to the conventional ones.

5.1 Measurement of Power Consumption in *Fast Ranging* mode

To ensure a short response time, the software has been optimized to operate as fast as possible, while guaranteeing a safe transmission of the data. This is achieved mainly by choosing a short preamble and a large data rate to speed up the transmission, as well as a large pulse repetition frequency to enhance the distance with reasonable energy cost. The latter three settings result in a higher current consumption, as can be seen in Table 4, which can be accepted as the savings in time and therefore the savings in energy far outweigh those losses.

The optimized mode will further be referred to as *Fast Ranging* mode. Opposed to the optimized mode, a *Long Ranging* mode will be discussed for comparison and a 'healthy' mixture of both, referenced as *Typical* mode, which can cover the need of ranging over long distances in reasonable time.

---

[11] Up to about 145 mA during RX.

TX Power Consumption Measurements in Different Modes						
	Channel	Prmbl Code	PRF	Data Rate	Prmbl Length	DC Power [mA]
* "Fast Ranging" mode	2	9	64 MHz	6,8 Mbps	128	76,7
** typical mode	2	9	64 MHz	110 kbps	1024	56,3
*** "Long Ranging" mode	2	9	64 MHz	850 kbps	128	57

Table 4 - Current Consumption in Different Modes

Let us first discuss the *Fast Ranging* mode, as it is ideal for our purposes. Table 5 shows the measured current consumption in the different states for a single ranging measurement of the DW1000. Also, the time and the total charge that is needed in the different states are listed.

Capacity Calculation (*Fast Ranging* Mode)				
mode	state	time [μs]	current [mA]	total charge [mAs]
POLL	TX (Poll)	237	76,7	1,82E-02
	IDLE	52	14,26	7,42E-04
	RX	481	145	6,97E-02
	IDLE	43	14,26	6,13E-04
FINAL	TX (Final)	824	76,7	6,32E-02
TOTALS		1.637,00		1,52E-01

Table 5 - Current Consumption During a Single Distance Measurement in *Fast Ranging* Mode

5.2 Properties of a Typical CR2032 Coin Cell

To get a good estimate of the minimal battery voltage at the battery's end of life, some properties of a typical coin cell should be taken into account. To do so, a few different CR2032 coin cells were compared first and a worst-case scenario using a standard brand coin cell was considered.

In the worst case, we must expect a minimum average voltage of the battery, when operating a circuit that needs high peak currents. To estimate those values, one has to analyze some datasheets of coin cells.

In Figure 21 the difference of the average output voltage of a CR2032 coin cell by the brand Energizer can be seen when operating it with a continuous drain in comparison to a pulse drain. [16]
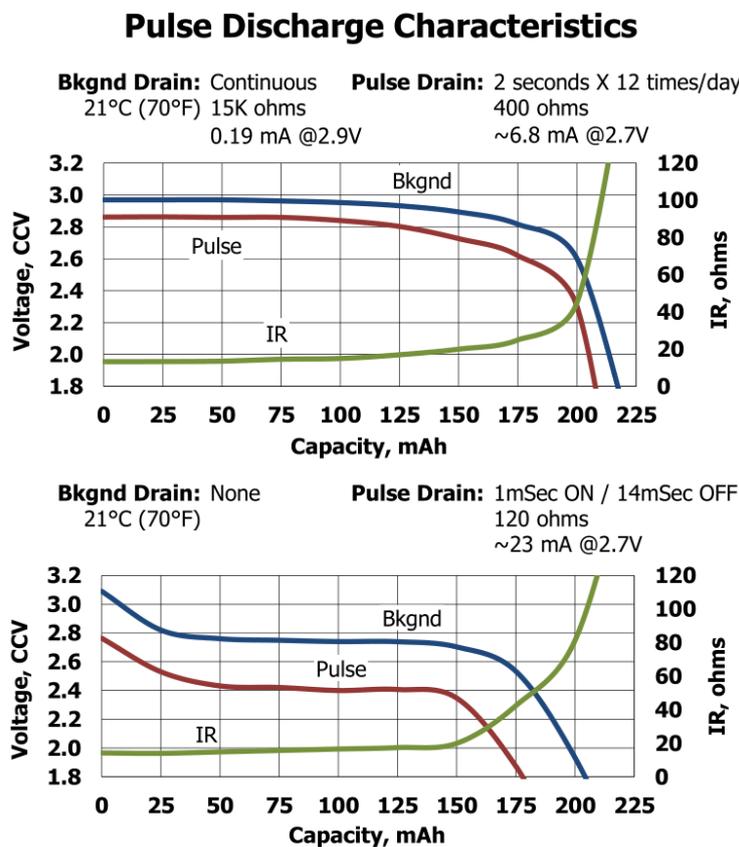
Figure 21 - Pulse Discharge Characteristics of a Lithium CR2032 Coin Cell by Energizer [16]

As can be seen, for a 2 second discharge with 6.8 mA 12 times a day, the maximum voltage of the battery is about 2.85 V. For a 1 ms discharge with 23 mA every 15 ms the average voltage drops dramatically.

For the purpose of this power supply, according to [17], a maximum discharge current of 15 mA should be chosen to be easy on the battery. This should hold up for the estimation of the maximum current, disregarding the actual time to reload the capacitor. Besides, it increases the capacity of the battery by about 10 % [17]. Also, the estimation for U_{Bat} of 2.7 V as an average voltage seems to be a good value for most of the battery's life.

Nevertheless, we want to calculate for the worst case. Therefore, we take a value for $U_{Bat,min}$ at the battery's end of life, which is in nearly every datasheet of C2032 coin cells denoted with 2 V. The voltage of the battery of course is heavily dependent on the temperature, as can be seen in Figure 22 and Figure 23, which shows different temperature performances of button cells by Renata [18] and VARTA [19].
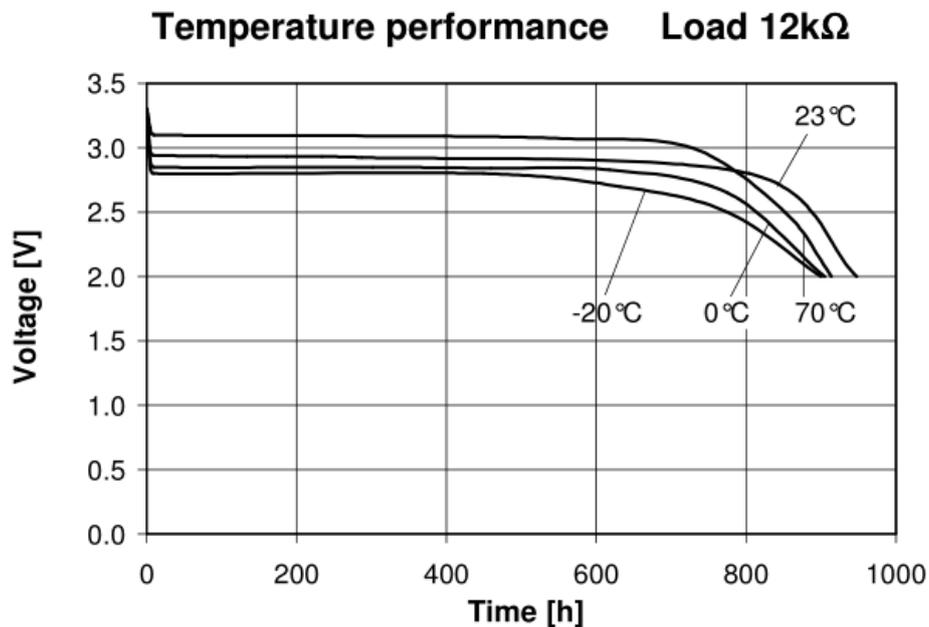
Figure 22 - Temperature Performance of a CR2032 MFR Lithium Coin Cell by Renata Batteries [18]
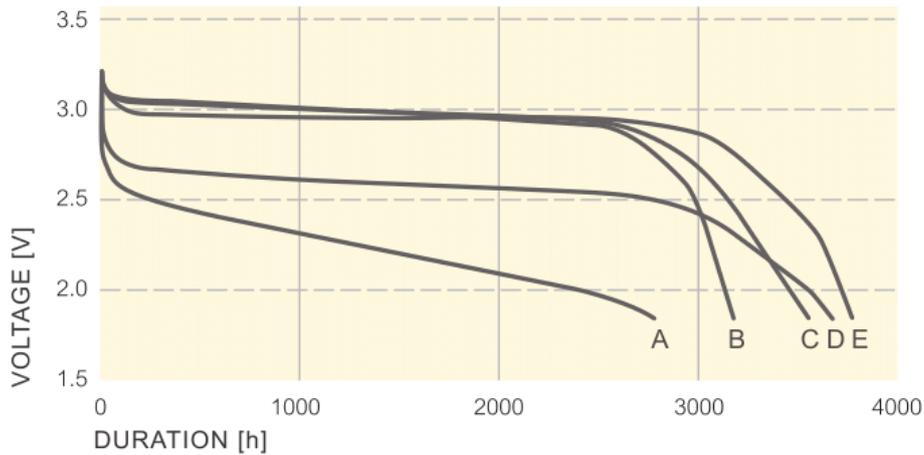
A = -40°C; B = +80°C; C = +60°C; D = -20°C; E = +23°C

Figure 23 - Temperature Performance of a Li/MnO2 Button Cell by VARTA [19]

5.3 Dimensioning of the Capacitor

When dimensioning the supercapacitor, a few a priori assumptions were made beforehand. The original requirement was to power the whole prototype with a single coin cell. Another calculation was also made to see if an additional coin cell would bring an indispensable advantage for the power supply, in which case this solution would be open to debate.

The final prototype only needs to do ranging measurements wihtin a radius of 12 meters around the car. For this purpose, the *Fast Ranging* mode is ideal as it provides low power consumption and should be able to perform trouble-free over this distance. Nevertheless, calculations were made for the worst case of *Long Ranging* to be absolutely on the safe side in case a measurement over long distance should be necessary someday.

To simplify the dimensioning of the capacitor, a few simplifications are made according to [17].

During the high current states the battery voltage is fixed at $U_{Bat,min}$, which is the minimal battery voltage allowed and is estimated with 2 V for all further purposes. This will cause an error on the safe side, meaning that the battery will deliver slightly more energy than calculated.

53

The current consumed by the circuit when no ranging measurement is being performed is normally in the 10 μA range and is therefore omitted. The focus of the calculation lies on the high load states.

To calculate the needed capacity we look at the total energy consumed by the DW1000, denoted as E_{DW1000}, which must equal the energy needed by the DC-to-DC converter, denoted as E_C. Also, we allow for a worst-case efficiency η_{worst} of the converter, which is given by the respective datasheet.

$$E_C \cdot \eta_{worst} = E_{DW1000}$$

(21)

$$\frac{C \cdot \Delta U^2}{2} \cdot \eta_{worst} = U_{DW} \cdot \Delta Q$$

(22)

$$\Delta Q = Q_{dis} - Q_{relode}$$

(23)

Q_{dis} is the total charge consumed during one ranging process and is calculated as

$$Q_{dis} = \sum I_n \cdot t_n$$

(24)

as can be seen in the last row of Table 5.

Q_{relode} is the minimal charge supplied by the battery during discharge of the capacitor and is calculated as

$$Q_{relode} = \frac{U_{Bat,min}}{R_i} \cdot t_{tot}$$

(25)

where R_i is the maximum internal resistance the circuit is able to manage and is estimated with 1 $k\Omega$ for all further purposes, which is also a worst-case value for the average resistance of the actual circuit. t_{tot} is the total time for one complete measurement.

U_{DW} is the average voltage needed to supply the DW1000 and

$$\Delta U^2 = U_{\max}^2 - U_{\min}^2$$

(26)

is the maximal allowed potential drop in the capacitor, where $U_{\max}$ is the voltage over the capacitor at the start of the discharge pulse at the battery's end of life, and must be initially estimated. $U_{\min}$ is the minimal voltage the DC-to-DC converter is able to handle.

The needed capacity can now be calculated as

$$\rightarrow \frac{C \cdot \Delta U^2}{2} \cdot \eta_{worst} = U_{DW} \cdot \left(\sum I_n \cdot t_n - \frac{U_{Bat,min}}{R_i} \cdot t_{tot} \right)$$

(27)

$$\rightarrow C = \frac{2 \cdot U_{DW} \cdot \left(\Sigma I_n \cdot t_n - \frac{U_{Bat,min}}{R_i} \cdot t_{tot} \right)}{\eta_{worst} \cdot (U_{\max}^2 - U_{\min}^2)}$$

(28)

Finally, yet importantly, care should be taken that the capacitor will be able to provide enough energy for a second ranging if the first one fails or if it is necessary for any other reason. The needed charging time should be calculated for a minimum voltage at the battery's end of life. It can be derived by rearranging equation (29).

$$u(t) = U_0 \cdot \left(1 - e^{-\frac{t}{\tau}} \right)$$

(29)

$$U_0 = U_{max} - U_{min}$$

(30)

$$u(t) = 0.993 \cdot U_0$$

(31)

$u(t)$ is the time until the capacitor is loaded to 99.3 % of the original value or $t = 5\tau$.

Let us assume that the battery is at its end of life and the capacitor's nominal voltage to drive the converter is $U_{max} = 1.8\,V$. The voltage of the capacitor must not drop below U_{min}, which – as described above - is the lowest operating voltage of the DC-to-DC converter.

Aside from any additional resistance we put into the circuit to affect the time constant τ, the main resistance that is affecting τ, is not the inner resistance of the circuit, but the inner resistance of the coin cell $R_{i,Bat}$ as the input resistance of the converter is very high at the time the capacitor

is reloading. According to the datasheet of a standard coin cell by the brand Energizer, the inner resistance of the battery can be estimated with 40 Ω at its end of life [16].

We now apply these values in the upper equation and get

$$0.993 \cdot U_0 = U_0 \cdot \left(1 - e^{-\frac{t}{\tau}}\right)$$

(32)

$$\rightarrow -\frac{t}{\tau} = \ln(1 - 0.993)$$

(33)

$$\rightarrow t = -R_{i,Bat} \cdot C \cdot \ln(0.007)$$

(34)

5.3.1 Calculations for a Single Coin Cell

First, we look at the common area of application, where the capacity should be dimensioned for driving the power supply with a single coin cell.

To get the necessary supply voltage for the DW1000 of 2.8 V – 3.6 V, a boost converter is placed right after the capacitor. The APD1607[12] by Analog Devices [20] was chosen as a boost converter to amplify the voltage of the single coin cell (U_{max}), which is 1.8 V in the worst case at the battery's end of life. The converter can handle very low input voltages (U_{min}) down to 1.2 V with a very high efficiency $\eta_{worst} = 85$ % and drive an output current of 200 mA at 3.3 V output voltage.

The value for Q_{dis} can be looked up in Table 5. All other values are chosen as described above. The capacity finally calculates to

$$C = \frac{2 \cdot U_{DW} \cdot \left(\sum I_n \cdot t_n - \frac{U_{Bat,min}}{R_i} \cdot t_{tot}\right)}{\eta_{worst} \cdot (U_{\max}^2 - U_{\min}^2)}$$

(35)

---

[12] Refer to chapter 7.2.1 for additional information on the ADP1607.

$$C = \frac{2 \cdot 3.3\,V \cdot \left(0.152\,mAs - \frac{2\,V}{1000\,\Omega} \cdot 1.637\,ms\right)}{0.85 \cdot ((1.8\,V)^2 - (1.2\,V)^2)} = 642\,\mu F$$

(36)

Keep in mind that

$$Q_{relode} = \frac{U_{Bat,min}}{R_i} \cdot t_{tot}$$

(37)

usually is much bigger than the calculated value in this example[13] with peak values of 24.5 µAs since the maximal allowed battery current is as high as 15 mA.

5.3.2 Reload Time (for Single Coin Cell)

It should be verified that the capacitor will be able to recharge during sleep state, so the minimal sleep time needs to be calculated as follows.

$$t = -R_{i,Bat} \cdot C \cdot \ln(0.007)$$

(38)

$$t = -40\,\Omega \cdot 642\,\mu F \cdot \ln(0.007) = 127.42\,ms$$

(39)

To stay on the safe side and account for the sleep current and the leakage of the capacitor a slightly lager capacity of 680 µF should be chosen, which results in a slightly larger recharge time of 134.96 ms.

Problems with a Single Coin Cell
The major problem that comes with a single-cell power supply is the power loss due to leakage of the used components. Boost converters tend to have a high quiescent current. Although this can be controlled by disabling the converter when the DW1000 is not active, it can result in a considerable expenditure of the needed control circuit and port pins of the host controller.

Also, the leakage of the capacitor has to be considered, which in general gets higher the bigger the needed capacity is. To minimize the leakage a

---

[13] Only about 1.27 µAs.

super capacitor can be chosen, which will be discussed in detail in chapters 5.3.5 and 7.2.2.

5.3.3 Calculation for Two Coin Cells

As shown before, the same calculations are now made for a key fob, which is driven by two CR2032 coin cells and a buck converter.

According to the previous calculation, the voltage of a single coin cell at the end of its life is assumed to be 2 V. The buck converter - for this example a TPS62040 by Texas Instruments [21] -can safely operate at a minimum voltage of $U_{min} = 3.3\ V$. The minimal voltage of the capacitor U_{max} should be 3.8 V.

We can see that the capacity gets smaller but the reload time stays the same because of the additional inner resistance of the second battery.

$$C = \frac{2 \cdot 3.3\ V \cdot \left(0.152\ mAs - \frac{4\ V}{1000\ \Omega} \cdot 1.637\ ms\right)}{0.85 \cdot ((3.8\ V)^2 - (3.3\ V)^2)} = 318\ \mu F$$

$$(40)$$

$$t = -80\ \Omega \cdot 318\ \mu F \cdot \ln(0.007) = 126.23\ ms$$

$$(41)$$

As it was done before, a slightly larger capacitor of 390 μF should be chosen. Doing so the time for recharging changes to 154.81 ms, which is even slightly more time than with one coin cell.

All in all a second battery has no noteworthy advantage compared to a single-cell solution. Sure the capacity can be smaller, but as we will see in the next chapter, for the worst case of *Long Ranging* an even bigger capacitor has to be chosen anyway.

5.3.4 Calculations for *Long Ranging* Mode with a Single Coin Cell

For the worst-case calculation, we want to restrain the data rate in case the ranging distance for the *Fast Ranging* mode is too short for later purposes.

The data rate for *Fast Ranging* is 6.8 Mbps. If we choose another mode with a lower data rate (e.g. 850 kbps), but the same preamble code,

preamble length and pulse repetition frequency (PRF), we get a slightly lower power consumption.

Table 6 shows an example of the settings and power consumption in TX state for different modes. *Fast Ranging* is colored green, *Typical* mode is colored red and the chosen mode for our purposes is highlighted in orange.

TX power consumption for different modes (suggested by user manual)					
Channel	Prmbl Code	PRF	Data Rate	Prmbl Length	DC Power [mA]
2	9	16 MHz	110 kbps	128	46,7
2	9	16 MHz	110 kbps	1024	48,8
2	9	64 MHz	110 kbps	128	52,2
2	9	64 MHz	110 kbps	1024	56,3
2	9	16 MHz	850 kbps	128	49,9
2	9	16 MHz	850 kbps	1024	57,8
2	9	64 MHz	850 kbps	128	57
2	9	64 MHz	850 kbps	1024	72,8
2	9	16 MHz	6,8 Mbps	128	64,3
2	9	16 MHz	6,8 Mbps	1024	68,8
2	9	64 MHz	6,8 Mbps	128	76,7
2	9	64 MHz	6,8 Mbps	1024	92

Table 6 - TX Power Consumption in Different Modes

For further calculations, the average TX current shall be 52.2 mA. For the estimation of the TX time we simply assume that it takes us eight times as long as in *Fast Ranging* mode (824 µs -> refer to Table 5) to transmit the *Final Message*.

For the *Final Message* the time calculates to

$$\frac{0.824 \, ms \cdot 6.8 \, Mbps}{0.85 \, Mbps} = 6.592 \, ms$$

(42)

Furthermore, we take into account the time the DW1000 takes to power up. It takes 1.5 ms in INIT mode after a wake up until the oscillator frequency is locked and even as long as 3 ms starting from power off

state.[14] For this time, the IDLE current is the worst case current, therefore 14.3 mA shall be assumed.

The new estimate for the power consumption in *Long Ranging* mode can be seen in Table 7.

Average Power Consumption worst case for *Long Ranging* mode				
mode	state	time [ms]	current [mA]	total charge [mAs]
WAKE UP	IDLE	3,00	14,30	4,29E-02
POLL	TX (Poll)	1,90	57,00	1,08E-01
	IDLE	0,07	14,30	1,03E-03
	RX	3,85	145,00	5,58E-01
	IDLE	0,07	14,30	1,03E-03
FINAL	TX (Final)	6,59	57,00	3,76E-01
TOTALS		15,48		1,04E+00

Table 7 – Worst-Case Power Consumption in *Long Ranging* Mode

We assume that a single coin cell battery and the previous boost converter by Analog Devices [20] are used for the power supply. The calculation should prove that it is possible to run the DW1000 in *Long Ranging* mode with only one coin cell. The calculation shall be carried out as before.

$$C = \frac{2 \cdot 3.3\,V \cdot \left(1.04\,mAs - \frac{2\,V}{1000\,\Omega} \cdot 15.48\,ms\right)}{0.85 \cdot ((1.8\,V)^2 - (1.2\,V)^2)} = 4.57\,mF$$

(43)

$$t = -40\Omega \cdot 4.57\,mF \cdot \ln(0.007) = 907.03\,ms$$

(44)

It now takes nearly a second to reload the capacitor. Still we can do a ranging every second in theory, but practically the voltage is likely to drop with every consecutive ranging attempt, which means that we can only do a finite number of ranging reports.

---

[14] Refer to chapter 4.3.1.

According to the previous calculations, we choose a slightly bigger capacitor[15], which is 4.7 mF, to be on the safe side. With a reload time of 932.83 ms, this will probably affect the maximal number of consecutive reports that are possible, so we have to calculate this number to get a better estimate.

Calculation of the Maximal Number of Ranging Reports

For the worst case of *Long* Ranging, we can calculate how many times the DW1000 can make a ranging report consecutively until the capacitor can't provide enough energy to operate the boost converter anymore.

U_{DW} is again the average input voltage of the DW1000. It allows for a range between 2.8 V and 3.6 V, so we assume it to be 3.3 V. E_{DW1000} is the total energy the DW1000 needs for one complete ranging report.
E_C is the energy stored in the capacitor.

First, we calculate for the given worst case of *Long Ranging*. The capacitor should be slightly larger than calculated. We choose the next value in the E12 series, which is 4.7 mF.

$$E_{DW1000} = U_{DW} \cdot \left(\sum I_n \cdot t_n - \frac{U_{Bat,min}}{R_i} \cdot t_{tot} \right)$$

(45)

$$E_{DW1000} = 3.3\ V \cdot \left(1.09\ mAs - \frac{2\ V}{1000\ \Omega} \cdot 15.48\ ms \right) = 3.46\ mWs$$

(46)

$$E_C = \frac{C \cdot (U_{max}^2 - U_{min}^2)}{2}$$

(47)

$$E_C = \frac{4.7\ mF \cdot ((1.8\ V)^2 - (1.2\ V)^2)}{2} = 4.23\ mWs$$

(48)

With an efficiency of $\eta_{worst} = 85\ \%$[16] we get the number of possible consecutive ranging reports.

---

[15] According to the E12 series.
[16] According to [20].

$$n = \frac{E_C}{E_{DW}} \cdot \eta_{worst} = \frac{4.23 \; mWs}{3.46 \; mWs} \cdot 0.85 = 1.22$$

<div align="right">(49)</div>

We can only make one 'consecutive' measurement. Since we have to wait at least one second to reload the capacitor, we cannot tolerate this result. We have to increase the capacity to be able to make more ranging attempts if necessary.

A short look at a datasheet for supercapacitors [22] shows us that there is no considerable difference in size of the casing for a 10 mF capacitor compared to one with 140 mF. If we therefore boldly assume that we can fit a 140 mF capacitor into the fob, we will see that this is more than enough even for *Long Ranging* mode. According to the previous calculations, we get a new value for E_C.

$$E_C = \frac{140mF \cdot ((1.8V)^2 - (1.2V)^2)}{2} = 126mWs$$

<div align="right">(50)</div>

We account again for an efficiency of $\eta_{worst} = 85\,\%$ and get a new number of possible consecutive ranging reports.

$$n = \frac{E_C}{E_{DW}} \cdot \eta_{worst} = \frac{126 \; mWs}{3.43 \; mWs} \cdot 0.85 = 31.22$$

<div align="right">(51)</div>

This means we can send a complete ranging report up to 31 times in *Long Ranging* mode until the 140 mF capacitor cannot provide the voltage for the boost converter anymore, which should be enough if we remember that these are all worst-case calculations at the battery's end of life. Also, if we take into account that we only need to make one measurement per second, we probably can make a lot more ranging attempts as long as the battery provides enough energy. According to the simulation in the next chapter, we can actually make many more than 30 attempts.

The chosen supercapacitor provides 140 mF with a leakage current of only 5 µA and is, with a size of 5.3mm x 8.2mm x 5.8mm[17], small enough

---

[17] According to the data sheet of the AVX BestCap High Power Pulse Supercapacitors [22].

to easily fit into the case of the key fob. In addition, the leakage is just acceptable for our purposes.

The downside of this solution is that the battery has to load the capacitor for quite a while when either one makes over 30 consecutive ranging measurements, or the battery is put into the key for the first time.

$$t = -40\Omega \cdot 140 \, mF \cdot \ln(0.007) = 27.79 \, s$$

(52)

It would take about half a minute to reload.

Again, these are all worst-case calculations. A good battery would still load the capacitor a bit faster than calculated and one could probably make a few more ranging attempts until the capacitor needs to be reloaded.

5.3.5 Super capacitors

We have already calculated the minimal size of a capacitor for driving the fob with a single coin cell. According to the necessary calculation for the worst case, the required capacity of at least 16 mF is quite large for an electrolyte capacitor.

There are two major problems with common electrolyte capacitors, namely the large physical dimensions (about 18x40 mm for radial standard aluminum capacitors) and a high leakage current over 1 mA.

Furthermore, if we want to use our system for other ranging modes in the future, even larger capacitors might be necessary. Since there is no way to fit such big electronic components into the key fob, for our purposes the use of super capacitors seems to be a good choice.

Supercapacitors have a much higher energy density than electrolyte capacitors while still providing a sufficiently good power density to support large currents, which are needed for this application. This means that the physical dimensions are only a fraction of a standard electrolyte capacitor.

If we account for heavy use[18], loss of capacity due to aging and a possible enhancement of the desired ranging distance via UWB, we can assume to be on the safe side if we use a 140 mF super capacitor. Also, the leakage with such big super capacitors is much lower[19] even though the capacitor still has to be disconnected when fully loaded.

Keeping all that in mind, we decided to use a "BestCap® Ultra-low ESR High Power Pulse Supercapacitor" by AVX [22].

In contrast to a standard electrolyte capacitor, supercapacitors have a limited amount of charge- and discharge-cycles, but since they lie between 10^5 and 10^6 this should be of no concern. The key fob will be functioning properly for at least 27 years when used ten times a day.

---

[18] 10 or more times a day.
[19] About 5 μA for a capacitance of 140 mF at 3.6 V rated voltage according to [22].

6   Simulation Model of the Power Supply

6.1   Model of the Coin Cell

For a simulation in *LTspice,* an adequate model of the coin cell has to be designed. For our purposes, a standard CR2032 coin cell by Energizer should serve as model. The basic characteristics can be looked up in the datasheet [16] where we can find a diagram of the pulse characteristics.

Load: 100 ohms - 21°C (70°F)
Pulse Duration: 2 seconds
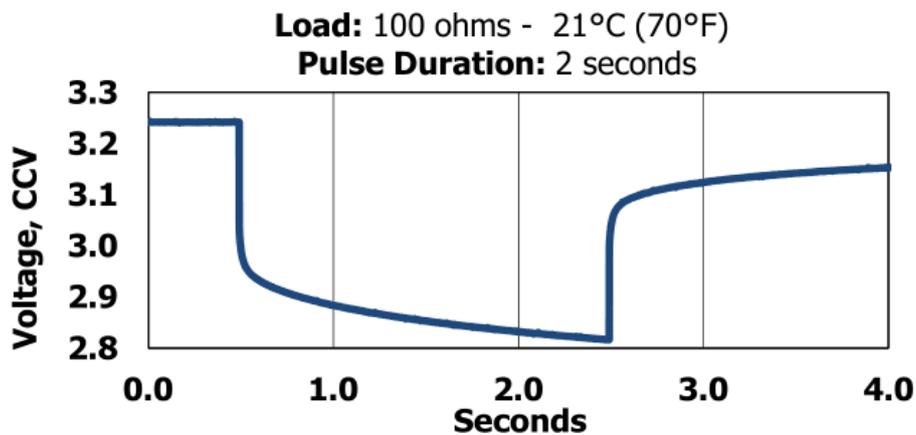
Figure 24 - Pulse Characteristics of an Energizer CR2032 Coin Cell

For the Spice model a basic equivalent circuit diagram, which can be seen in Figure 25, was chosen.[20] The first resister R_i represents the inner resistance of the coin cell. The parallel-connected resistor and capacitor represent the diffusion of electrons in the electrolyte and the electrodes [23]. For the first simulation the load R_L is high (1 $M\Omega$) for 0.5 seconds and then switches to 100 Ω for 2 seconds before it goes back to its first value.

---

[20] According to [23]

R_t and C_t can be calculated with the values obtained from Figure 24 as follows:

$u(2s) = 2.8\,V$
$U_0 = 3.25\,V$
$t = 2\,s$

$$\tau = -\frac{t}{\ln\left(1 - \frac{u(t)}{U_0}\right)} = -\frac{2\,s}{\ln\left(1 - \frac{2.8\,V}{3.25\,V}\right)} = 1.0116$$

(53)

Since

$$\tau = R_t \cdot C_t$$

(54)

we chose the value of R_t and C_t such that the outcome of the simulation fits the given diagram in Figure 24. Therefore we chose $R_t = 10\,\Omega$ and $C_t = 101.16\,mF$.
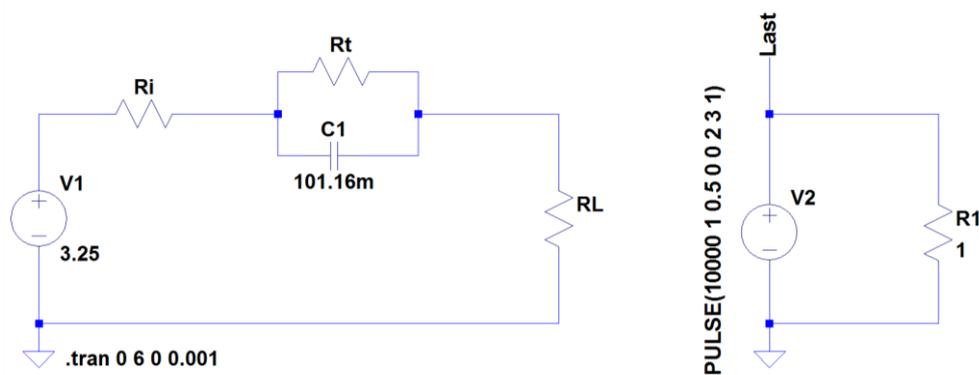
Figure 25 - Equivalent Circuit Diagram of a Standard Coin Cell

As can be seen in Figure 26, the simulation works best for a fully charged battery with $R_i = 10\Omega$, which is what is to be expected for the original measurement in Figure 24.

66
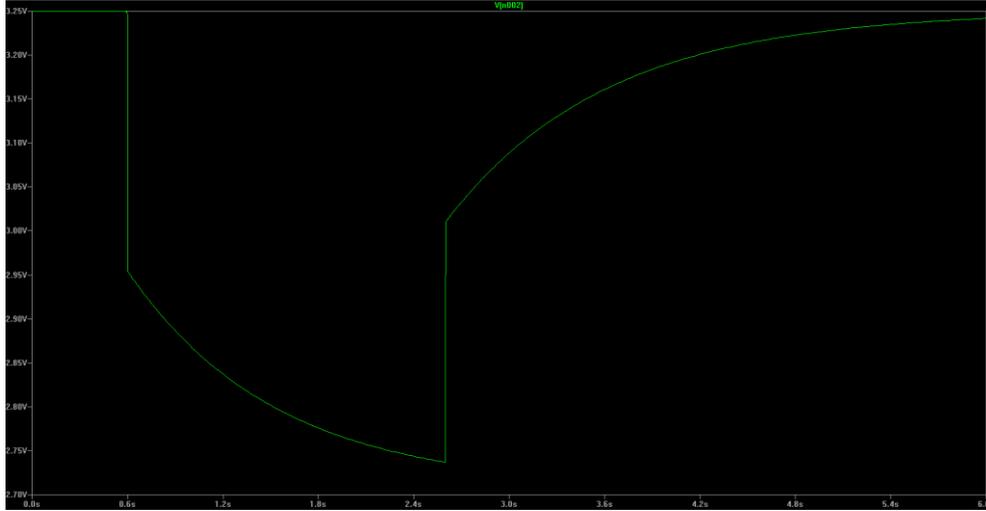
Figure 26 - Output Voltage of a Simulated Standard Coin Cell

6.2 Simulation of the Power Supply in *Fast Ranging* Mode

To simulate the whole battery, we added a limiter to the coin cell, which guarantees a maximum discharge current of 15 mA, as is proposed in [17].

To represent the load we chose a variable resistor that switches between different values to simulate the different states of the ranging transmission. The calculation of the appropriate resistance is based on the values of the current consumption in *Fast Ranging* mode in Table 5.

To account for the higher current on the input of the DC-to-DC converter, we calculated the corresponding resistance as follows.

$$P_{DW} = P_C$$

$$(55)$$

$$U_{DW} \cdot I_{DW} = U_{min} \cdot I_C$$

$$(56)$$

$$I_C = \frac{U_{DW} \cdot I_{DW}}{U_{min}}$$

$$(57)$$

P_{DW} is the power on the output and P_C the power on the input of the converter, which must be equal.

67

With this method, we get the value for the current on the input of the converter in the worst case of $U_{min} = 1.2\,V$. The lowest voltage (U_{max}) over the capacitor at the start of the discharge pulse at the battery's end of life was chosen, to calculate a substitute resistance and the corresponding load for every state.

$$R_{load} = \frac{U_{max}}{I_n}$$

Table 8 shows the values of R_{load} in the different states.

Calculation of substitute resistance at 1,2V in Fast Ranging Mode*					
mode	state	time [μs]	current in DW1000 [mA]	current in DC/DC [mA]	subst. Resistance [Ohm]
POLL	TX (Poll)	237	76,7	210,93	8,53
	IDLE	52	14,26	39,22	45,90
	RX	481	145	398,75	4,51
	IDLE	43	14,26	39,22	45,90
FINAL	TX (Final)	824	76,7	210,93	8,53
TOTALS		1.637,00			

Table 8 - Substitute Currents Ic and Resistance R for the Load

Figure 27 shows the whole circuit used for the simulation. C2 is the capacitor calculated in 5.3.1 and has a value of 642 μF. The inner resistance of the battery is 40 Ω, as is suggested in the data sheet [16] at the battery's end of life. RL factors in the worst-case efficiency of the DC-to-DC converter.
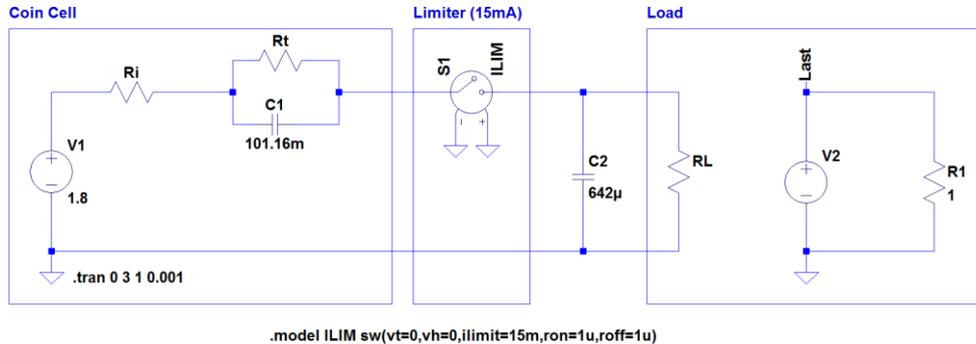
Figure 27- Equivalent Circuit Diagram of the Whole Power Supply

After a certain time to load the capacitor a ranging attempt is simulated, as can be seen in Figure 28. One can see that even if the battery is nearly empty and the maximal voltage is about 1.8 V, the voltage measured at the load (in green) drops to about 1.18 V, which is not quite enough for the boost converter to operate.

One can also see the current through the capacitor, which is limited to 15 mA. The negative current is a result of the capacitor powering the load in the opposite direction of the positive current flow.

The voltage drop is a little higher than in the calculation, which is mainly the consequence of the simplification of the load, as is the sinking current consumption because the load is not dependent on the voltage of the capacitor.
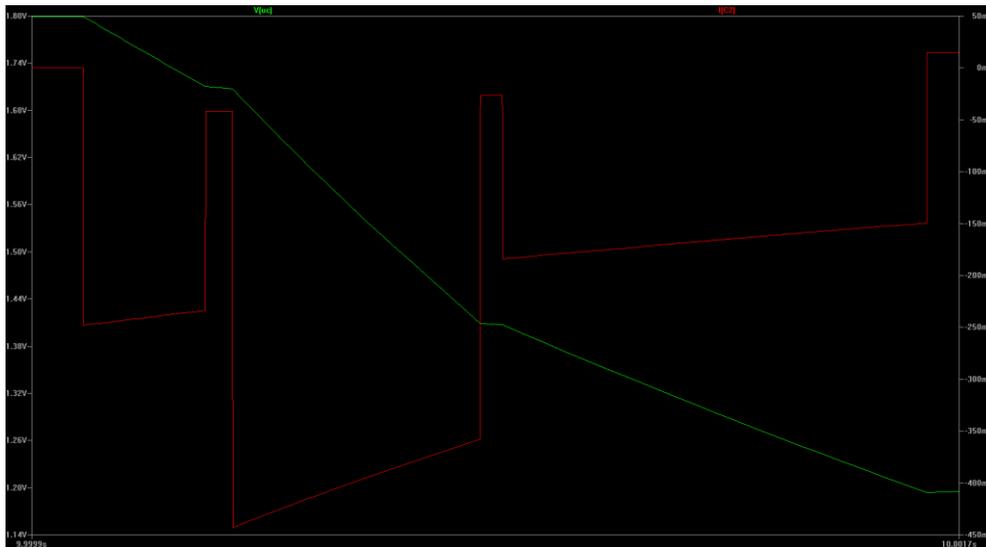
Figure 28 - Voltage Drop (Green) and Current Through the Capacitor (Red)

6.3 Simulations in *Long Ranging* mode

Last but not least, a simulation for the calculated worst case of *Long Ranging*, with the chosen 140 mF capacitor by AVX should be conducted. Figure 29 shows that the voltage drop in *Long Ranging* mode is in the 25 mV region. This time the wake up time of 3 ms is also taken into account.
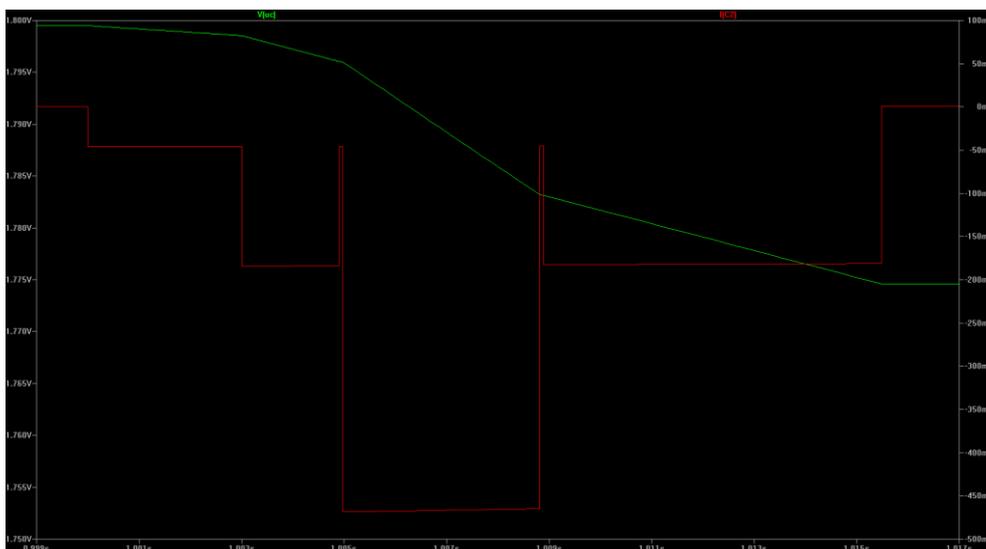
Figure 29 - Voltage Drop in "Long Ranging" Mode with 140mF Capacitor

70

Figure 30 shows the voltage drop of the capacitor during two consecutive ranging reports. One can see that the capacitor does not have enough time to fully reload when the reload time is only one second. We can calculate the maximal ranging attempts that can be made as has already been shown in chapter 5.3.4.

Figure 30 - Voltage Drop of Two Consecutive Ranging Attempts (Green)

These results are all very promising. The last simulation is for a typical ranging report. The values for the needed time in every state and the calculated substitute resistor can be seen in Table 9.

mode	state	time [ms]	current [mA]	current in DC/DC [mA]	subst. Resistance [Ohm]
		Calculation of substitute resistance at 1,2V in typical mode			
POLL	TX (Poll)	3,5	56,3	154,83	11,63
	IDLE	0,061	14,3	39,33	30,51
	RX	9,3	145	398,75	3,01
	IDLE	0,072	14,3	39,33	30,51
FINAL	TX (Final)	153,7	56,3	154,83	7,75
TOTALS		166,633			

Table 9 - Substitute Resistance for the Load in a Typical Ranging Mode

The result in Figure 31 shows that at least two or three ranging attempts are possible in a typical ranging mode according to the simulation. Even

if this is possible at the battery's end of life, it is not recommended to do so as it will drain the battery quite fast.

Figure 31 - Voltage Drop in a Typical Ranging Mode with 140mF Capacitor

6.3.1 Simulation of Multiple Ranging Attempts for *Long Ranging*

If we guarantee that we are making only one measurement every second, we can run a simulation for a few consecutive full ranging reports. For this simulation, again the *Long Ranging* mode was chosen to simulate the worst case.

The value of the capacitor is again 140 mF and the coin cell is at the end of its life with a maximum voltage of 1.8 V.

Figure 32 shows 60 consecutive ranging reports. Every report is scheduled to last one second including the sleep time where the capacitor has time to recharge. One can see that the voltage drop after 60 measurements will not fall under 1.63 V, which is more than enough to power the DC-to-DC converter. After 60 seconds the capacitor is given time to fully recharge, which lasts about a minute or respectively the calculated 27.79 s to reach 99.3 % of its original value.
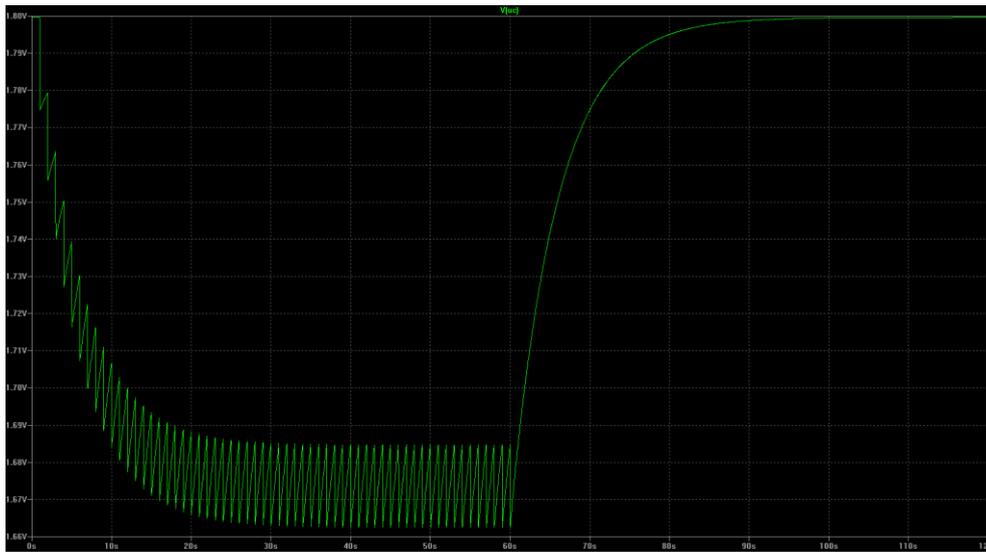
Figure 32 - Voltage Drop (Green) for 60 Consecutive Ranging Reports

To sum up the results of the simulation, it can be safely said that we can do more than just 31 ranging reports consecutively if we allow a short recharge time of about 987.5 ms after every individual measurement.

7 Component features, energy consumption and leakage

One of the specifications for the prototype, besides that it has to run on a single coin cell, was a very low power consumption of the key. This is not only important for the ranging process itself, but especially also for all the time the DW1000 is not being used. The goal is that all the components have minimal leakage. The current consumption should stay below 10 µA when the device is not being used.[21]

7.1 The NCF29A1 (Token 3D) IC by NXP

The *NCF29A1* IC, further referred to as *Token IC*, is a single chip solution by NXP, providing all the features needed for a PKE system. The device incorporates a Security Transponder, UHF Transmitter and RISC Controller on the same chip. It can be powered by a single Lithium cell (1.8 V to 3.6 V) and provides a low power mode, referred to as *POWER OFF* mode with very low current consumption.

The IC also provides a 3D LF active interface operating at 125 kHz that can do a tree axis (3D) LF signal strength measurement. In addition, it can wake up from POWER OFF mode when detecting an LF signal, which shall later be used as a trigger to do a ranging measurement via UWB.

The RISC controller is powered by a low power hardware extended 16-Bit Micro RISC Kernel (MRK IIIe) employing a 2-stage pipeline architecture. It features a uniform reference frequency of 27.6 MHz, a 2048 Byte EEPROM[22] for data storage, 10 I/O-ports[23], and provides a pin that can detect changes in a motion sensor for a motion detection function.

The device also supports many different useful features, about which we will not go into detail, like capacitive tuning for maintaining an optimal resonance frequency to optimize reception of an incoming LF signal.

---

[21] i.e. when the device is out of the vicinity of the car

[22] A fact that led to a few problems over the course of the development of the software.

[23] A fact that also led to some problems. This time concerning the development of schematic for the prototype.

7.2 Additional Components

It is crucial that the current consumption of the prototype is minimized when the device is inactive. This should guarantee that the key could be used for at least 2 years without changing the battery. If the key is out of the vicinity of the car, the Token IC shall be in POWER OFF mode, which means that it can only be woken up in case it recognizes a wake-up sequence of an LF field or if one of the safe-fail ports is high, e.g. if a button is pushed. Also, the DW1000 should be switched off completely by disabling the DC-to-DC converter. As a consequence of this approach, the DW1000 must be programmed from scratch before every ranging measurement if the device was in sleep mode beforehand.

To achieve the goal of a low current consumption the quiescent current of all implemented parts must be as low as possible. The most important parts to mention are the super capacitor, which was already described in chapter 5.3.5 and the DC-to-DC converter.

7.2.1 DC-to-DC converter ADP1607

The *ADP1607* by *Analog Devices* is a synchronous, fixed frequency, step-up dc-to-dc switching converter with an adjustable output voltage between 1.8 V and 3.3 V. It has a very high efficiency of 96 % according to the datasheet [24] and can work with an input voltage as low as 0.9 V. The quiescent current during operation is maximally 29 µA, but more importantly, the shutdown current $I_{leak\ DCDC}$ lies between 0.06 µA and 0.67 µA.
The typical current limit is 1 A, which is more than enough to power the DW1000. Like with most DC-to-DC converters, a well-designed PCB layout is required to guarantee high efficiency, good regulation and stability.

7.2.2 High Power Pulse Supercapacitor

The two most important criteria for the capacitor were its size and a very low leakage current. Since ordinary electrolyte capacitors with 140 mF capacity are usually not available and would probably be excessively big for a car key anyway, a supercapacitor by AVX was chosen to do the job. With a dimension of 5.3 x 8.2 x 5.8 mm, it is sufficiently small to fit into the key and with a maximum leakage current $I_{leak\ Cap}$ of 5 µA it should

be a good solution to provide the high peak currents which are needed for the distance measurements.[24]

7.2.3 Multiplexer

Since the final design of the layout was based on an earlier design, most of the ports of the Token IC were already being used. It was a challenge to make enough ports available to include all the new functions. Unfortunately, there was only one port and so it was decided to use a multiplexer to gain one more port.

There is no scenario where the motion sensor is needed while the key does a range measurement. This is why port P21 could be used for two input signals, the motion sensor signal and the SPI input (MISO). It is possible to switch between the two signals with a signal of port P15.[25]

A low-power 2-input multiplexer by NXP was chosen, namely the 74AUP1G157. It can select data of two data inputs under control of a data select input, guarantees a wide voltage supply range from 0.8 V to 3.6 V and has a leakage current $I_{leak\ MP}$ of 0.4 μA in the worst case [25].

7.2.4 Level shifters

The communication between the Token IC and the DW1000 is established through SPI. The problem is that the supply voltage of the Token is usually far below the supply voltage of the DW1000. According to the datasheet of the DW1000 [15], the minimal input voltage for high level should be 0.7 x VDDIO, where VDDIO is the supply voltage of the IC. This means that for a supply voltage of 3.3 V, the minimal input voltage must be

$$V_{IN\ min} = 0.7 \cdot 3.3\ V = 2.31\ V$$

(58)

which is less than the minimal output voltage of the Token IC at the battery's end of life. The voltage of the SPI signals coming from the Token IC must therefore be translated upwards to guaranty a steady data transmission. Three level shifters are needed for the SPI communication,

---

[24] Refer to [22] for the datasheet.
[25] Compare Figure 35 - Schematic of the Prototype.

in particular for the clock-, output- and chip-select lines[26]. Only the input (DW_MISO) does not have to be shifted, since the Token IC can cope with input voltages over 3.3 V.[27]

The final decision was a 74AUP1T34 low-power dual-supply translating buffer by NXP. It allows low voltage interfacing between two voltage nodes with a range from 1.1 V to 3.6 V. It needs 0.5 µA supply current and the maximal power-off leakage $I_{leak\ LV}$ is as low as 0.4 µA.

7.2.5 MOS-FET

Finally a P-channel MOS transistor had to be chosen to regulate the charging process of the supercapacitor. First and foremost, it should only be switched on and off to charge the capacitor at specific moments. In later applications, the charging current shall be regulated by applying a PWM signal to the gate.

The crucial value for saving power is the gate source leakage current $I_{leak\ MOS}$, which has a maximal value of 100 nA with the Philips BSH201 according to [26].

---

[26] Compare to Figure 35. Those are the three nets DW_SPIclk, DW_MOSI and DW_SPICS.
[27] This is a company intern information. The Datasheet only offers info about the minimal input voltage for high level.

7.3 Total Leakage Current

Altogether, the expected additional current leakage $I_{leak\ add}$ adds up to

$$I_{leak\ add} = I_{leak\ DCDC} + I_{leak\ Cap} + I_{leak\ MP} + 3 \cdot I_{leak\ LV} + I_{leak\ MOS}$$
$$(59)$$

$$I_{leak\ add} = 0.67\ \mu A + 5\ \mu A + 0.4\ \mu A + 3 \cdot 0.4\ \mu A + 0.1\ \mu A = 7.37\ \mu A$$
$$(60)$$

With an additional maximal quiescent current of 2.1 μA from the Token IC with active LF receiver and about 50 nA supply current of the DW1000 in DEEP SLEEP mode, we can only just achieve our goal of a maximal leakage of 10 μA.

$$I_{leak\ total} = 7.37\ \mu A + 2.1\ \mu A + 0.05\ \mu A = 9.475\ \mu A$$
$$(61)$$

Since this is a worst-case calculation and the total leakage strongly depends on the leakage of the supercapacitor (~ 5 μA), only the final measurement can show the actual power consumption when the device is inactive. In addition, there is probably a strong dependence on the production tolerance of the capacitor.

8   Final Prototype

8.1   Requirements

One of the main challenges in the development of the hardware was the power supply. It has to provide a constant supply voltage of a minimum of 1.8 V for the Token IC, as well as a minimum supply voltage of 2.8 V for the DW1000. The challenge is the rather high power consumption of the DW1000 during receiving an UWB signal. It consumes up to 145 mA of current during RX and up to about 77 mA during TX according to the measurements detailed in chapter 5.

As also shown in chapter 5, power consumption of the chip strongly depends on the data rate, the pulse repetition frequency (PRF) and the overall length of the message which is being sent or received. The stated values were recorded for the highest possible data rate of 6.8 MHz, a PRF of 64 MHz and a short preamble length of 128 bits. With a longer preamble the current can even increase to a maximum value of 95 mA in TX mode.

Although, with optimized software, the complete ranging process only lasts about 10 ms, a single coin cell battery can certainly not provide such high currents for the DW1000 IC. To meet the requirement of a single CR2032 coin cell battery, powering the whole prototype, a capacitor has to provide the energy for the peak currents. We chose to use supercapacitor which can store 10 to 100 times more energy per unit volume or mass than electrolytic capacitors.[28]

---

[28] Refer to chapter 5 for information about the power supply design.

8.2 Layout of the Prototype
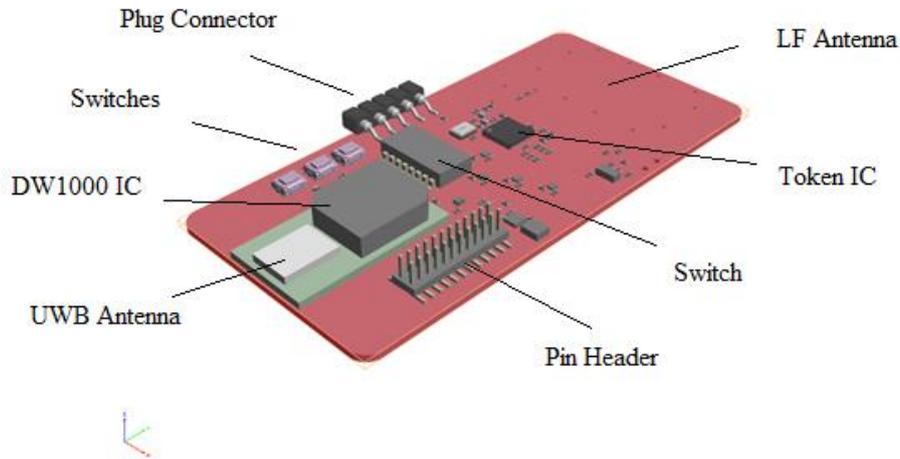
Figure 33 - 3D Animation of the Prototype (Frontside)

Figure 33 shows the frontside of the prototype in a 3D animation. One can see the DW1000 and the UWB antenna in the front on the green subsurface. To the left there are three switches and to the right there is a pinheader to do, e.g., some timing-measurements. Above of the DW1000 there is an analog switch. The black square above the switch and next to the plug connector at the edge of the board, there is the Token IC. The area above is entirely for the LF antenna.
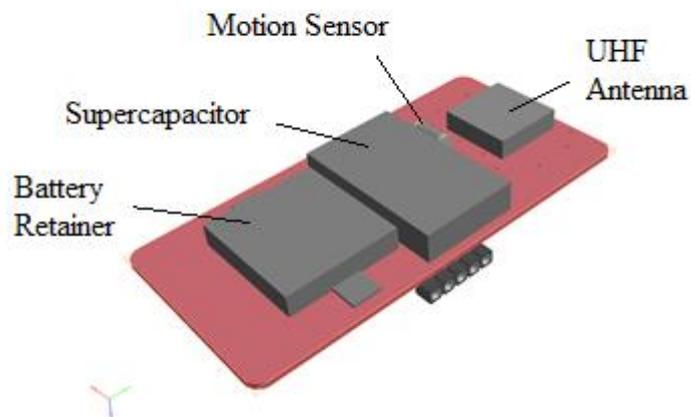
Figure 34 - 3D Animation of the Prototype (Backside)

80

The capacitor, as well as the battery retainer, the motion sensor and the UHF antenna can be found on the backside of the board, as depicted in Figure 34. In the schematic depiction in Figure 35, the super capacitor is represented as C20. Since there was trouble with the supplier, we actually got a 60 mF capacitor instead of the depicted 140 mF. It can be charged over the resistor R6, which has a value of 100 Ω, by switching on the PMOS.

R6 is necessary to restrict the current flow from the battery into the capacitor as long as we have not established the possibility to limit the current by applying a PWM signal to the base of the PMOS.

According to chapter 5.3.2 we have to calculate a new time for the capacitor to recharge. We again make the assumption that the battery is at its end of life and therefore has an inner resistance of 40 Ω.

$$t = -(R_{i,Bat} + R6) \cdot C \cdot \ln(1 - 0.993)$$

(62)

$$t = -(40 \; \Omega + 100 \; \Omega) \cdot 60 \; mF \cdot \ln(0.007) = 41.6 \; s$$

(63)

The gate of the PMOS is controlled by the Token's P15 pin. This controlled loading function of the prototype board can also be switched off manually with the SW1-4 switch. The capacity provides the input voltage of the DC-to-DC converter (ADP1607). There is also a possibility to disconnect the capacitor by opening the jumper J3 and connect e.g. an external power source to the pin header P3. To do so, the jumpers J12 and J5 also have to be closed to connect the external source to the input of the ADP1607.

The DC-to DC converter is a boost converter with very high efficiency up to 96 %. It can guarantee an output voltage of 3.3 V with an input voltage as low as 0.9 V (minimum start-up voltage)[29]. If no DC-to-DC converter is needed, e.g. if a Lithium polymer battery should power the device, the output of the ADP1607 can also be disconnected via the J4 jumper. In this case the jumpers J11 and J5 must be closed and the alternative battery can be connected to the pin header P3.

---

[29] Refer to chapter 7.2.1 for detailed information about the ADP1607.

For general use of the prototype a CR2032 coin cell retainer is provided on the backside of the device. When power is provided by a coin cell the jumpers J3, J4, J10 and J11 must be closed to ensure functionality. Also, the SW1-1 switch must be in the ON position because the Token IC must switch on the DC-to-DC converter before every measurement.

As mentioned before, in standard operation mode the Token IC communicates with the DW1000 IC over SPI. It is also possible to connect an external host controller for the DW1000 to the board via the P1 header (pins 2-5). The SPI interface to the Token can therefore be disconnected manually by switching off the four switches SW1-5 to SW1-8. If no external host controller is used one has to make sure that those switches are always on to ensure SPI communication between Token and DW1000.

For general use the Token IC is always connected directly to the battery which provides a steady voltage between 1.8 V and 3 V. Since the DW1000 is usually supplied by a higher voltage of 3.3 V the SPI interface provides three level translators (LTs) to adapt to the different voltages when the Token IC sends or receives data to or from the DW1000. The Token provides the main clock signal (DW_SPICLK) over LT3, the chip select signal (DW_SPICS) over LT1 and the output signal (DW_MOSI) over LT2. Only the input signal (DW_MISO) does not have to be adjusted as the Token IC can handle input voltages up to 3.6 V even if its own supply voltage is below that level. This is why there is no level translator for the DW_MISO signal.

There is one specific character of the DW_MISO signal, though. As it uses the same port (P21) of the token IC as the motion sensor, it is connected to a multiplexer. To ensure functionality of both SPI and motion sensing, jumper J2 has to be closed to enable switching between the two functionalities.

The prototype also features three pushbuttons, two of which are connected to the two fail-safe wake up pins P10 and P11 of the Token. The third is connected to P12. All three buttons can take over all kinds of different functions in future applications such as locking or unlocking the car via remote.

Last but not least the device features two more antennas for LF and UHF signals and an LED. The latter only can be controlled by the DW1000. The Token IC can use the LF interface as a contactless transponder and is capable of deriving its power supply and system clock by inductive coupling to an LF field generated by a corresponding base station. It can

also be used to detect the presence of an LF field to wake up the IC from POWER OFF state.

The POWER OFF state is treated in detail in the software description. Furthermore the IC features an UHF transmitter which comprises a Frequency Shift Keying (FSK) and Amplitude Shift Keying (ASK) modulator. All these features are not implemented in the software yet.
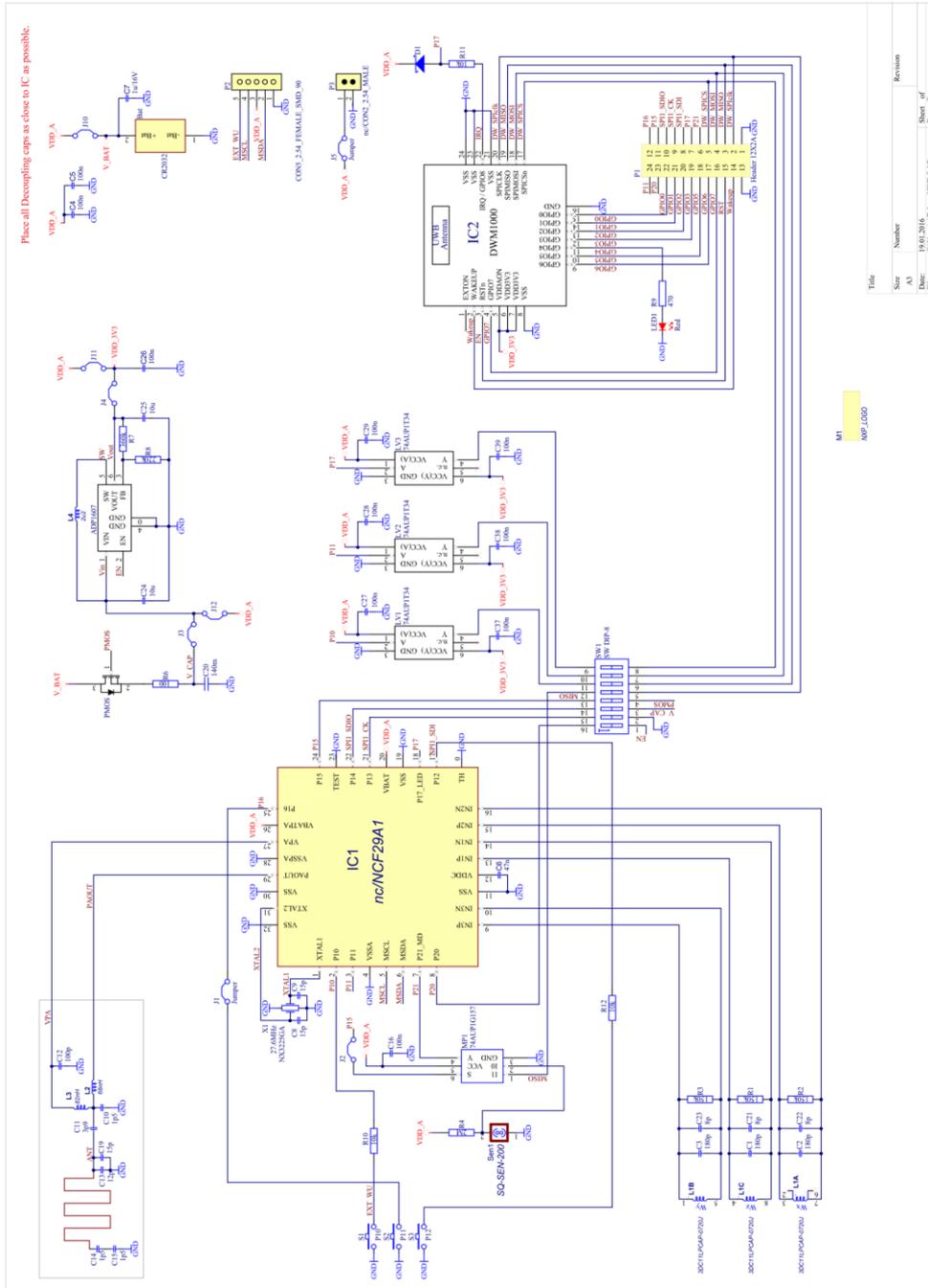
Figure 35 - Schematic of the Prototype

9　Software Description

The software is slightly based on the ranging software by Decawave as it also uses a state machine to handle the different states of the ranging process. Since the Token IC has a different architecture and generally less capacities than the STM32 IC concerning internal memory, clock frequency, available port pins, etc.[30], the source code is quite a bit different though. The ranging process, too, is a little different to the process proposed by Decawave to save time and energy. This procedure is explained in chapter 9.2 below.

9.1　First Time Power-Up

At first time power-on, e.g. when a battery is inserted into the device, the system clock, Watchdog Timer and Timer0 along with some other registers, like the Battery System Register of the Token, have to be initiated. Also all GPIO ports are set to input at first to save power. Afterwards port P20 is set to output and the SPI functionality is initiated.

After initiation, the key has to be given time to fully load the capacitor C20, which takes about 5 minutes. During this time a ranging measurement is not recommended (and actually not possible), although later versions of the software might make it possible to do so after a minimum loading time of 30 seconds.

To initiate a TOF measurement, the DW1000 has to be powered up beforehand. This is done by switching on the DC-to-DC converter by setting its enable input to high via the P20 pin of the Token. The converter has to be given a little time[31] to guarantee a stable output voltage. After power is applied to the DW1000 the IC also needs about 2 ms time for its power-up sequence. This is mainly caused by the time it takes for the oscillator to start up and stabilise. During this process the RSTn pin is driven low by the DW1000 internal circuitry as part of its power up sequence. [32]

---

[30] Refer to chapters 4.4.2 and 7.1.
[31] The Soft Start Time is typically 1.3 ms according to the datasheet.
[32] Refer to chapter 4.3.1 for a detailed description.

9.2 Standard Ranging Procedure after Power–Up

After powering up the DW1000 IC, the SPI baud rate is set to 2 MHz[33] and the Device ID of the Decawave chip is read to test the communication between the DW1000 and the Token IC. If the Device ID cannot be read, the program effects a reset and the process starts from the beginning. If the ID is correctly transmitted, the baud rate is set to maximal speed (4 MHz with the Token) and some basic configurations are made, i.e. preamble code, data rate, preamble length and pulse repetition frequency, TX power level, antenna delay, etc. are written into AON and OTP memory of the DW1000.

The ranging procedure itself is handled with a state machine. The state machine consists of eight cases which handle all the different states the DW1000 can get into during a ranging process. In addition, the state machine is able to let the prototype be either Tag or Anchor. This will not be necessary in further applications, since the car key always gets the role of the Tag, but was quite a useful feature during development. Every TOF measurement starts with an initiation case were some custom settings can be made. If some former delay between Poll transmission and Final transmission is already known from a preceding measurement, it will be taken into account for the next one.

After the initiation case the device sends a Poll Message. This message is only a Function Code[34]. The Function Code itself consists of 7 bytes, as is depicted in Table 10. The Frame Control tells the Anchor what kind of message it is dealing with. The PAN ID can be used to associate the network or might be an installation-configured constant. The sequence number (SEQ) byte is incremented modulo-256 for every frame sent and the 2-octet FCS is a CRC frame check sequence, as per IEEE rules. Although the Poll Message does not contain an actual message, e.g. timestamps or any other additional data, the time when it is sent is stored into the RAM of the Token to later calculate the TOF. On the Anchors side the Poll Message is used to initiate a range measurement. It triggers the Anchor to send a Response Message which then contains the first timestamp used to calculate the TOF.

---

[33] This should ensure a hitch-free communication.
[34] The Function Code distinguishes different messages from another.

2 bytes	1 byte	2 bytes	variable # of bytes	2 bytes
Frame Control (FC)	Sequence Number	PAN ID	Message	FCS

Table 10 – Function Code of a Ranging Message

The next case is a wait-state where the DW1000 switches on its receiver module and waits either for a response or a timeout, both of which will cause an interrupt, which is handled in the respective interrupt routine. If a timeout occurs the ranging process starts from the beginning. Only the initiation case will not be repeated. If the DW1000 gets a response in time the timestamp of the Response Message from the Anchor is transferred via SPI and stored in the RAM of the Token. The state machine moves on to the next case right away, which handles preparation of the *Final Message*.

During the time the Tag waits to receive a message, the Anchor has to detect the Poll Message, note its time of arrival (TOA) and send a Response Message, which is basically built up like the Poll Message, with a different FC of course.

In this last case the Token calculates the *roundtrip time* and its own *response time*. The *roundtrip time* is the difference between the two noted time stamps of the previously sent Poll Message and the only just received Response Message. The *response time* is the difference between the just received Response Message and the expected time when the *Final Message* will be sent to the Anchor, which can be estimated. The *Final Message* therefore consists of the usual seven bytes (2 for FC, 1 for SEQ, 2 for PAN ID and 2 for FCS) plus an additional 8 bytes of message data, 4 bytes for the roundtrip time and 4 for the expected response time.

As soon as the *Final Message* is sent,[35] the Token switches off the DC-to-DC converter, clears all interrupts, sets the wakeup registers and goes into POWER OFF state. In this state the Token can only be woken up by an external trigger like when a fail save switch has been pressed or an LF wake up pattern has been detected. In future applications the Token of course will not go to sleep, but continue with the PKE process as soon as the key is confirmed to be in range. For now only the ranging process is implemented in the firmware.

---

[35] A respective flag of the DW1000 reports this. The flag is cached in yet another state of the state machine.

When the Anchor receives the *Final Message* it has all the information it needs to calculate the TOF. It only needs to extract the roundtrip- and response time of the Tag out of the *Final Message*. These two timestamps paired with the self-recorded roundtrip- and response time of the Anchor is all the information required to calculate the TOF[36] and consequentially the distance between Tag and Anchor.

9.3 Alternative software for the CES 2016

Additionally to the basic function of TWR, a second firmware was developed for the CES 2016[37]. In this case the capacitor was removed from the key and it was powered by a strong accumulator. The task was to carry out a position estimation in a TOA scheme at least 2 times a second with two different Anchors to estimate a position on the driver's side of a car. With this information a light was programmed to follow the position of the car key.

The software was therefore adapted and slightly changed. It had to support ranging between two different Anchors. This was achieved by switching between two different PAN IDs[38] after every measurement.

Two EVB1000 boards were used as Anchors and the result of the measurement was provided at the SPI2-pins of the STM32 IC. The output data was presented in ASCII code and consisted of the Anchor address, the Tag address, the range in mm and the number of the measurement. An example of the output can be seen in Figure 36.

---

[36] According to the formula in chapter 3.7.5.
[37] Consumer Electronics Show 2016 in Las Vegas.
[38] Refer to Table 10 – Function Code of a Ranging Message.
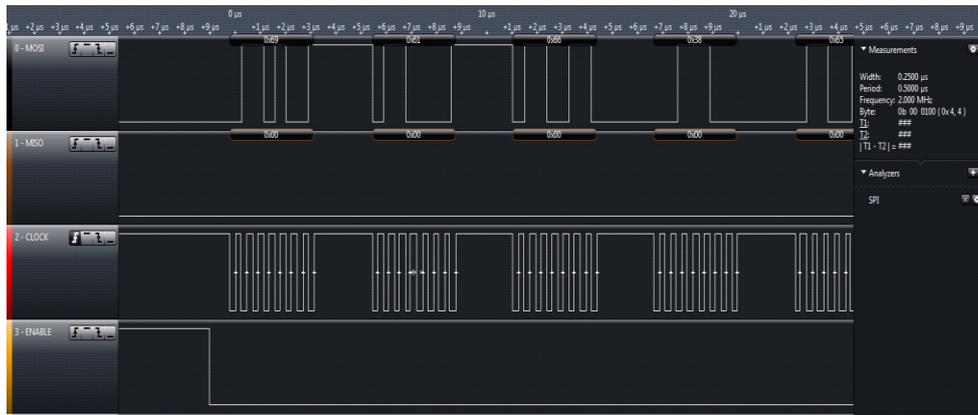
Figure 36 - Example of the Output at the SPI2 Connector

10 Final Measurements and Calculations

During the measurements of the current consumption, I discovered an error in the layout. The PMOS is connected wrongly and as a result, the Token IC cannot switch it off. Luckily enough, the capacitor can still be loaded over the body diode of the PMOS, but since it cannot be switched off, a constant current is loading the capacitor as soon as the threshold voltage of the diode is exceeded. The final measurements are still valuable to make a good guess how much energy the prototype consumes in total.

After optimizing the software to ensure a minimum time for the whole ranging process, the actual current consumption of the whole prototype and the voltage level at the capacitor was measured. To do so, the key was connected to a high precision power supply with an output voltage of 3 V.

We gave the capacitor more than enough time to charge[39] before one single ranging measurement was performed. Afterwards the DC-to-DC converter was switched off and the Token IC was put into low power consuming POWER OFF mode.
Figure 37 and Figure 39 show the voltage at the supercapacitor and the current consumption during the time the capacitor is loading.

---

[39] The time was set to 4 minutes and 40 seconds.
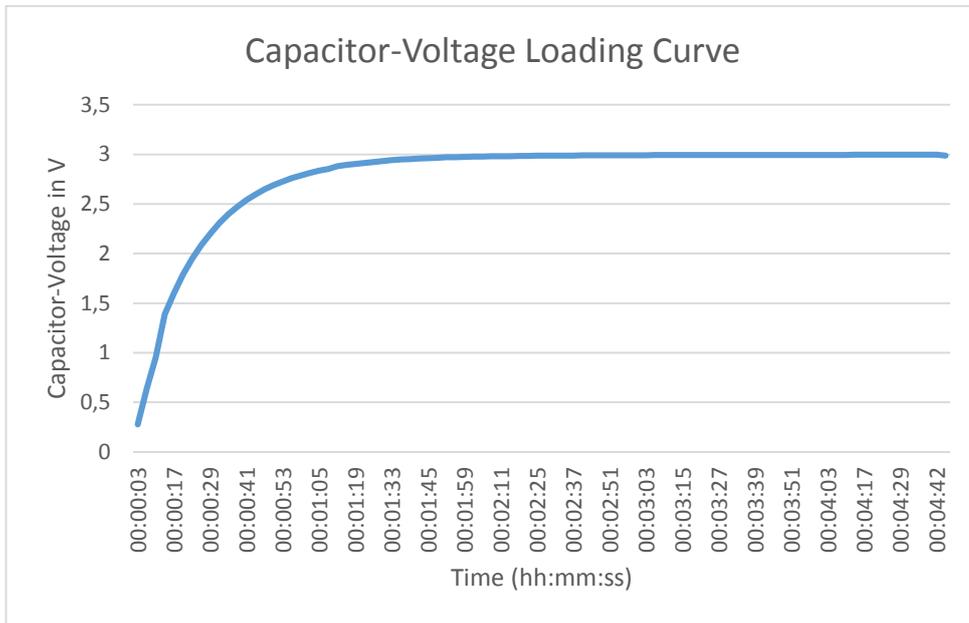
Figure 37 - Loading Curve of the Supercapacitor
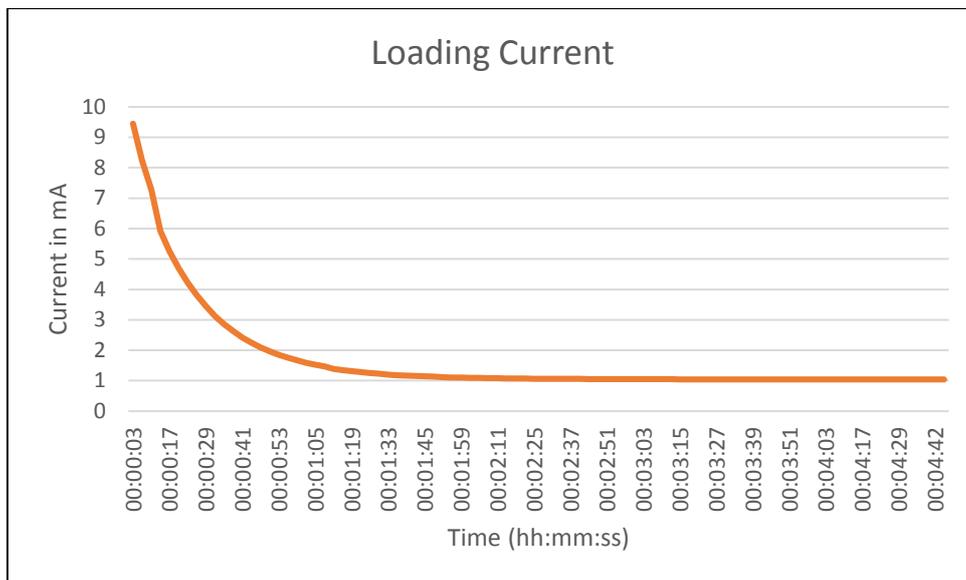
Figure 38 - Current Consumption while Loading

Figure 39 finally shows the current consumption after the ranging process has finished and the device goes into POWER OFF state. The current consumption in this mode lies between 1.14 µA and 1.16 µA.

91

Additionally the leakage of the capacitor has to be taken into account. Figure 40 shows the voltage drop of the capacitor over time. It can be seen that the voltage drops by about 0.3 V in 1.5 hours' time. We can calculate the leakage current I_{C_loss} by

$$I_{C\_loss} = C \cdot \frac{\Delta U}{\Delta t}$$

(64)

$$I_{C\_loss} = 60\ mF\ \cdot \frac{0.3082\ V}{5103\ s} = 3.62\ \mu A$$

(65)

Which gives us an estimated total current consumption of

$$I_{total\_loss} = 1.16\ \mu A + 3.64\ \mu A = 4.78\ \mu A$$

(66)
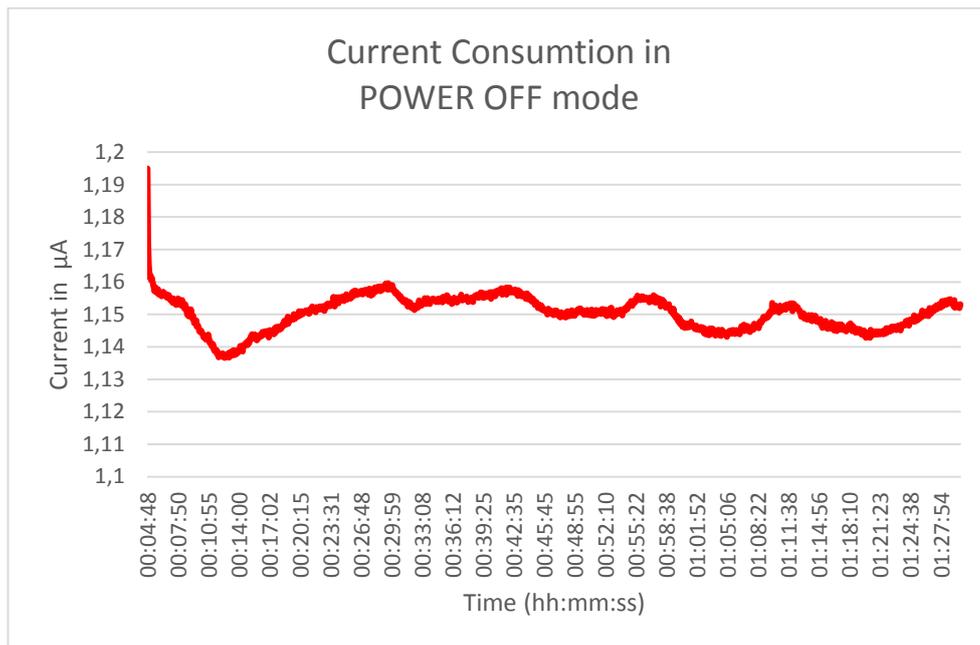
Figure 39 - Current Consumption in POWER OFF Mode
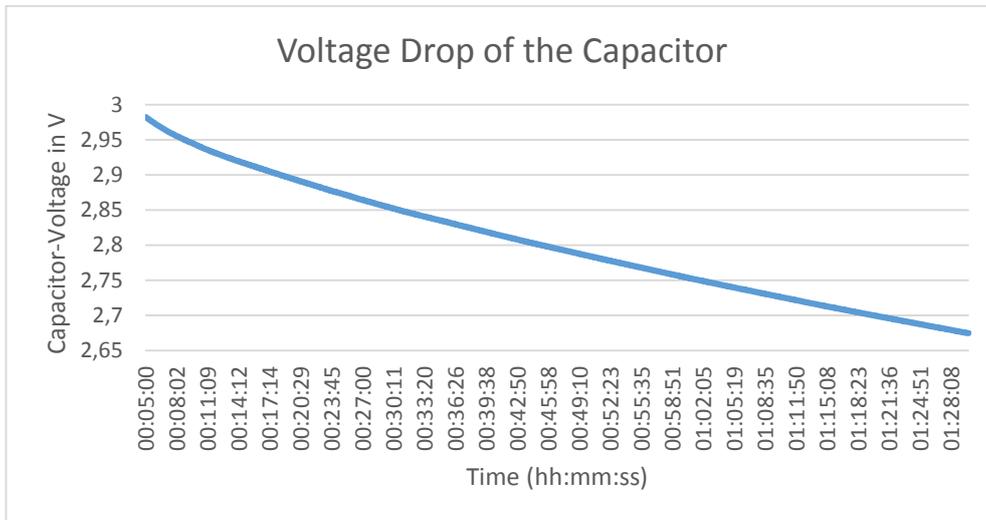
Figure 40 - Voltage Drop of the Supercapacitor

We cannot finally calculate how long the key can function with a single CR2032 coin cell when 10 ranging measurements are performed every day. The capacity of a standard coin cell is about 240 mAh[40]. The total charge consumed during a single ranging process in *Fast Ranging* mode, Q_{dis}, is 0.125 mAs according to Table 5, which means with 10 measurements a day it adds up to 1.25 mAs.

We can assume that the key consumes 4.78 µA of current the rest of the day when it is in POWER OFF mode, which adds up to

$$Q_{sleep\_day} = 86400 \; s \; \cdot 4.78 \; \mu A = 412.99 mAs$$

(67)

which means that the key consumes a total energy of

$$Q_{total\_day} = Q_{dis\_day} + Q_{sleep\_day} = 414.24 \; mAs = 0.2877 \; mAh$$

(68)

per day. If we now calculate how many days, the key can sustain with a single coin cell we get

$$t_{total} = \frac{240 \; mAh}{0.2877 \; mAh} = 834.29 \; days = 2.29 \; years$$

(69)

---

[40] According to [16].

93

11 Conclusion

The purpose of the thesis is to close a security loophole in PKE systems by measuring the distance to a car with an UWB system. It has been shown that this can be done in an energy-efficient way by only using a single CR2032 coin cell. The main problem was to minimize the current consumption when the device is not being used. This could be achieved by using components with very low leakage current and by optimizing the software to minimize the time for a single ranging measurement.

As can be seen in chapter 10, a practical use of such a key is possible given that the key must work for at least 2 years without changing the battery. To be fair, the whole PKE system will consume a little more power than proclaimed in the calculation. This is hardly of any consequence though, since the major part of the energy is consumed during the time where the device is inactive. This makes up for about 99.70 % of the total energy consumption in one day. It can therefore safely be said that the PKE system, which is also only executed the proclaimed 10 times a day in the worst case, does not play a big part in the total energy consumption of the key.

This thesis does not focus on the accuracy of the TOF measurements. The average precision of the positioning system is currently in the range of 10 cm, which is enough for detecting the driver outside of the car. In further investigation, care should be taken to either improve this accuracy or at least maintain it, while further reducing the power consumption.

In conclusion, the prototype shows that this solution is practical in principle. It is now ready to undergo further testing. For a further development of the product, of course, other factors like a reasonable price will play a role. These are questions to be addressed by further research.

12 Bibliography

[1] S. Drude, „IR-UWB Ranging Customer Requirements Specification," NXP, 2015.

[2] M.-G. D. Benedetto, T. Kaiser, A. F. Molisch, I. Oppermann, C. Politano und D. Porcino, UWB Communication Systems - A Comprehensive Overview, New York: Hindawi Publishing Corporation, 2006.

[3] M. Y. a. B. G. Nickerson, *Ultra Whideband Wireless Positioning Systems,* Faculty of Computer Science University of New Brunswick Fredericton, N.B. E3B 5A3 Canada , 2014.

[4] E. G. S. S. D. L. Jeff Foerster, „Ultra-Wideband Technology for Short- or Medium-Range Wireless Communications," 2001.

[5] Radio-Electronics.com, „www.radio-electronics.com," [Online]. Available: http://www.radio-electronics.com/info/wireless/uwb/uwb_development.php. [Accessed 29 12 2015].

[6] S. Emami, UWB Communication Systems: Conventional and 60 GHz, Springer, 2013.

[7] C. E. Shannon, *Communication in the presence of noise,* Proc. Institute of Radio Engineers , 1949.

[8] Wikipedia, „IEEE 802.15.4," [Online]. Available: https://en.wikipedia.org/wiki/IEEE_802.15.4. [Accessed 15 01 2016].

[9] A. Azim, M. A. Matin und A. a. N. Amin4, „UWB Technology for WSN Applications," 2011.

[10] D. Zeng, *Pulse Shaping Filter Design and Interference Analysis in UWB Communication Systems,* Virginia, 2005.

[11] Decawave, „RTLS Introduction," Decawave, Dublin, 2014.

[12] Decawave, "APS013 - DW1000 and Two Way Ranging," Decawave, 2015. [Online]. Available: http://www.decawave.com/support. [Accessed 19 01 2016].

[13] T. Baier, „Building blocks for sensor localization in WSN's for technology items cross-use case and cross-domain interoperability requirements and specifications," NXP-AT, Gratkorn, 2015.

[14] Decawave, „APS011 - Sources of Error," Decawave, Dublin, 2014.

[15] Decawave, „DW1000-Datasheet V2.03," Dublin, 2014.

[16] I. Energizer Holdings, „data.energizer.com," Energizer, [Online]. Available: http://data.energizer.com/PDFs/cr2032.pdf. [Accessed 29 07 2015].

[17] M. Jensen, "White Paper SWRA349 - Coin cells and peak current draw," Texas Instruments, 2010.

[18] S. Retena, "www.renata.com," Renata Batteries, 2011. [Online]. Available: http://www.renata.com/fileadmin/downloads/productsheets/lithium/3V_li thium/CR2025MFR_v04.pdf. [Accessed 29 07 2015].

[19] M. VARTA, "www.varta-microbattery.com," [Online]. Available: http://www.varta-microbattery.com/applications/mb_data/documents/sales_literature_varta /HANDBOOK_Primary_Lithium_Cells_en.pdf. [Accessed 29 07 2015].

[20] A. Devices, „http://www.farnell.com/datasheets/1854060.pdf," Analog Devices, Inc., 2012-2014. [Online]. Available: http://www.farnell.com/datasheets/1854060.pdf. [Accessed 05 08 2015].

[21] T. Instruments, „www.ti.com," Texas Instruments Incorporated, [Online]. Available: http://www.ti.com/lit/ds/symlink/tps61090.pdf. [Accessed 29 07 2015].

[22] AVX, „BestCap® Ultra-low ESR High Power Pulse Supercapacitors V 12.6," AVX, Pennsylvania U.S.A..

[23] S. C. Hageman, „Using PSpice to Simulate the Discharge Behavior of Common Batteries," EDN Magazine, 1993.

[24] A. Devices, „ADP1607- Datasheet," Analog Devices, 2012 - 2014.

[25] NXP, „74AUG1G157 Low-power 2-input multiplexer - Datasheet," 2012.

[26] P. S. (NXP), „BSH201 Product Specification," Philips Semiconductors (NXP), 1998.

[27] B. Lembrikov, Novel Applications of the UWB Technologies, InTech, 2011.

[28] Vishay, „www.farnell.com," Vishay Intertechnology, Inc, 11 02 2010. [Online]. Available: http://www.farnell.com/datasheets/614504.pdf. [Accessed 11 08 2015].

[29] H. K. T. u. Wirtschaft, „www.hs-karlsruhe," [Online]. Available: https://www.hs-karlsruhe.de/fakultaeten/fk-mmt/fk-mmtlabore/ieem/ieem-forschung/automotive-diagnose.html. [Accessed 06 08 2015].

[30] F. Andre, „www.mdt.tu-berlin.de," Tu Berlin - Elektrische Mess- und Diagnosetechnik, 22 10 2008. [Online]. Available: https://www.mdt.tu-berlin.de/fileadmin/fg184/Lehre/Projekte/projekt-battery-model-andre.pdf. [Accessed 06 08 2015].

[31] A. BestCap, „Farnell," AVX BestCap, [Online]. Available: http://at.farnell.com/avx/bz05ca103zsb/kondensator-bestcap-1012v/dp/1302045. [Accessed 2015].

[32] Wikipedia, „Ultra-Wideband," [Online]. Available: https://en.wikipedia.org/wiki/Ultra-wideband#cite_note-1. [Accessed 29 12 2015].