FORSCHUNGSINITIATIVE
K O - F A S

Development of communication protocols for dynamic C2X networks

Entwicklung von Kommunikationsprotokollen für dynamische Car2x-Netzwerke

Prof. Dr.-Ing. Axel Sikora,
Manuel Schappacher, Simon Gutjahr
Steinbeis-Innovationszentrum Embedded Design & Networking

Supported by:

Federal Ministry of Economics and Technology

on the basis of a decision by the German Bundestag

Overview Work Packages

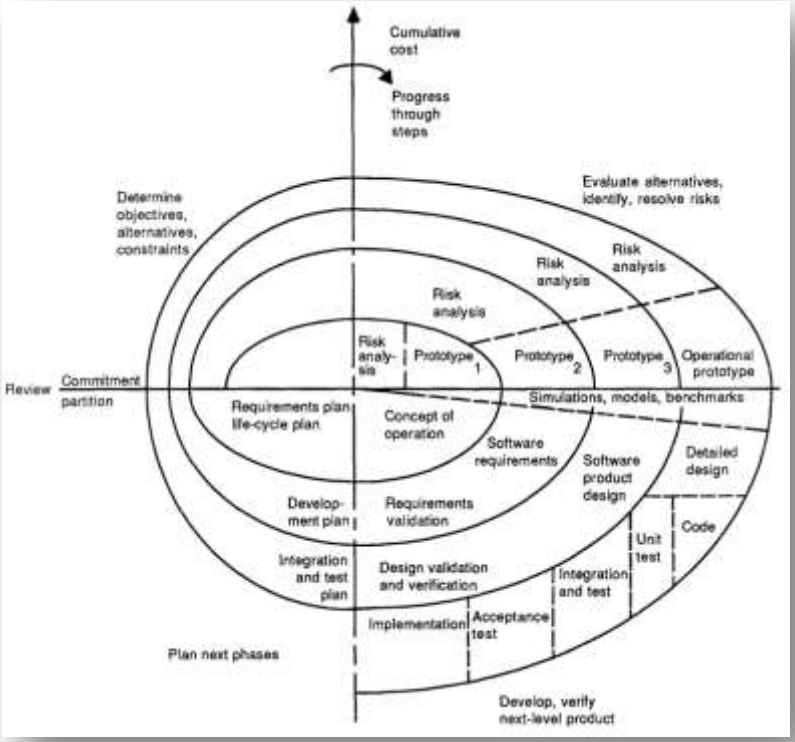
FORSCHUNGSINITIATIVE
K O - F A S

- **(1) design process & protocol specification**
- **(2) protocol integration and verification**:
  - (1) simulation
  - (2) emulation testbed
  - (3) monitoring tools
- **(3) security**: authentication, privacy, stability
- **(4) system & hardware design**:
  - (1) PCB for digital communication part
  - (2) system FPGA
  - (3) system integration

(1) design process & protocol specification
(1.1) design process

- development process following spiral development process

- specification
- simulation
- emulation
- field tests



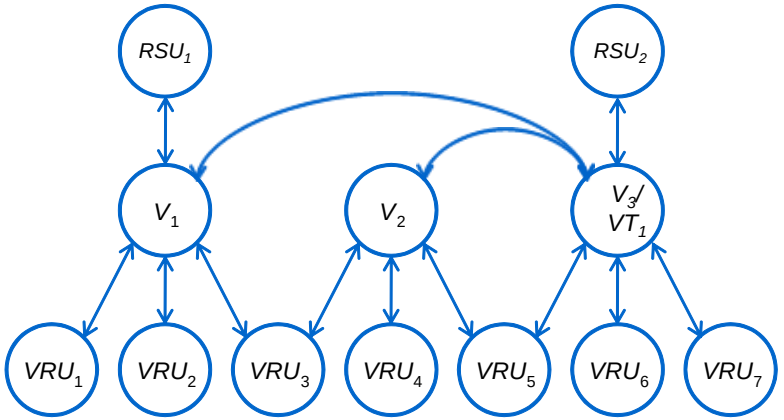
B.W. Boehm, "A Spiral Model of Software Development and Enhancement", IEEE Computer 1988, Vol. 21, No. 5, S. 61-72

(1) design process & protocol specification
(1.2) system architecture

FORSCHUNGSINITIATIVE
K O - F A S

- On Board Unit (OBU) built in vehicles consist of
  - A Localization Unit (LU) that communicates with SafeTAGs and is able to localize them (distance and angle measurements).
  - A Fusion Unit (FU) that reads measurement data from the LU and tracks objects. It reads in further sensor data e.g. from cameras to elaborate the tracking algorithms.

- SafeTAG can be
  - A Vulnerable Road User (VRU) such as a pedestrian or cyclist.
  - A Vehicle TAG (VT) to support pre-crash safety among vehicles.
  - A Road Side Unit (RSU) that gives an OBU the possibility of a precise self localization.



(1) design process & protocol specification
(1.3) system specification

FORSCHUNGSINITIATIVE
K O - F A S

- SafeTAG sends cyclic announcements
- OBU within communication range receives announcements and replies with a network ID that includes time slot information (further packets e.g. if assigned time slot is occupied)
- Cyclic ToF measurements during assigned time slot in the ToF channel
- SafeTAG sends sensor data on request during DoA/Data phases
- OBU estimates the angle of incoming data frames

→ **Endangerment level of the SafeTAG is determined using angle, distance and sensor data**

(1) design process & protocol specification
(1.3) system specification

FORSCHUNGSINITIATIVE
K O - F A S

Registration

- Observation of the management channel
- Reply to registration requests of the TAGs
- Assignment of addresses and time slots

AoA (Angle Measurement)/Data

- Transmission of a Request-Beacon
- Transmission of the replies by the addressed TAGs
- Angle Measurement of the arrived signal

ToF (Distance Measurement)

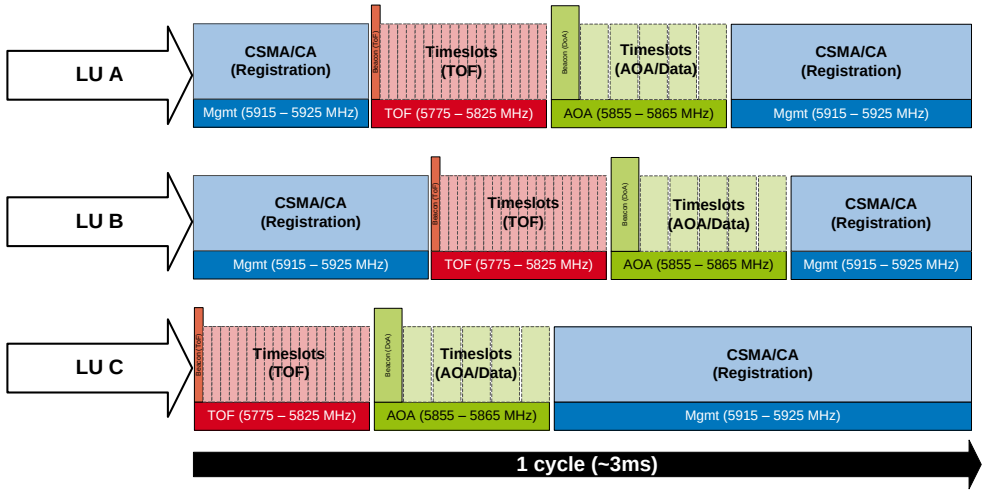
- Transmission of Beacons
- Time-Of-Flight Measurements for each TAG in its time slot
- Duration of a time slot < 15µs

(1) design process & protocol specification
(1.3) system specification

FORSCHUNGSINITIATIVE K O - F A S

Communication flow consists of 3 superframes in different channels

- Network Management
  - channel arbitration with a CSMA/CA algorithm
  - detection of new devices and connection establishments.
  - reconfiguration of connected devices
- Time of Flight (TOF) Measurements
  - 50 MHz bandwidth
  - time slots to provide a deterministic behaviour
  - time synchronisation driven by beacon

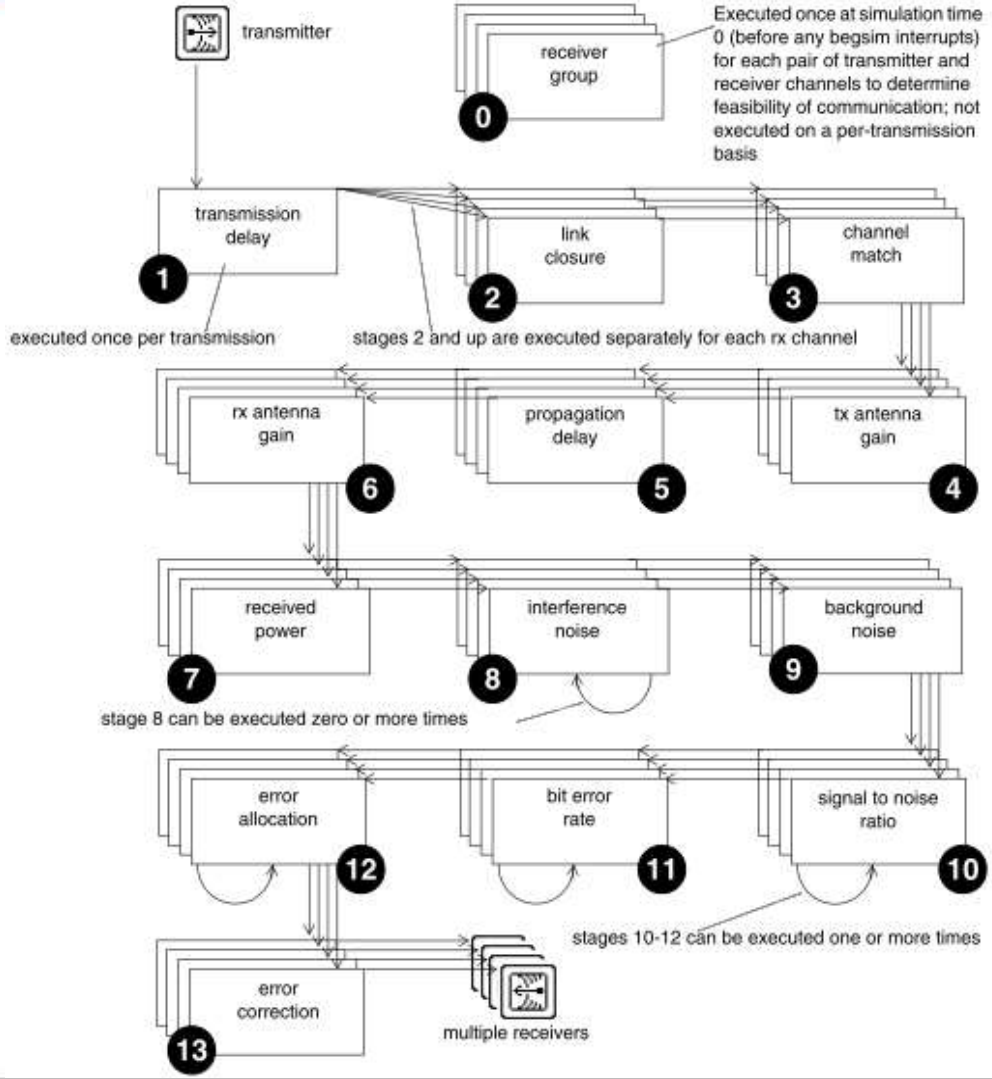


- Angle of Arrival (AOA) Measurements/Data
  - transmission of sensor data
  - angle measurements with 802.11p data frames
  - time slotted channel access
  - beacon driven phases. Beacon contains configuration of the following time slots

(2) protocol integration and verification
(2.1) network simulation

FORSCHUNGSINITIATIVE
K O - F A S

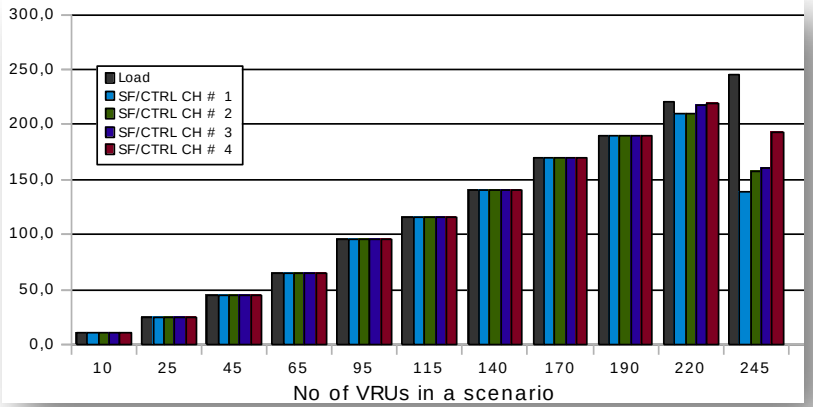
- network simulation with *OPNET Modeler 16*
  - close to real physical channel characteristics (data rate, bandwidth…)
  - definition of relevant scenarios and statistics to verify proposed protocol
  - node movement based on defined paths or on random
  - parameterization of network protocol



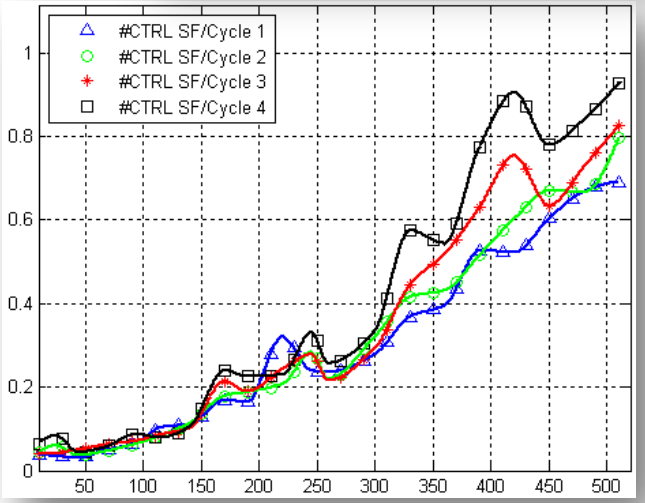
(2) protocol integration and verification
(2.1) network simulation

FORSCHUNGSINITIATIVE
K O - F A S

- simulation automation
  - scripting to automatically generate scenarios to generate statistical data
  - simulation server for long-term scenarios



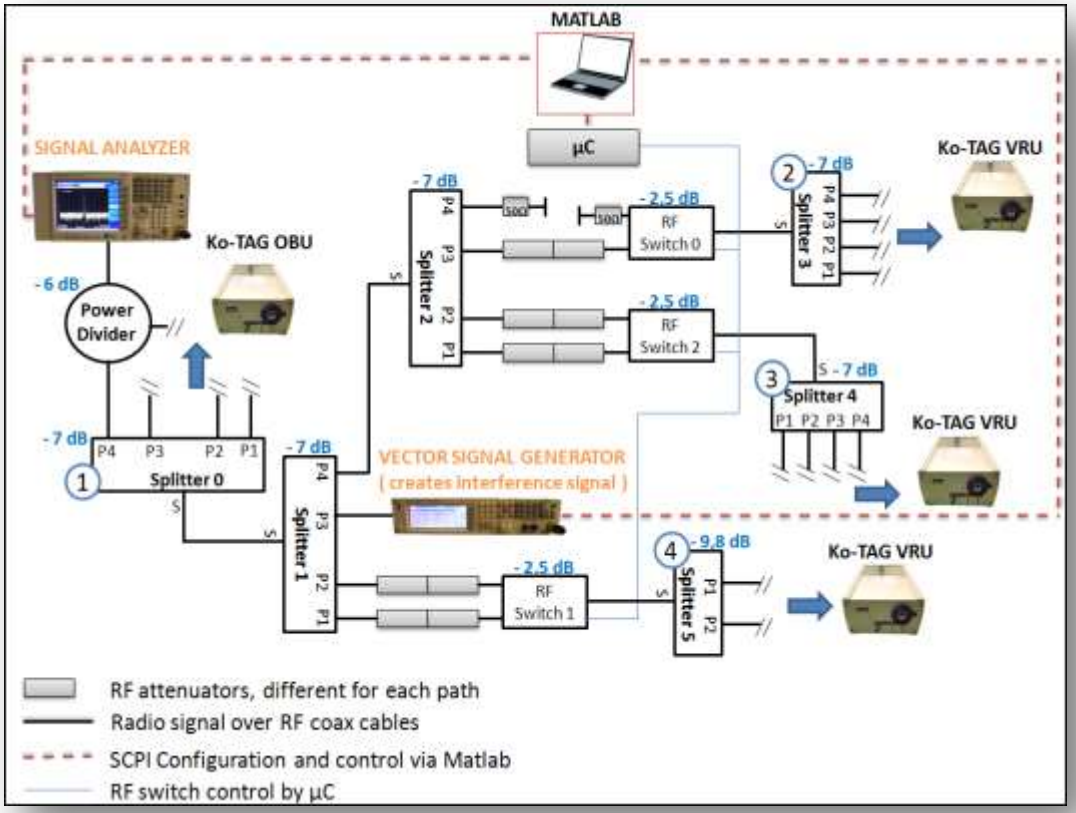
- statistical analysis using Matlab
  - automated presentation of *OPNET* simulation results
  - comparison & analysis



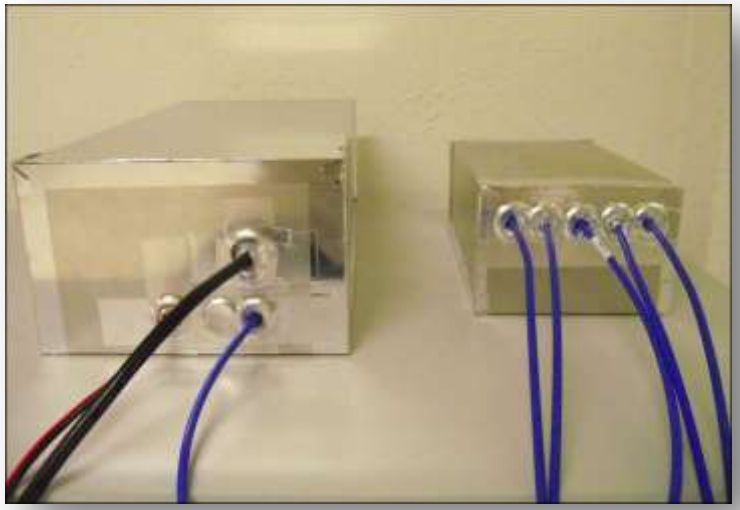
(2) protocol integration and verification
(2.2) emulation & testbed

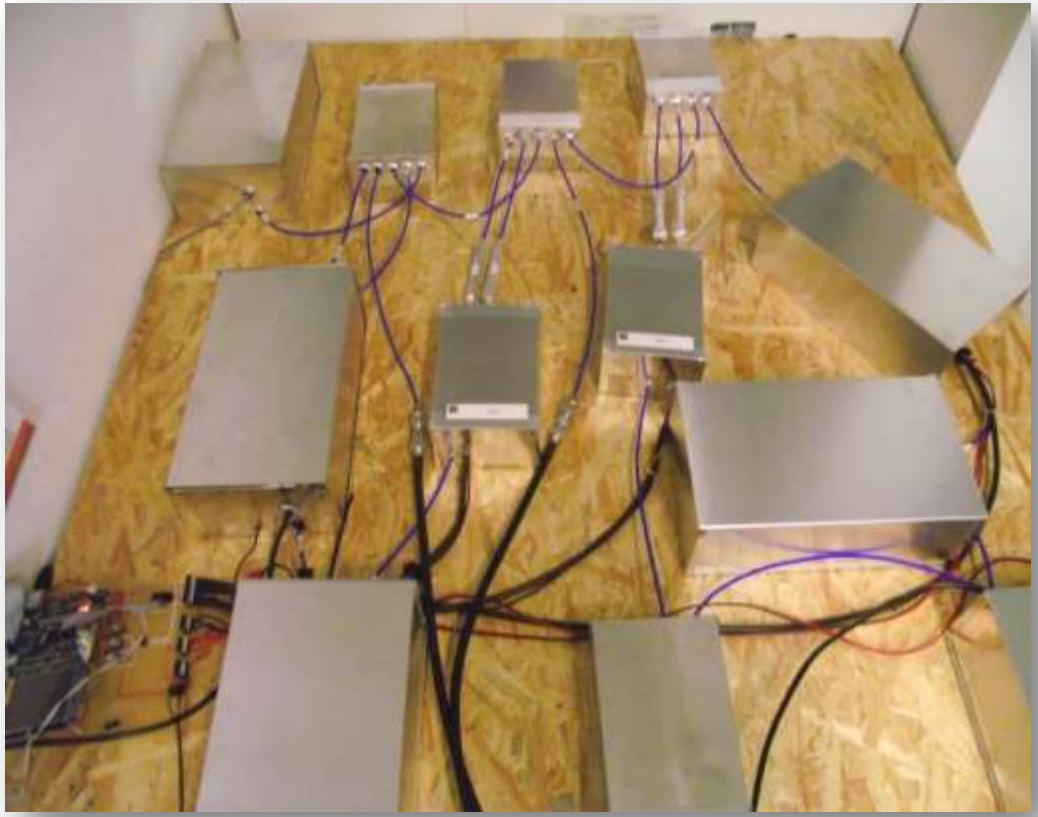
FORSCHUNGSINITIATIVE
K O - F A S

- objective: verify stability, compatibility and coexistence
- design of emulator / testbed



(2) protocol integration and verification
(2.3) emulation & testbed

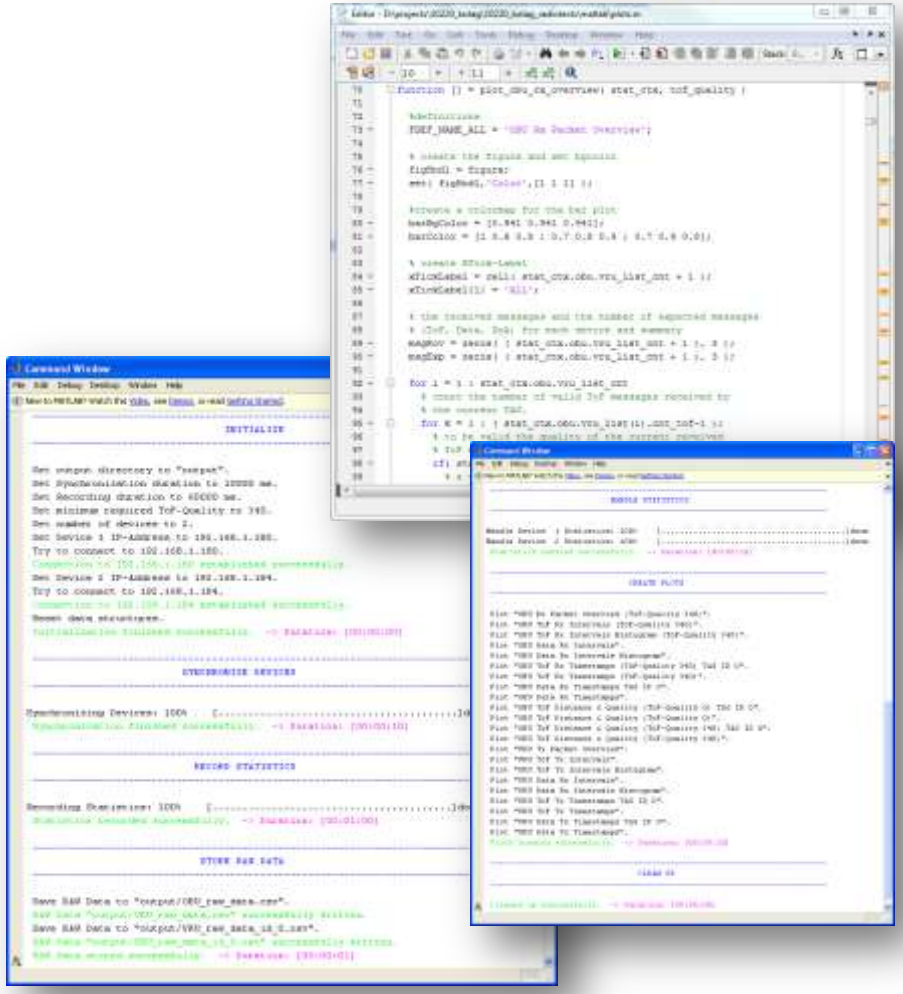




(2) protocol integration and verification
(2.3) emulation & testbed

FORSCHUNGSINITIATIVE
K O - F A S

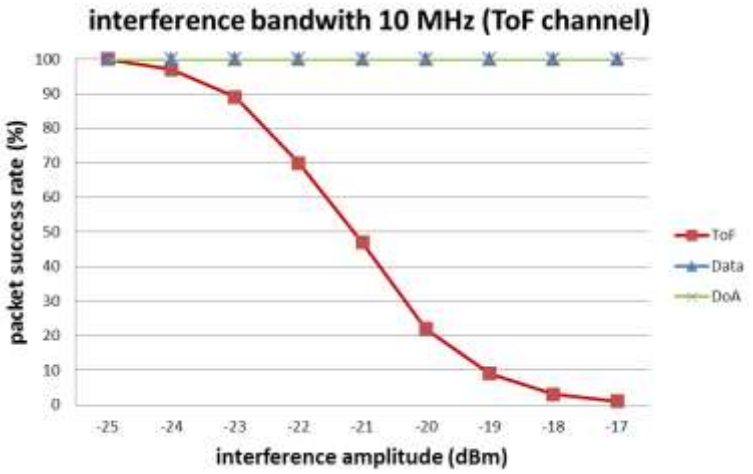
- automated measurements in MATLAB environment
  - Parameterisation of test cases
  - configuration and launch of devices
  - collection of measurement and statistical data
    - using extended firmware
- automated generation of pre-defined plots and tables

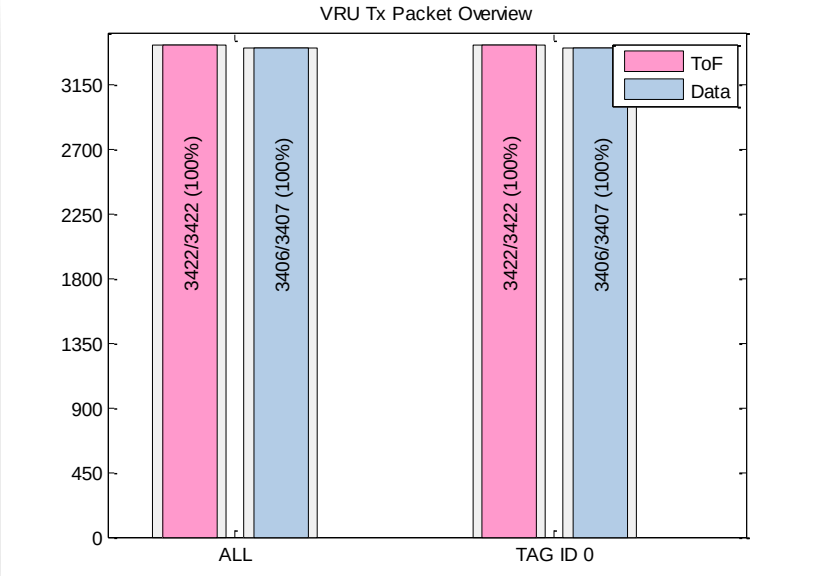


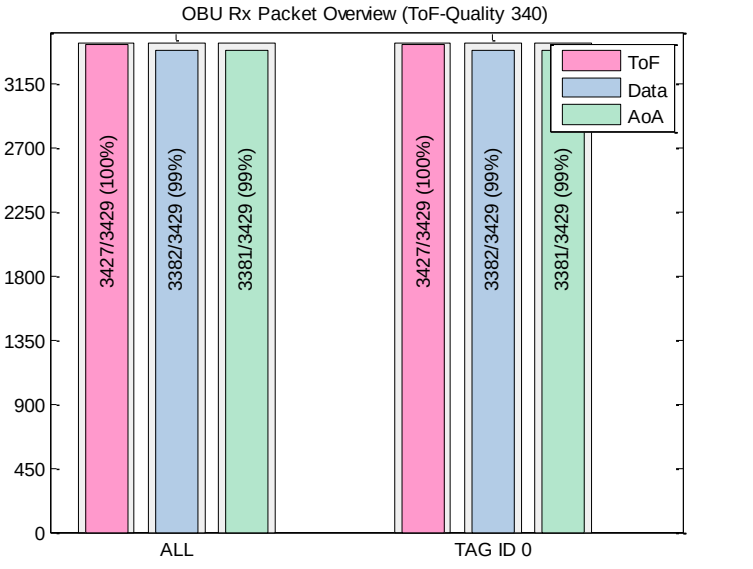
(2) protocol integration and verification
(2.2) emulation & testbed

FORSCHUNGSINITIATIVE
K O - F A S

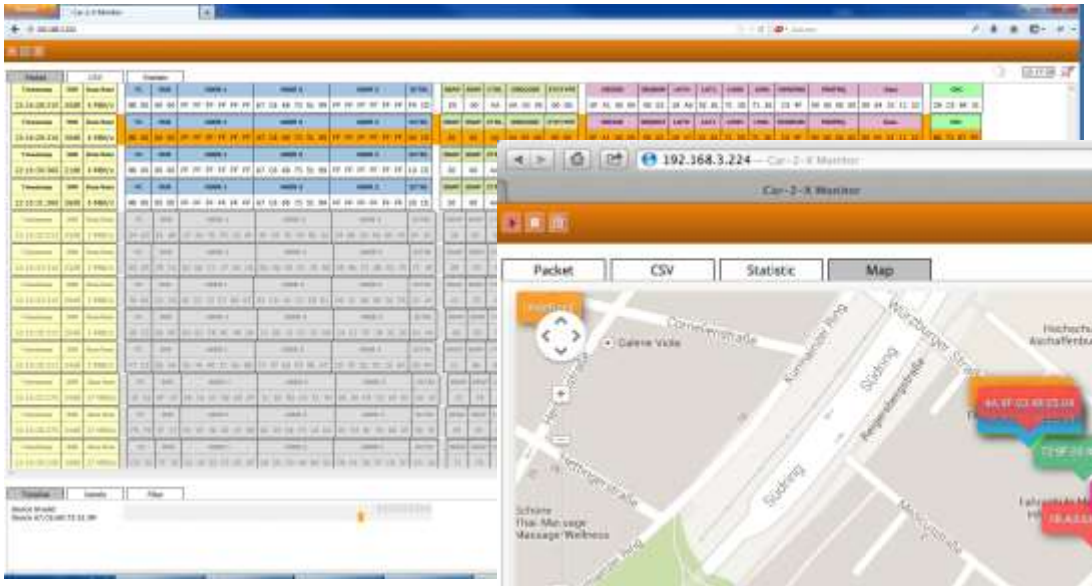
- example:
  communication with
  disturbed ToF channel

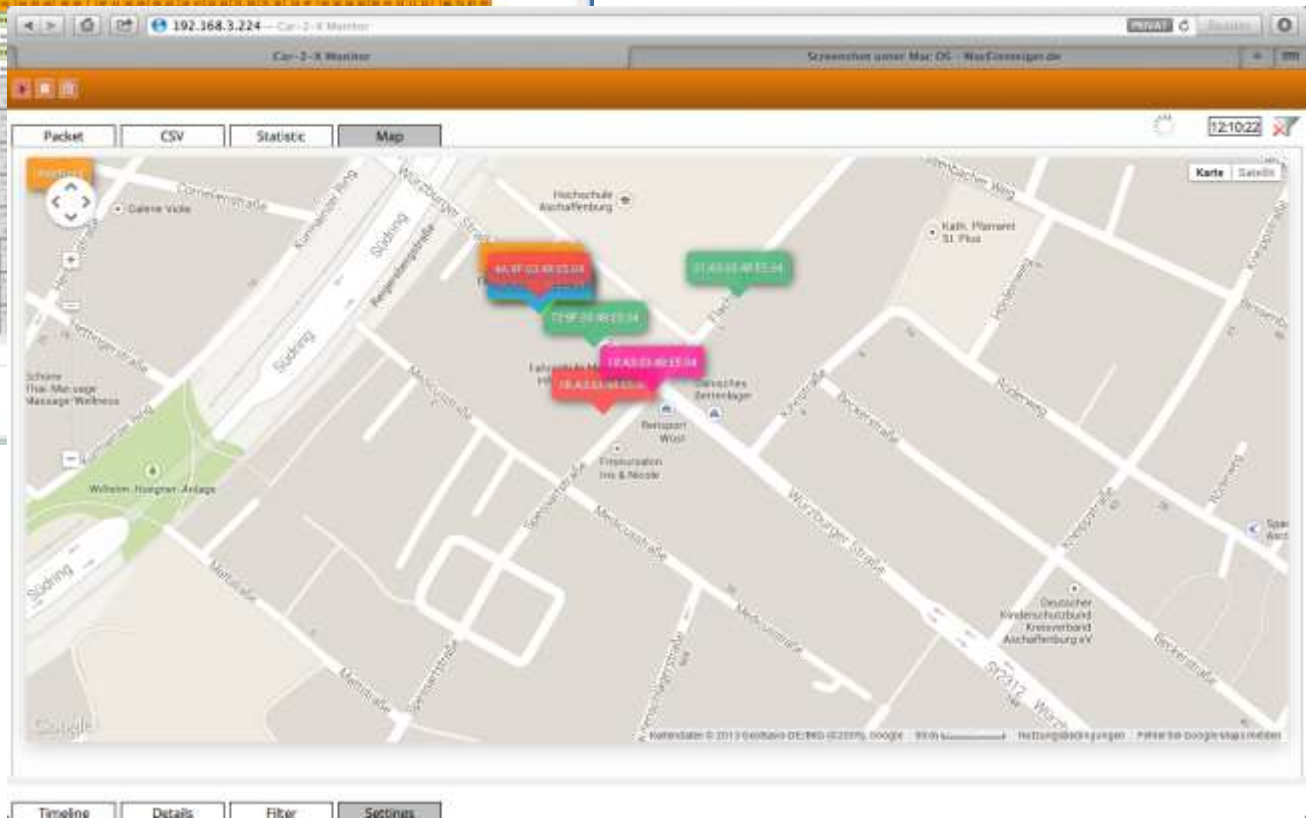






(2) protocol integration and verification
(2.3) tools



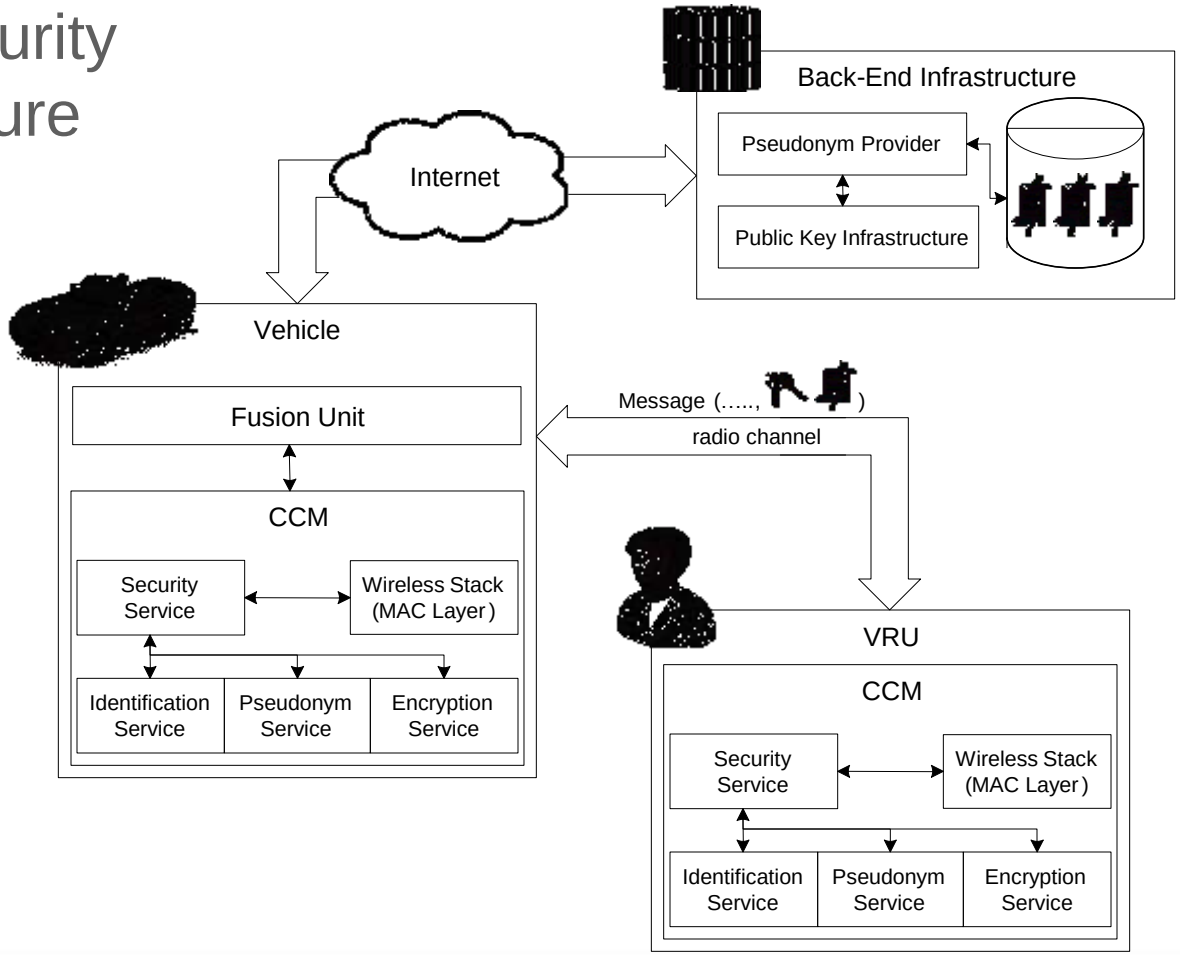


(3) Security & Safety
(3.1) Objectives

- security
  - confidentiality
  - authentication
  - integrity
  - no traceability of network nodes
  - unambiguous identification of anonymous nodes
- safety / functional safety
  - support hard real-time constraints
  - support all-around safety (RUS) in software
  - distinction between SafeTAGs and RUS-TAGs
- robustness
  - error detection using Cyclic Redundancy Checks (CRC)
  - plausibility check for detection of external attacks

(3) Security & Safety
(3.2) Architecture Elements

- concept and implementation of an integrated security and safety architecture



(3) Security & Safety
(3.3) Concepts

- multiple identities per participant
  - basic identity
    - one time identity for authentication at back-end server
  - pseudonym identity
    - continuously changing identities for authentication in wireless network

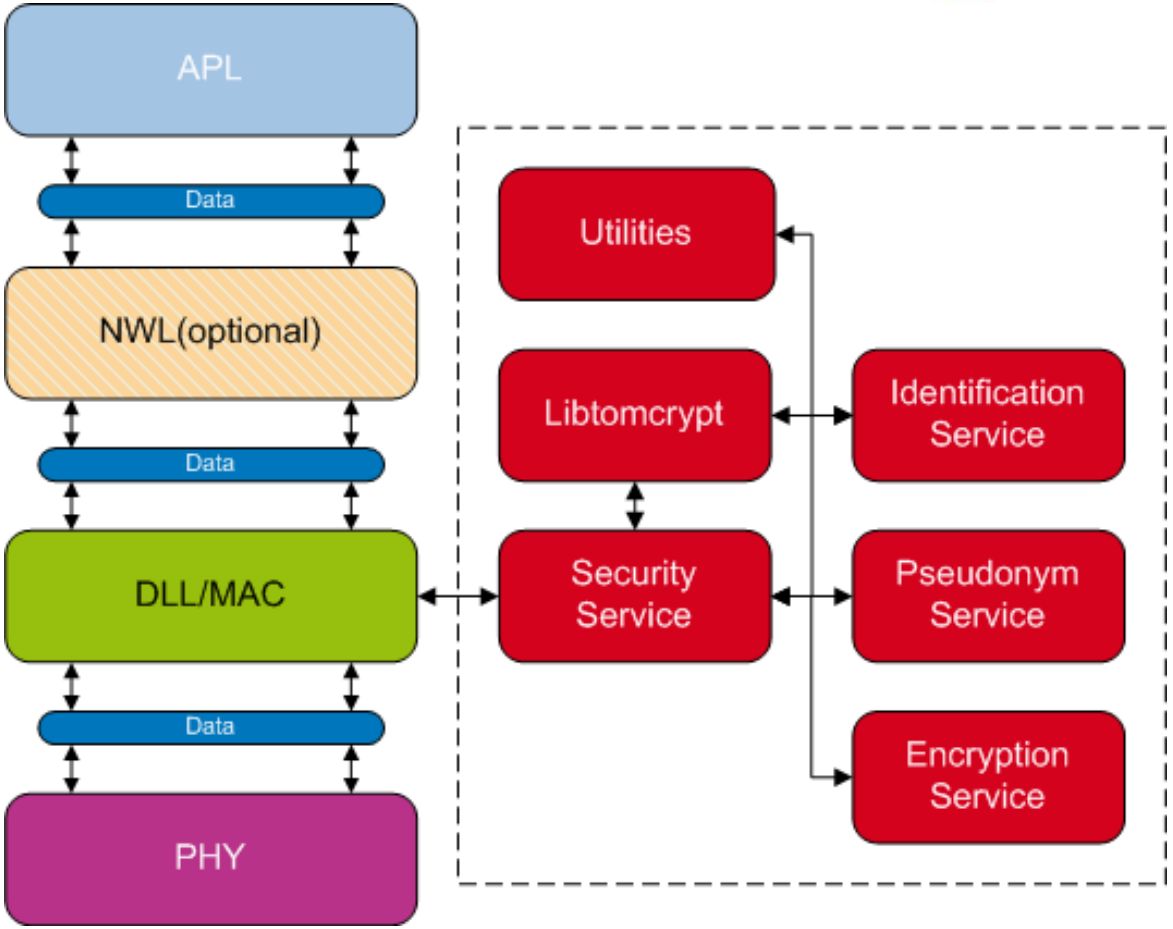
  ➢unambiguous identification of anonymous nodes
- public key infrastruktur / pseudonym provider
  - certificates according to IEEE 1609.2 standard for basic identity & pseudonyms
  - generation and distribution of certificates
  - assignment of pseudonyms to basic identity

(3) Security & Safety
(3.3) Concepts

- identification service
  - signing and verification of all RF messages
  - Elliptic Curve Digital Signature Algorithm (ECDSA) 256 Bit
- encryption service
  - symmetric encryption of all relevant RF messages
  - Advanced Encryption Standard (AES) 128 Bit
    - in hardware
- pseudonym service
  - application of new certificates (pseudonyms, basic identities) at PKI back-end

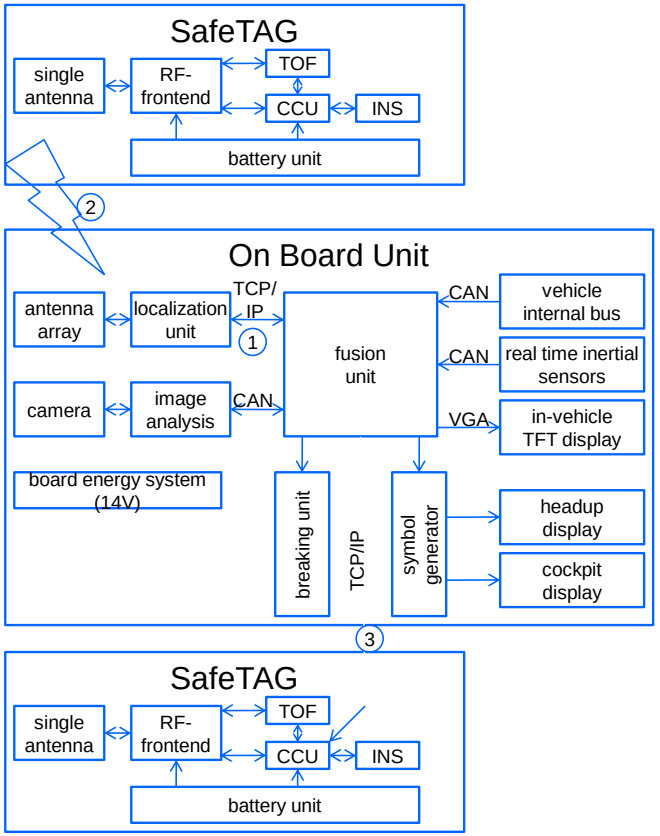
(3) Security & Safety
(3.4) Implementation

- Libtomcrypt
  - Open Source Library
- security service:
  - platform: FPGA NIOS2 and OPNET simulator
  - C
- Back-End infrastructure:
  - Windows application in C/C++



(4) Hardware Design

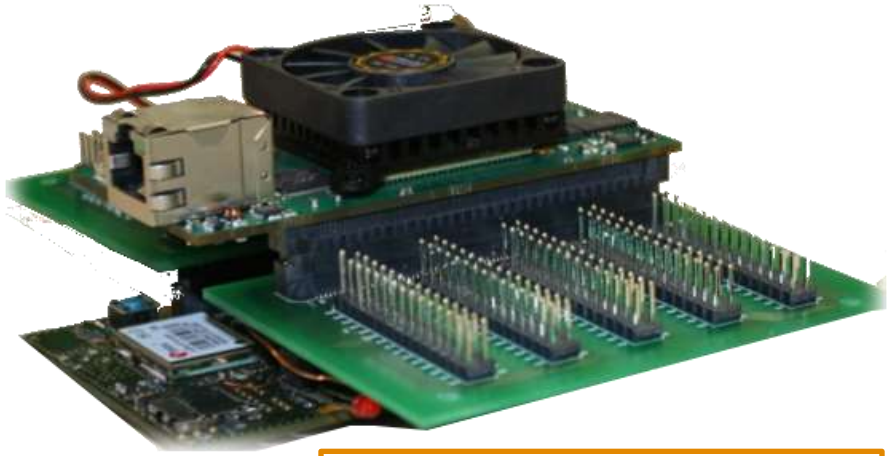
- overall architecture with modular OBU and TAG-approach



(4) Hardware Design
(4.1) PCB

- PCB Design of Altera Arria2GX Board
  - split of layout into FPGA board and base board
  - FPGA board contains FPGA and peripherals (memory, CPLD…)
  - base board for power distribution & Ko-TAG components (interfaces, reference clock, MCU …)
  - for future cost-optimized FPGA boards the base board can be re-used

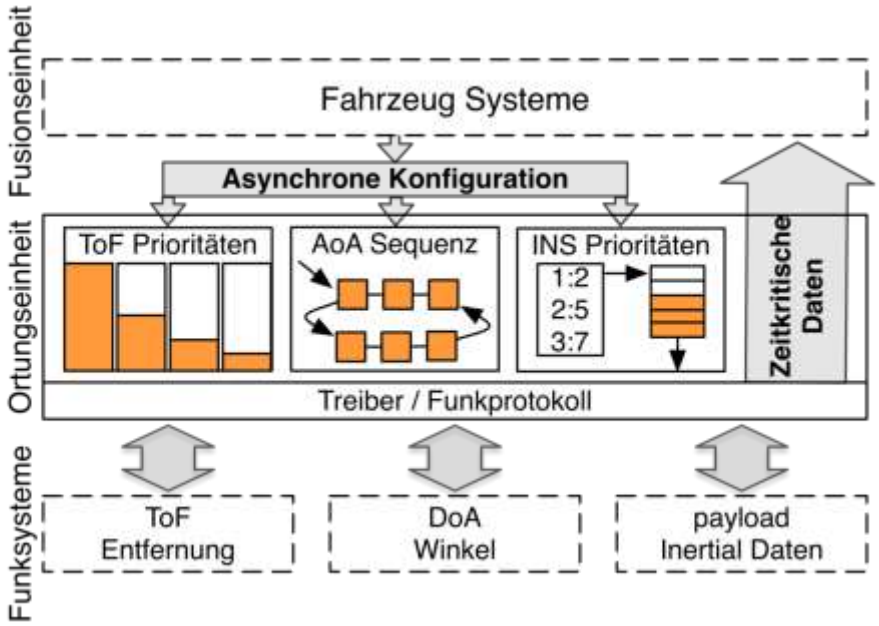
hardware platform (without FPGA)



modular PCB-stack with cooling fan and adaption board

(4) Hardware Design
(4.2) system FPGA

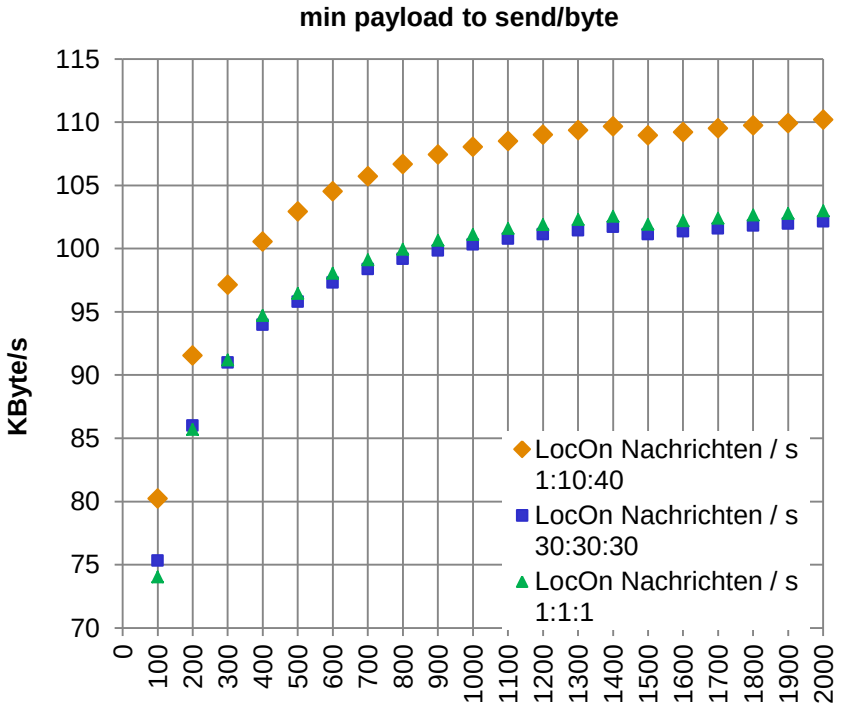
- abstraction of system complexity for fusion unit
  - LocON protocol for standardised exchange of localisation and data information
  - separation of asynchronous configuration from real-time data
  - autonomous administration of TDMA-time slots
  - arbitration of communication bandwidth depending on risk level per RUS-TAG and SafeTAG.
  - control and synchronisation of AoA functionality



(4) Hardware Design
(4.3) system integration

- Implementation of LocON protocol between localization and fusion units
  - basic implementation of LocON protocol as NIOS firmware
  - integration of own GBit-Ethernet MAC hardware
  - integration of own embedded TCP/IP stack
  - selection of optimum parameter for communication with fusion unit

data throughput depending on packet sizes at different packet elements: angle : data : distance



Thank you for your attention!

BMW Group
Forschung und Technik

DAIMLER

Continental

Fraunhofer IIS

Fraunhofer Heinrich-Hertz-Institut

Steinbeis-Innovationszentrum Embedded Design und Networking

Technische Universität München