Lucerne University of
Applied Sciences and Arts

HOCHSCHULE
LUZERN

Technik & Architektur
FH Zentralschweiz

MSE | MASTER OF SCIENCE
IN ENGINEERING

UAV Serial Switch Documentation

Stefanie Schmidiger

MASTER OF SCIENCE IN ENGINEERING
Vertiefungsmodul I

Advisor: Prof. Erich Styger

Experte: Dr. Christian Vetterli

Horw, 2018

Hiermit erkläre ich, dass ich die vorliegende Arbeit selbstständig angefertigt und keine anderen als die angegebenen Hilfsmittel verwendet habe. Sämtliche verwendeten Textausschnitte, Zitate oder Inhalte anderer Verfasser wurden ausdrücklich als solche gekennzeichnet.

Horw, 10.01.2018 Stefanie Schmidiger

Versionen

Version 0	Initial Document	10.01.18	Stefanie Schmidiger

Abstract

With unmanned vehicles, there are always on-board and off-board components. Data transmission between those components is of vital importance. Depending on the distance between vehicle and ground station, different data transmission technologies are ideal. So far, each device was connected to a single modem and the data transmission technology used could not be switched during operation. In a previous project, a serial switch had been designed with four RS-232 interfaces that act as data input and output for devices and four RS-232 interfaces for transmitters and modems. This hardware is very flexible: data routing and transmission behavior is configurable by the user. The application running on the serial switch collects data from connected devices, puts it into a data package and sends it out via the configured transmitter. The corresponding second serial switch receives this package, extracts and verifies the payload, sends it out to the corresponding device and optionally sends an acknowledge back to the package sender.
A Teensy 3.2 development board has been used as a micro controller unit. The software was written in the Arduino IDE with the provided Arduino libraries. As the project requirements became more complex, the limit of only a serial interface available as a debugging tool became more challenging. In the end, the software ran with more than ten tasks and an overhaul of the complex structure was necessary.
This document describes the refactoring process of the previous project. In the scope of this work, an adapter board has been designed so the previous hardware could be used with the more powerful Teensy 3.5 development board and a hardware debugging interface. A new software concept for the Teensy 3.5 was developed and implemented.
The Teensy 3.5 is configured to run with FreeRTOS. The developed software uses the task scheduler and queues of the operating system to provide the same functionalities as the previous software for Teensy 3.2.
The new software concept for the Teensy 3.5 is easy to understand, maintainable and expandable. Even though the functionality of the finished project remains the same as in the first version with Teensy 3.2 and Arduino, a refactoring has been necessary. Now further improvements and extra functionalities can be implemented more easily as suggestions are given and issues are reported within this document.

Horw, January 2017 Stefanie Schmidiger

Summary

With unmanned vehicles, there are always on-board and off-board components. Data transmission between those components is of vital importance. Depending on the distance between vehicle and ground station, different data transmission technologies have to be used.
In a previous project, the hardware for a Serial Switch has been designed that features four RS-232 interfaces to connect data processing and generating devices and four RS-232 interfaces to connect modems for data transmission. The application running on the designed base board assembled data packages with the received data from its devices and sent those data packages out to the modems for transmission. The corresponding second Serial Switch received those data packages, checked them for validity and extracted the payload to send it out to its devices.
A Teensy 3.2 development board acted as the main micro controller. Teensies are small, inexpensive and powerful USB development boards for Arduino applications. The software developed was flexible and in its header files the user could configure individual baud rates for each RS-232 interface, data routing and the use of acknowledges for data packages for each modem side. The application was running with many tasks, was complex and not easy to debug because of no hardware debugging interface.
Then this follow up project was initiated with the aim of an application with better maintainability and expandability. The main requirement for this follow up project were the use of a more powerful micro controller with Free FROS as an operating system, the use of an SD card for a configuration file and data logging and a hardware debugging interface.
In the scope of this project, the Teensy 3.2 was replaced with a Teensy 3.5 development board, which featured an on-board SD card slot. The Teensy 3.5 was prepared for hardware debugging and an adapter board to use the new Teensy 3.5 with headers meant for the Teensy 3.2 was designed. This adapter board allowed the use of the same base board as was designed in the previous project.
For the Teensy 3.5 application, the concept with data packages is applied as well and the same configuration parameters are used. The configuration is read from an .ini file saved on the SD card.
The functionality of the application remains the same as in the Teensy 3.2 software but with better maintainability and an easier software concept with less tasks. Hardware debugging is now possible which is of vital importance for this application to be further expandable.
The Teensy 3.2 application was neither well documented nor running stable. While the Teensy 3.5 application provides the same functionalities as the previous software, all its issues are documented and possible workarounds are suggested. Data handling and data loss in case of unreliable data transmission channel is handled better and the application is running stable.

Table of Contents

1 Introduction

This work is being done for Aeroscout GmbH, a company that specialized in development of drones. With unmanned vehicles, there are always on-board and off-board components. Data transmission between those components is of vital importance. Depending on the distance between on-board and off-board components, different data transmission technologies have to be used.
So far, each device that generates or processes data was directly connected to a modem. This is fine while the distances between on-board and off-board components does not vary significantly. But as soon as reliable data transmission is required both in near field and far field, the opportunity of switching between different transmission technologies is vital. When data transmission with one modem becomes unreliable, an other transmission technology should be used to uphold exchange of essential information such as exact location of the drone.
The goal of this project is to provide a flexible hardware that acts as a switch between devices and modems. Data routing between all connected devices and modems should be configurable and data priority should be taken into account when transmission becomes unreliable.
It should be possible to transmit the same data over multiple modems to reduce the chance of data loss for vital information. At receiving side, this case should be handled so the original information can be reassembled correctly with the duplicated data received. In case of data loss or corrupted data, a resend attempt should be started.
The configuration should be read from a file on an SD card. This SD card should also be used to store logging data. The system should run with Free RTOS and have a command/shell interface. When no devices are connected, the Free RTOS should go into low power mode.
Data loss should be handled and encryption and interleaving should be implemented for data transmission.
A hardware should be designed that is ready for field, with a good choice of connectors, small and light weight.

It was not necessary to start from scratch for this project. Andreas Albisser has already developed a hardware with four RS-232 interfaces to connect different data generating and processing devices and four RS-232 interfaces to connect modems. As a micro controller he used the Teensy 3.2, a small, inexpensive and yet powerful USB development board that can be used with the Arduino IDE.
Andreas Albisser also developed a software for the designed UAV Serial Switch base board. The software concept implemented became more complex as the requirements were expanded during development. The finished product did not fulfill all requirements of Aeroscout GmbH. Therefore this follow up project was initiated with new requirements and the hope of a better and easier expandable software as an outcome.
Not all requirements can possibly be implemented within one semester, but good ground work should be provided for further modifications and expansions.
Because encryption requires a more powerful micro controller than has been used by Andreas Albisser, some hardware modifications are required in the scope of this project. The most profund change is the micro controller and usage of Free RTOS. This will therefore be the main focus inside the project. The aim is to have a stable application with at least as many features and working configuration parameters as the old software had.
Some requirements demand hardware changes on the base board so an evaluation needs to be done inside this project to decide how to proceed and where to invest time.
A detailed task description can be found in chapter two. An overview and critical analysis of the

hardware and software provided by Andreas Albisser is in chapter three. In chapter four, all hardware changes that have been done in the scope of this project are described, followed by chapter four with a description of the software developed. Chapter six is for the conclusion and lessons learned.

2 Task Description

This project has been done for the company Aeroscout GmbH. Aeroscout specialized in the development of drones for various needs.
With unmanned aerial vehicles, the communication between on-board and off-board devices is essential and a reliable connection for data transmission is necessary. While the drone is within sight of the control device, data can be transmitted over a wireless connection. With increasing distances, other means of transmission have to be selected such as GPRS or even satellite.
So far, the switching between different transmission technologies could not be handled automatically. The data stream was directly connected to a modem and transmitted to the corresponding receiver with no way to switch to an other transmission technology in case of data transmission failure. A visualization of this set up can be seen in Figure 2.1. In the previous project, a flexible platform was developed that acted as a serial switch with multiple input and output interfaces for connecting devices and transmitters. See a sample setup in Figure 2.2. The hardware has four UART interfaces for devices such as sensors and actors and four UART interfaces for modems. The software developed provides basic functionalities such as routing data between devices and modems and retransmission in case of data loss. The application was still in its first stage but mostly running stable and working correctly.
In the scope of this project, the software should first be refactored and all pending points that are necessary for further development should be implemented. The main goal of this project is to implement two more key features: Reliability and security. Both are elaborated in more detail below.

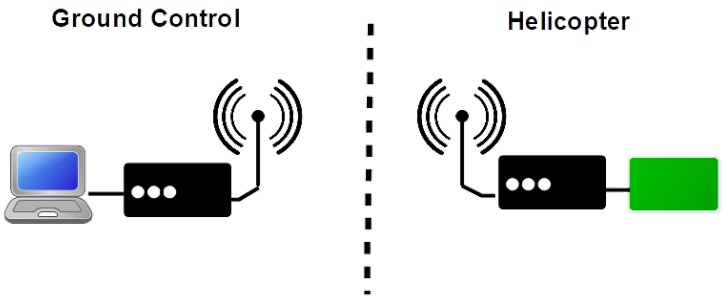

Figure 2.1: Previous system setup for data transmission

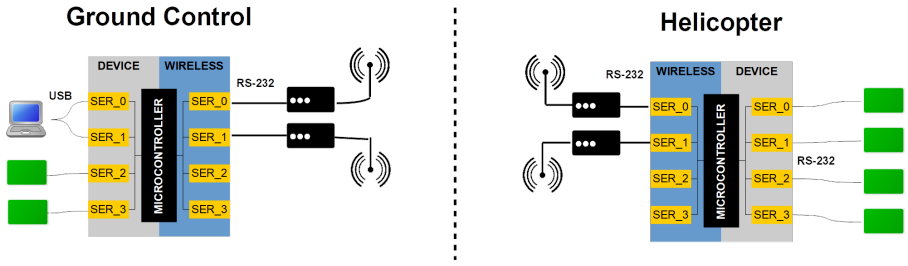

Figure 2.2: New system setup for data transmission

Reliability

Because unmanned aerial vehicles constantly change their position, transmission is not always reliable. About 10% - 20% of the transmitted data are lost and the transmitted data might be corrupted due to interference. The application developed in the scope of this project should take this into account and ensure a reliable data stream as well as implement an error correcting code.

Security

Data communication between the two serial switches should not be interceptable. A suitable encryption algorithm needs to be chosen that requires little computational power and little additional data transfer. A solution for encryption key generation and encryption key storage should be found.
Additionally, data transfer between the two serial switches should be logged, similar to the blackbox concept known from aviation. To ensure that the logged data cannot be tempered with unnoticed, the application should implement some sort of authenticity certificate to the log files.

3 Software Refactoring

In the scope of a previous project, the basic functionality of the Serial Switch was implemented.

3.1 Logging

3.2 Throughput Limitation

3.3 CRC

3.4 Debug Output

3.5 Package Reordering

4 System Analysis

Before expanding the application and implementing more features, the system performance needs to be analyzed to ensure sufficient capacity for error correcting codes and encryption.
In the previous project, SEGGER SystemView was used to analyze the runtime behavior and CPU load of each task.
SEGGER SystemView is a real-time recording and visualization tool for embedded systems that reveals information about runtime behavior of an application. SystemView can track down inefficiencies and show unintended interactions and resource conflicts.[12].
In the scope of this project, Percepio Tracealyzer was used instead of SEGGER SystemView because it provides a more in-depth insight into the runtime behavior of the software. The Tracealyzer not only shows the task execution times and RTOS events, it also shows this information in interconnected views and collects data about the CPU load and memory usage.
There is both a Processor Expert component for the SEGGER SystemView and one for Percepio Tracelyzer. These components are configured and enabled so that the corresponding code is generated. To use either one of these components, they have to be enabled in the FreeRTOS Processor Expert component. Only then will the debugger provide runtime information to the correct tool.

4.1 SEGGER SystemView

The application developed in the scope of this project runs with four main tasks that perform the main functionality of the software. Task intercommunication is done with queues, where one task always pushes data to a queue and another task pops this data from the queue to process it. This results in thousands of queue operations each second when the UAV Serial Switch is busy.
Queue operations are part of the FreeRtos. Because SystemView logs all FreeRtos calls, the additional traffic caused by SystemView when the software is already working to capacity can cause the application to crash. This can be prevented by disabling the logging of queue operations for SystemView. Simply comment the following code lines out in the file SEGGER_SYSTEM_VIEW_FreeRTOS.h (can be found in the GeneratedCode folder):

```
1 //#define traceQUEUE_PEEK( pxQueue )
      SYSVIEW_RecordU32x4(apiID_OFFSET + apiID_XQUEUEGENERICRECEIVE,
      SEGGER_SYSVIEW_ShrinkId((U32)pxQueue), SEGGER_SYSVIEW_ShrinkId((U32)pvBuffer),
      xTicksToWait, xJustPeeking)
2 //#define traceQUEUE_PEEK_FROM_ISR( pxQueue )
      SEGGER_SYSVIEW_RecordU32x2(apiID_OFFSET + apiID_XQUEUEPEEKFROMISR,
      SEGGER_SYSVIEW_ShrinkId((U32)pxQueue), SEGGER_SYSVIEW_ShrinkId((U32)pvBuffer))
3 //#define traceQUEUE_PEEK_FROM_ISR_FAILED( pxQueue )
      SEGGER_SYSVIEW_RecordU32x2(apiID_OFFSET + apiID_XQUEUEPEEKFROMISR,
      SEGGER_SYSVIEW_ShrinkId((U32)pxQueue), SEGGER_SYSVIEW_ShrinkId((U32)pvBuffer))
4 //#define traceQUEUE_RECEIVE( pxQueue )
      SYSVIEW_RecordU32x4(apiID_OFFSET + apiID_XQUEUEGENERICRECEIVE,
      SEGGER_SYSVIEW_ShrinkId((U32)pxQueue), SEGGER_SYSVIEW_ShrinkId((U32)pvBuffer),
      xTicksToWait, xJustPeeking)
5 //#define traceQUEUE_RECEIVE_FAILED( pxQueue )
      SYSVIEW_RecordU32x4(apiID_OFFSET + apiID_XQUEUEGENERICRECEIVE,
      SEGGER_SYSVIEW_ShrinkId((U32)pxQueue), SEGGER_SYSVIEW_ShrinkId((U32)pvBuffer),
      xTicksToWait, xJustPeeking)
```

```
6  //#define traceQUEUE_RECEIVE_FROM_ISR( pxQueue )
       SEGGER_SYSVIEW_RecordU32x3(apiID_OFFSET + apiID_XQUEUERECEIVEFROMISR,
       SEGGER_SYSVIEW_ShrinkId((U32)pxQueue), SEGGER_SYSVIEW_ShrinkId((U32)pvBuffer), (U32)
       pxHigherPriorityTaskWoken)
7  //#define traceQUEUE_RECEIVE_FROM_ISR_FAILED( pxQueue )
       SEGGER_SYSVIEW_RecordU32x3(apiID_OFFSET + apiID_XQUEUERECEIVEFROMISR,
       SEGGER_SYSVIEW_ShrinkId((U32)pxQueue), SEGGER_SYSVIEW_ShrinkId((U32)pvBuffer), (U32)
       pxHigherPriorityTaskWoken)
8  #define traceQUEUE_REGISTRY_ADD( xQueue, pcQueueName )
       SEGGER_SYSVIEW_RecordU32x2(apiID_OFFSET + apiID_VQUEUEADDTOREGISTRY,
       SEGGER_SYSVIEW_ShrinkId((U32)xQueue), (U32)pcQueueName)
9  #if ( configUSE_QUEUE_SETS != 1 )
10 // #define traceQUEUE_SEND( pxQueue )
       SYSVIEW_RecordU32x4(apiID_OFFSET + apiID_XQUEUEGENERICSEND, SEGGER_SYSVIEW_ShrinkId((
       U32)pxQueue), (U32)pvItemToQueue, xTicksToWait, xCopyPosition)
11 #else
12 #define traceQUEUE_SEND( pxQueue )                                    SYSVIEW_RecordU32x4(
       apiID_OFFSET + apiID_XQUEUEGENERICSEND, SEGGER_SYSVIEW_ShrinkId((U32)pxQueue), 0, 0,
       xCopyPosition)
13 #endif
14 #define traceQUEUE_SEND_FAILED( pxQueue )                             SYSVIEW_RecordU32x4(
       apiID_OFFSET + apiID_XQUEUEGENERICSEND, SEGGER_SYSVIEW_ShrinkId((U32)pxQueue), (U32)
       pvItemToQueue, xTicksToWait, xCopyPosition)
15 //#define traceQUEUE_SEND_FROM_ISR( pxQueue )
       SEGGER_SYSVIEW_RecordU32x2(apiID_OFFSET + apiID_XQUEUEGENERICSENDFROMISR,
       SEGGER_SYSVIEW_ShrinkId((U32)pxQueue), (U32)pxHigherPriorityTaskWoken)
16 #define traceQUEUE_SEND_FROM_ISR_FAILED( pxQueue )
       SEGGER_SYSVIEW_RecordU32x2(apiID_OFFSET + apiID_XQUEUEGENERICSENDFROMISR,
       SEGGER_SYSVIEW_ShrinkId((U32)
```

The output of the SystemView will then not contain any information about queue events but only visualize task execution times and other FreeRtos calls.

4.2 Percepio Trace Analyzer

Just like the SEGGER SystemView, the Percepio Trace Analyzer logs all FreeRtos function calls, including queue operations. To prevent the application from crashing during high capacity due to the additional traffic caused by the Tracelyzer, logging of queue operations can be disabled. To do this, go to the Percepio Trace Processor Expert component and disable the inclusion of queue events.
The Percepio Trace component can log data in two ways:

– **Streaming mode:** All log data is transferred from the microcontroller to the Tracelyzer desktop application in real-time

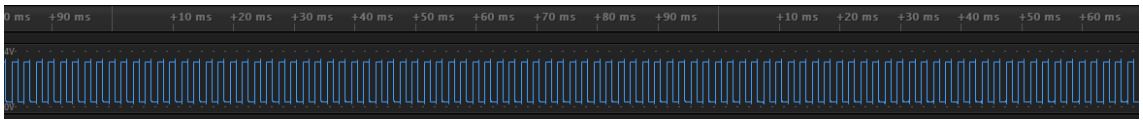

Figure 4.1: Periodic system ticks when Percepio disabled

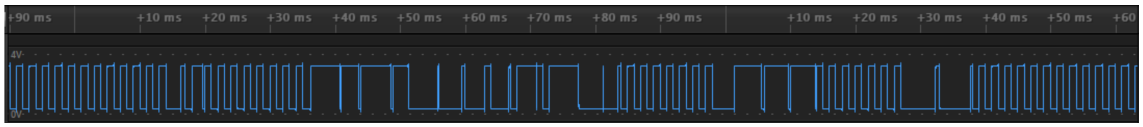

Figure 4.2: Irregular system ticks when Percepio enabled

– **Snapshot mode:** There is an on-board buffer that is filled with log data. This buffer can be imported into the Tracelyzer to analyze the performance of the application. No live streaming is possible.

When queue events are still included, the amount of data logged by the Tracelyzer has strong negative impacts the performance of the application. No matter if the Percepio Trace component is running in streaming mode or snapshot mode, the application cannot run correctly anymore when more than 1k Byte of data is exchanged between two Serial Switches.
During normal operation of the application, the FreeRtos is configured to generate a system tick event every millisecond. Inside the system tick event handler function, an output pin was toggled to verify periodic system ticks and correct FreeRtos execution. The code for the system tick event handler then looks as follows:

```
1 void FRTOS_vApplicationTickHook(void)
2 {
3     /* Called for every RTOS tick. */
4     TMOUT1_AddTick();
5     TmDt1_AddTick();
6     Pin33_NegVal(); /* toggle Pin 33  on Teensy */
7 }
```

While the Percepio Trace component was disabled, the system tick event was generated periodically every millisecond. This can be verified by looking at the toggling rate of Pin33 on the Teensy. The output was as seen in Figure 4.1.
When enabling tracing with Percepio by enabling it inside the FreeRtos Processor Expert component, the application was strongly overloaded with logging all queue events. This resulted in unregularities in the system tick events because of blocked FreeRtos calls. The output of Pin 33 on the Teensy can be seen in **??**. The above measurements have been done before the queue events could be disabled inside the Percepio Trace Processor Expert component. Whether disabling the logging of queue events can prevent irregular system ticks is to be evaluated. With enabled queue event logging, the application behavior was the same no matter if the Percepio Trace component was operating in streaming or snapshot mode.
Percepio Trace can therefore provide a good indicator for general system performance, task execution times and task intercommunication but is not ideal when lots of FreeRtos functions are used due to the additional traffic it generates.
Nevertheless, various inefficiencies were found with thanks to Percepio Trace and it provides good help with finding the cause of Hard Faults because the general area where the application stops is visible in streaming mode.

5 Modems

5.1 RF686x RFD900x

The RF686x is a long distance radio modem to be integrated into custom projects.
Its features include:

- 3.3V UART interface
- The RTS and CTS pins are available to the user
- 5V power supply, also via USB
- Default serial port settings: 57600 baud, no parity, 8 data bits, 1 stop bit
- MAVLink radio status reporting available (RSSI, remote RSSI, local noise, remote noise)
- The RFD900x has two antenna ports and firmware which supports diversity operation of antennas. During the receive sequence the modem will check both antennas and select the antenna with the best receive signal.
- There are three different communication architectures and node topologies selectable: Peer-to-peer, multipoint network and asynchronous non-hopping mesh.
- The RFD900x Radio Modem is compatible with many configuration methods like the AT Commands and APM Planner.
- Golay error correcting code can be enabled (doubles the over-the-air data usage)
- MAVLink framing and reporting can be turned on and off.
- Encryption level either off or 128bit

The 128bit AES data encryption may be set by AT command. The encryption key can be any 32 character hexadecimal string and less and must be set to the same value on both receiving and sending modems.

5.1.1 Peer to peer network

Abb: P2P
Peer to peer network is a straight forward connection between any two nodes. Whenever two nodes have compatible parameters and are within range, communication will succeed after they synchronize. If your setup requires more than one pair of radios within the same physical pace, you are required to set different network ID's to each pair.

5.1.2 Asynchronous non-hopping mesh

It is a straight foreward connection between two and more nodes. As long as all the nodes are within range and have compatible parameters, communication between them will succeed.

5.1.3 Multipoint network

Abb: P2MP, PTMP or PMP
In a multipoint connection, the link is between a sender and multiple receivers.

5.1.4 MAVLink

MAVLink or Micro Air Vehicle Link is a protocol for communicating with small unmanned vehicle. It is designed as a header-only message marshaling library. It is used mostly for communication between a Ground Control Station (GCS) and Unmanned vehicles, and in the inter-communication of the subsystem of the vehicle. It can be used to transmit the orientation of the vehicle, its GPS location and speed.

5.1.5 AT Commands

The AT Commands can be used to change parameters such as power levels, air data rates, serial speeds etc.
The AT command mode can be entered by using the '+++' sequence in a serial terminal connected to the radio. When doing this, you must allow at least 1 second after any data is sent out to be able to enter the command mode. This prevents the modem to misinterpret the sequence as data to be sent out.
The modem will reply with 'OK' as a feedback to the user. Then commands can be entered to set or get modem and transmission parameters such as RSSI signal report.

5.1.6 SiK

A SiK Telemetry Radio is a small, light and inexpensive open source radio platform that typically allows ranges of better than 300m "out of the box" (the range can be extended to several kilometres with the use of a patch antenna on the ground). The radio uses open source firmware which has been specially designed to work well with MAVLink packets and to be integrated with the Mission Planner, Copter, Rover and Plane.
SiK radio is a collection of firmware and tools for telemetry radios.
Hardware for the SiK radio can be obtained from various manufacturers/stores in variants that support different range and form factors. Typically you will need a pair of devices - one for the vehicle and one for the ground station.
A SiK Telemetry Radio is one of the easiest ways to setup a telemetry connection between your APM/Pixhawk and a ground station.
You can use the MAVLink support in the SiK Radios to monitor the link quality while flying, if your ground station supports it

5.2 ARF868URL

All information from datasheet:
ARF868 modem uses a packet oriented protocol on its RF interface. The data coming from the UART interface are accumulated in an internal fifo in the module and then encapsulated in an RF frame. The maximum amount of data that can be transferred into a single radio packet can reach 1024 Bytes.

The maximum packet size can be set up in S218 register from 1 to 1024 bytes. Each new packet introduces some latency in the transmission delay caused by the RF protocol overhead. The RF protocols encapsulate the data payload with the following elements:

– A preamble pattern required for receiver startup time
– A bit synchronization pattern to synchronize the receiver on the RF frame
– Other protocol field such as source address and destination address, payload length, optional CRC and internal packet type field.

The incoming fifo may accumulate up to 1024 data byte. No more data has to be set in the fifo while a 1024 bytes block of data has not been released by the radio transmission layer. To prevent from input fifo overrun, the hardware flow control may be activated. In this case, the RTS signal will be set when the incoming fifo is almost full to prevent the host controller from sending new data.
The user can configure the modem to run in non-secure packet mode where no acknowledges are sent out. The modem can also run in secure packet mode where acknowleges are expected and packages can be retransmitted two times before they are dropped.
RF protocol includes a 16 bit CRC. Each data extracted from an RF packet with an invalid CRC is silently discarded by the state machine module. The CRC ensures that all data received are valid. It can be disabled by the user whose protocols already have a control mechanism integrity or when some bug fixes user protocols are implemented.

5.2.1 RSSI

This modem can also transmit RSSI values

6 Channel Parametrization

Die wichtigste Eigenschaft eines Empfängers ist seine Empfindlichkeit. Bei digitalen Systemen wird sie über die Bitfehlerrate (BER) bestimmt.
Hierzu wird dem Empfänger ein Testsignal mit einer Pseudo-Random-Bitfolge und einem definierten Pegel zugeführt und an seinem Ausgang die Anzahl der Bitfehler gemessen. Das Grundprinzip der BER-Testmodi ist einfach: Der Funkmessplatz sendet einen Datenstrom an das Mobiltelefon, der vom diesem wieder zurückgesendet wird (Loop). Der Messplatz vergleicht gesendete und empfangene Datenströme und ermittelt daraus die Anzahl der Bitfehler. [1]

7 Error Correcting Codes

In information theory and coding theory with applications in computer science and telecommunication, error detection and correction or error control are techniques that enable reliable delivery of digital data over unreliable communication channels. Many communication channels are subject to channel noise, and thus errors may be introduced during transmission from the source to a receiver. Error detection techniques allow detecting such errors, while error correction enables reconstruction of the original data in many cases.
Common channel models include memory-less models where errors occur randomly and with a certain probability, and dynamic models where errors occur primarily in bursts. Consequently, error-detecting and correcting codes can be generally distinguished between random-error-detecting/correcting and burst-error-detecting/correcting. Some codes can also be suitable for a mixture of random errors and burst errors.
The general idea for achieving error detection and correction is to add some redundancy. Error-detection and correction schemes can be either systematic or non-systematic: In a systematic scheme, the transmitter sends the original data, and attaches a fixed number of check bits (or parity data), which are derived from the data bits by some deterministic algorithm. In a system that uses a non-systematic code, the original message is transformed into an encoded message that has at least as many bits as the original message.
The aim of encoding a message is to get the content to the recipient with minimal errors. The ground work for error detection and error correction methods has been done by Shannon in the 1940s. Shannon showed that every communication channel can be described by a maximal channel capacity with which information can be exchanged successfully. As long as the transmission rate is smaller or equal to the channel capacity, the transmission error could be arbitrarily small. When redundancy is added, possible errors can be detected or even corrected.
Generally, there are two ways to correct a faulty message once received:

- Foreward error correction
- Retransmission of the faulty message

Hier Bild einfügen von INKT Vorlesung: Info -> Encoder with Code Rate R -> Modulation -> Versand -> Empfang -> Demodulation -> Decoding -> Output

Block Codes and Convolution Codes

If the decoder only uses the currently received block of bits to decode the received message into an output, it is called an (n, k) block code with n being the number of output symbols and k the number of input symbols. Thereby, the last received block code does not matter for the decoding and is not stored. With convolutionary codes, the history of messages received is used to decode the next message.
Cyclic Codes
Cyclic codes are a subgroup of block codes. A random sequence of 1 and 0 are shifted to form other codes and inverted for even more codes. They can be represented as polynomes where the power of X represents the 1 in a sequence, starting with X^0 as the leftmost bit.
Systematic Block Codes
When the original information bits are unaltered and only accompanied by some redundancy such as CRC, the block code word is called systematic.

7.1 Error Detection

Error detection is most commonly realized using a suitable hash function (or checksum algorithm). A hash function adds a fixed-length tag to a message, which enables receivers to verify the delivered message by recomputing the tag and comparing it with the one provided. Example: CRC.

7.2 Error Correction

7.2.1 Automatic Repeat Request (ARQ)

ARQ is an error control method for data transmission that makes use of error-detection codes, acknowledgment and/or negative acknowledgment messages, and timeouts to achieve reliable data transmission. An acknowledgment is a message sent by the receiver to indicate that it has correctly received a data frame. Usually, when the transmitter does not receive the acknowledgment before the timeout occurs, it retransmits the frame until it is either correctly received or the error persists beyond a predetermined number of retransmissions.

7.2.2 Error Correcting Code

An error-correcting code (ECC) or forward error correction (FEC) code is a process of adding redundant data, or parity data, to a message, such that it can be recovered by a receiver even when a number of errors.
Error-correcting codes are usually distinguished between convolutional codes and block codes:

- Convolutional codes are processed on a bit-by-bit basis. They are particularly suitable for implementation in hardware, and the Viterbi decoder allows optimal decoding.
- Block codes are processed on a block-by-block basis. Examples of block codes are repetition codes, Hamming codes, Reed Solomon codes, Golay, BCH and multidimensional parity-check codes. They were followed by a number of efficient codes, Reed–Solomon codes being the most notable due to their current widespread use.

Reed Solomon

Reed Solomon is an error-correcting coding system that was devised to address the issue of correcting multiple errors, especially burst-type errors in mass storage devices (hard disk drives, DVD, barcode tags), wireless and mobile communications units, satellite links, digital TV, digital video broadcasting (DVB), and modem technologies like xDSL. Reed Solomon codes are an important subset of non-binary cyclic error correcting code and are the most widely used codes in practice. These codes are used in wide range of applications in digital communications and data storage.
Reed Solomon describes a systematic way of building codes that could detect and correct multiple random symbol errors. By adding t check symbols to the data, an RS code can detect any combination of up to t erroneous symbols, or correct up to [t/2] symbols. Furthermore, RS codes are suitable as multiple-burst bit-error correcting codes, since a sequence of b + 1 consecutive bit errors can affect at most two symbols of size b. The choice of t is up to the designer of the code, and may be selected within wide limits.
RS are block codes and are represented as RS (n, k), where n is the size of code word length and k is the number of data symbols, n – k = 2t is the number of parity symbols.

The properties of Reed-Solomon codes make them especially suited to the applications where burst error occurs. This is because

- It does not matter to the code how many bits in a symbol are incorrect, if multiple bits in a symbol are corrupted it only counts as a single error. Alternatively, if a data stream is not characterized by error bursts or drop-outs but by random single bit errors, a Reed-Solomon code is usually a poor choice. More effective cods are available for this case.
- Designers are not required to use the natural sizes of Reed-Solomon code blocks. A technique known as shortening produces a smaller code of any desired size from a large code. For example, the widely used (255,251) code can be converted into a (160,128). At the decoder, the same portion of the block is loaded locally with binary zero s.
- A Reed-Solomon code operating on 8-bits symbols has $n = 2^8 - 1 = 255$ symbols per block because the number of symbol in the encoded block is $n = 2^m - 1$
- For the designer its capability to correct both burst errors makes it the best choice to use as the encoding and decoding tool.

GoLay

There are two types of Golay codes: binary golay codes and ternary Golay codes.
The binary Golay codes can further be devided into two types: the extended binary Golay code: G24 encodes 12 bits of data in a 24-bit word in such a way that any 3-bit errors can be corrected or any 7-bit errors can be detected, also called the binary (23, 12, 7) quadratic residue (QR) code.
The other, the perfect binary Golay code, G23, has codewords of length 23 and is obtained from the extended binary Golay code by deleting one coordinate position (conversely, the extended binary Golay code is obtained from the perfect binary Golay code by adding a parity bit). In standard code notation tis code has the parameters [23, 12, 7]. The ternary cyclic code, also known as the G11 code with parameters [11, 6, 5] or G12 with parameters [12, 6, 6] can correct up to 2 errors.

7.2.3 Hybrid

When both Foreward correction and automatic repeat requests are enabled, it is called hybrid. [4]

8 Information Security

Information security is the practice of preventing unauthorized access, use or modification of information [5]. It key concepts are:

- Integrity: The same data is received as was transmitted, it cannot be modified without detection.
- Confidentiality: Data can only be read by the intended receiver.
- Availability: All systems are functioning correctly and information is available when it is needed.

To ensure these key concepts, different measurements can be taken, such as:

- Authentication: A means for one party to verify another's identity, e.g. by entering a password
- Authorization: Process by which one party verifies that the other party has access permission
- Encryption: Process of transforming data so that it is unreadable by anyone who does not have a decryption key

A mathmatical way to demonstrate authenticity and integrity of data is by using a digital signature. Each of these terms is elaborated in more details in the following sections.

8.1 Authentication

In information security, to verify if the data provider really is the one intended source, respectively if the data recepient really is the intended recepient

8.2 Authorization

8.3 Integrity

Integrity of data can be assured with a hash function. A hash is a string or number generated from a string of text. The resulting string or number is a fixed length, and will vary widely with small variations in input.
The only way to recreate the input data from an ideal cryptographic hash function's output is to attempt a brute-force search of possible inputs to see if they produce a match, or use a rainbow table of matched hashes. Therefore,hashing is a one-way function that scrambles plain text to produce a unique message digest.
A CRC is an example of a simple hash function and is used to check if the message received matches the message transmitted.
Integrity only does not provide security against tempering with the message itself. If someone knows the hash algorithm used, a message can be modified and its hash value recalculated without the receiver knowing about it.

8.4 Confidentiality

Encryption ensures that only authorized individuals can decipher data. Encryption turns data into a series of unreadable characters, that are not of a fixed length.
There are two primary types of encryption: symmetric key encryption and public key encryption.
In symmetric key encryption, the key to both encrypt and decrypt is exactly the same. There are numerous standards for symmetric encryption, the popular being AES with a 256 bit key.
Public key encryption has two different keys, one used to encrypt data (the public key) and one used to decrypt it (the private key). The public key is made available for anyone to use to encrypt messages, however only the intended recipient has access to the private key, and therefore the ability to decrypt messages.
Symmetric encryption provides improved performance, and is simpler to use, however the key needs to be known by both the systems, the one encrypting and the one decrypting data.

8.5 Availability

Availability of information refers to ensuring that authorized parties are able to access the information when needed.
Information only has value if the right people can access it at the right times.

8.6 Encryption

Information security uses cryptography to transform usable information into a form that renders it unusable by anyone other than an authorized user; this process is called encryption. Information that has been encrypted (rendered unusable) can be transformed back into its original usable form by an authorized user who possesses the cryptographic key, through the process of decryption. [10]

8.6.1 Encryption Algorithms Supported by Teensy 3.5

The Teensy 3.5 uses the ARM Coretex-M4 micro controller MK64FX512VMD12. In the MK64FX512xxD12 data sheet (see [3], p.1), it sais that this family supports hardware encryption such as DES, 3DES, AES, MD5, SHA-1, SHA-256. The supported encryption standards are elaborated in more detail in the following subsections.
There is a Crypto Acceleraction Unit (CAU) provided by NXP which is a encryption software library especially designed for the ARM Coretex-M4. The CAU is used for ColdFire and ColdFire+ devices while the mmCAU is for Kinetis devices (ARM Coretex-M4). For more information, consult the user guide and software API in [2].

DES

The Data Encryption Standard is a symmetric-key encryption algorithm developed in the early 1970s. It is now considered an insecure encryption standard and can be deciphered quickly, mostly due to its small key size (only 56 bit). [7] While the small key size was generally sufficient when the algorithm was designed, the increasing computational power made brute-force attacks feasible. [8]

3DES

The Triple Data Encryption Standard is a symmetric-key encryption algorithm which applies the DES cipher algorithm three times to each data block. Thereby, all three encryption keys can be identical or independent Theoretically, the resulting key length can be up to 3 x 56 bits = 168 bits. No matter if the keys are independent or identical, the resulting key has a shorter length due to vulnerability to different attacks. [8]

AES

The Advanced Encryption Standard is, just like the DES, a symmetric-key algorithm and has been established in 2001. It superseded the DES and is now one of the most widely used encryption protocols. Its key sizes can either be 128 bits, 192 bits or 256 bits. [6]

MD5

The MD5 algorithm is a widely used hash function producing a 128-bit hash value. Although MD5 was initially designed to be used as a cryptographic hash function, it has been found to suffer from extensive vulnerabilities. It can still be used as a checksum to verify data integrity, but only against unintentional corruption.
Like most hash functions, MD5 is neither encryption nor encoding. It can be cracked by brute-force attack and suffers from extensive vulnerabilities. [11]

SHA-1

The Secure Hash Algorithm 1 is a cryptographic hash function which takes an input and produces a 160-bit (20-byte) hash value as an output. Since 2005 SHA-1 has not been considered secure anymore and it is recommended to use SHA-2 or SHA-3 instead. [13]

SHA-256

The Secure Hash Algorithm 256 is, just like the SHA-1, a cryptographic hash function. It generates a fixed size 256-bit (32-byte) hash output.

8.7 Digital Signature

Digital signature is a mathematical scheme to demonstrate authenticity of a digital message. A valid digital signature gives a recipient reason to believe that the message was created by a known sender (authentication), that the sender cannot deny having sent the message (non-repudiation) and that the message was not altered in transit (integrity) [9].
A digital signature usually consists of three algorithms:

- Key generation algorithm: selects a random private key, outputs it and the corresponding public key.
- Signing algorithm: produces a signature when given a message and a private key.
- Signature verification: Verifies the authenticity of a message, when given the message, its signature and public key.

Non-repudiation can only be assured when an asymmetric encryption algorithm has been used, which means when the message was signed using a private key and can be verified using the corresponding public key. Symmetric encryption is not used for digital signatures because the sender and receiver are both in possession of the same key, therefore the receiver knows the scheme and cannot prove that

it has not been the creator of the message and its signature.

9 Conclusion

References

[1] "Bitfehlerraten-Messungen an GSM-Mobiltelefonen", in: *Neues von Rohde und Schwarz* 169 (2000), [20-Mar-2018, web page read], S. 11–13.

[2] Freescale, *ColdFire/ColdFire+ CAU and Kinetis mmCAU Software Library User Guide*, [10-Apr-2018, web page read], 2018.

[3] NXP, *Kinetis K64F Sub-Family Data Sheet*, [10-Apr-2018, web page read], 2017.

[4] *title*.

[5] Unknown, *Understanding Authentication, Authorization and Encryption*, [10-Apr-2018, web page read], 2018.

[6] Various, *Advanced Encryption Standard*, [10-Apr-2018, web page read], 2018.

[7] Various, *Data Encryption Standard*, [10-Apr-2018, web page read], 2018.

[8] Various, *Data Encryption Standard*, [10-Apr-2018, web page read], 2018.

[9] Various, *Digital Signature*, [11-Apr-2018, web page read], 2018.

[10] Various, *Information Security*, [11-Apr-2018, web page read], 2018.

[11] Various, *MD5*, [10-Apr-2018, web page read], 2018.

[12] Various, *SEGGER SystemView*, [24-Apr-2018, web page read], 2018.

[13] Various, *SHA-1*, [10-Apr-2018, web page read], 2018.

Abbrevations

ALOHA	System for coordinating access to a shared communication channel
COM port	Simulated serial interface on computer
GND	Ground reference, usually 0V
HSLU	Lucerne University of Applied Sciences and Arts
HW	Hardware
ISO/OSI	7 Layers Model
MCU	Micro Controller Unit
PC	Personal Computer
PCB	Printed Circuit Board
RS-232	Serial interface with +-12V
RTT	Real Time Transfer, Segger terminal
RTOS	Realtime Operating System
RX	Received signal
SPI	Serial Peripheral Interface, synchronous communication standard
SW	Software
SWD	Serial Wire Debug, hardware debugging interface
TX	Transmitted signal
TTL	Transistor Transistor Level, 5V level
UART	Universal Asynchronous Receiver Transmitter
UAV	Unmanned Aeral Vehicle
USB	Universal Serial Bus

Appendix A A

Lebenslauf

Personalien

Name	Stefanie Schmidiger
Adresse	Gutenegg 6125 Menzberg
Geburtsdatum	30.06.1991
Heimatort	6122 Menznau
Zivilstand	ledig

Ausbildung

August 1996 - Juli 2003	Primarschule, Menzberg
August 2003 - Juli 2011	Kantonsschule, Willisau
August 2008 - Juni 2009	High School Exchange, Plato High School, USA
August 2011 - Juli 2013	Way Up Lehre als Elektronikerin EFZ bei Toradex AG, Horw
September 2013 - Juli 2016	Elektrotechnikstudim Bachelor of Science Vertiefung Automation & Embedded Systems Hochschule Luzern - Technik & Architektur, Horw
Juli 2015 - Januar 2016	Austauschsemester, Murdoch University, Perth, Australien
September 2016 - jetzt	Elektrotechnikstudium Master of Science Hochschule Luzern - Technik & Architektur, Horw

Berufliche Tätigkeit

Juli 2003 - August 2003	Produktionsarbeiten bei Schmidiger GmbH, Menzberg
Juli 2004 - August 2004	Produktionsarbeiten bei Schmidiger GmbH, Menzberg
Juli 2005 - August 2005	Produktionsarbeiten bei Schmidiger GmbH, Menzberg
Juli 2006 - August 2006	Produktionsarbeiten bei Schmidiger GmbH, Menzberg
Juli 2007 - August 2007	Produktionsarbeiten bei Schmidiger GmbH, Menzberg
Juli 2009 - August 2009	Produktionsarbeiten bei Schmidiger GmbH, Menzberg
Juli 2010 - August 2010	Produktionsarbeiten bei Schmidiger GmbH, Menzberg
Juli 2014 - August 2014	Schwimmlehrerin bei Matchpoint Sports Baleares, Mallorca
September 2016 - jetzt	Entwicklungsingenieurin bei EVTEC AG, Kriens