FernUniversität in Hagen

Zur sicheren Vernetzung von Kraftfahrzeugen

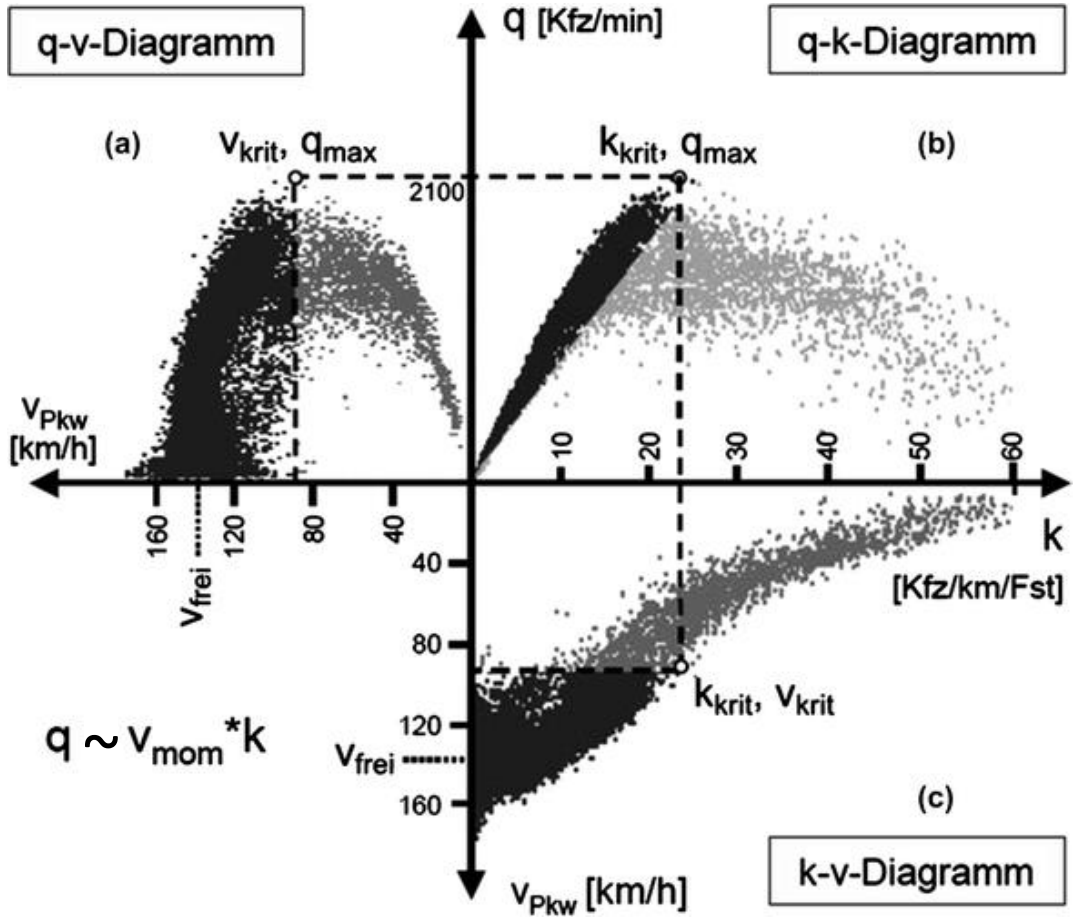
Christoph Maget

Problem

- Kapazitätsgrenze von Straßen erreicht oder überschritten
  - Stau
  - Zeitverluste
- Volkswirtschaftlicher Schaden
- Aus- und Neubau teuer bzw. langwierig

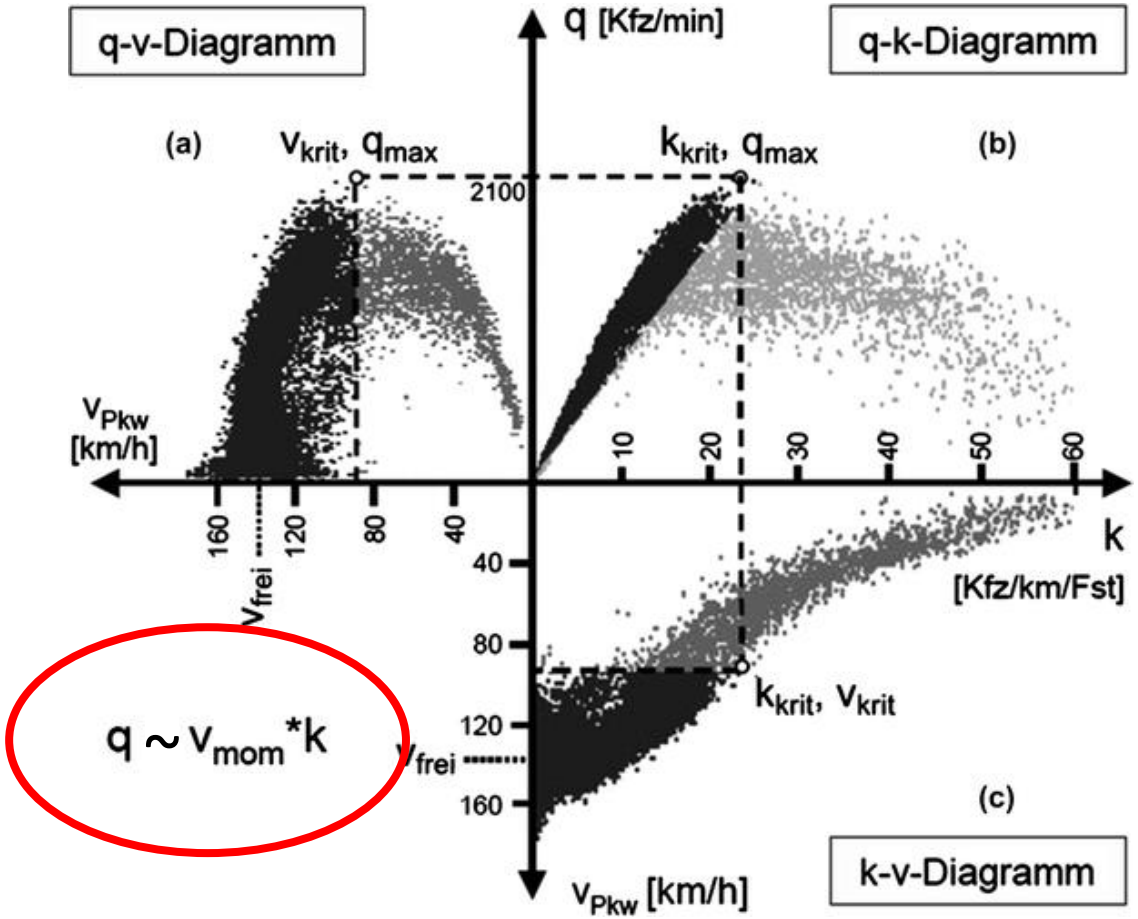
Hintergrund: Fundamentaldiagramm

- Zusammenhang zwischen
  - Kapazität q [Kfz/min]
  - Geschwindigkeit v [km/h]
  - Fahrzeugdichte k [Kfz/km]
    (~1/Abstand)



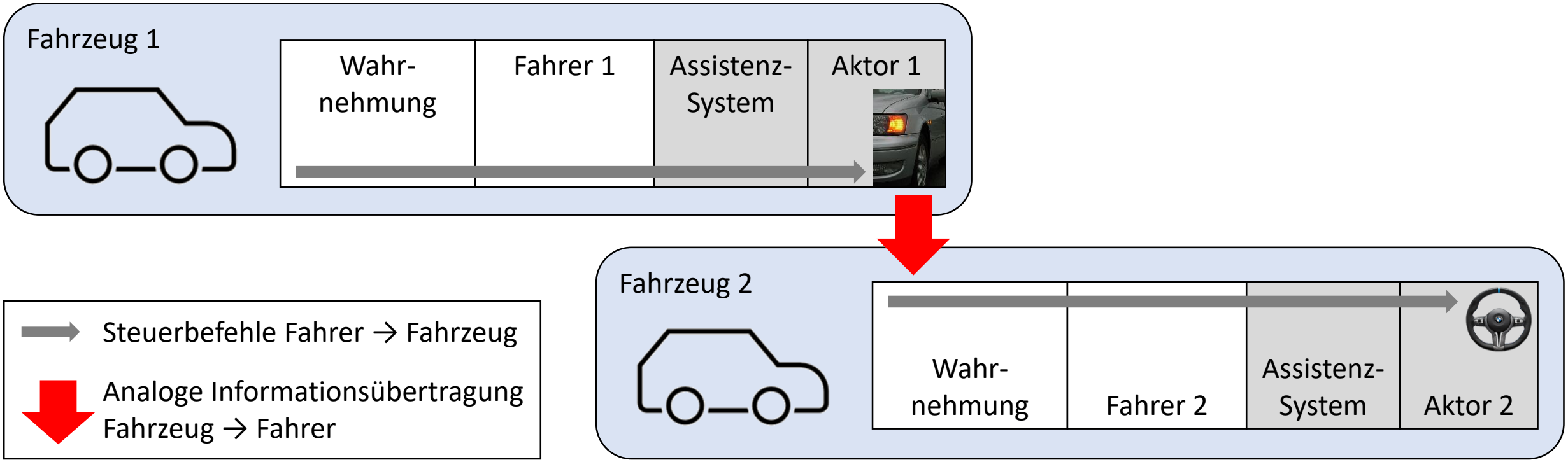
Hintergrund: Fundamentaldiagramm

- Zusammenhang zwischen
  - Kapazität q [Kfz/min]
  - Geschwindigkeit v [km/h]
  - Fahrzeugdichte k [Kfz/km]
    (~1/Abstand)



Limitation

- Reaktionszeit des Menschen: *v* und *k* nicht beliebig optimierbar



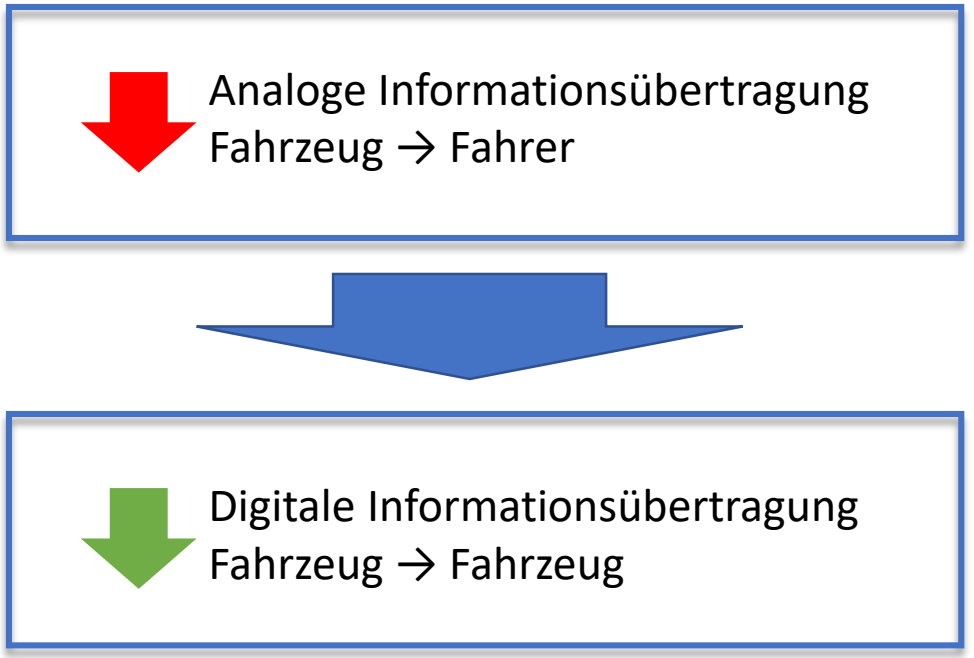
Lösungsansatz

"Intelligente Verkehrssysteme"

- Einsatz von Digitalrechnern
- Steigerung der Verarbeitungsgeschwindigkeiten
- Geringere Reaktionszeiten

➢Steigerung von *v* und *k*

Beitrag dieser Arbeit:
Sichere Kommunikationsarchitektur



Spezifische Herausforderungen (Auswahl)

Informationssicherheit

- Asymmetrische Kryptografie
  - Brechbar durch Lösen des mathematischen Problems
  - „Wettlauf“ mit Rechenleistung
- Symmetrische Kryptografie
  - Teilweise Brechbar durch Bruteforce
  - WEP, A5/1 (GSM) gebrochen

Rechtzeitigkeit

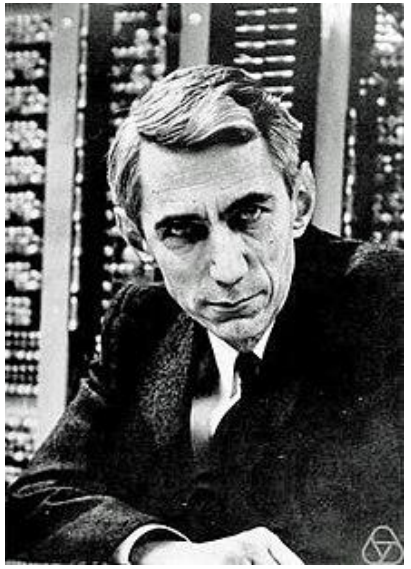
- Vorhersehbare Verarbeitungszeit für alle Verfahrensschritte
- Vorhersehbare Anzahl logischer Übertragungsstrecken

Lösung Informationssicherheit

- “Perfekte Sicherheit” nach C. Shannon (1949)
- *K*: Schlüssel, *P*: Klartext, *C*: Schlüsseltext

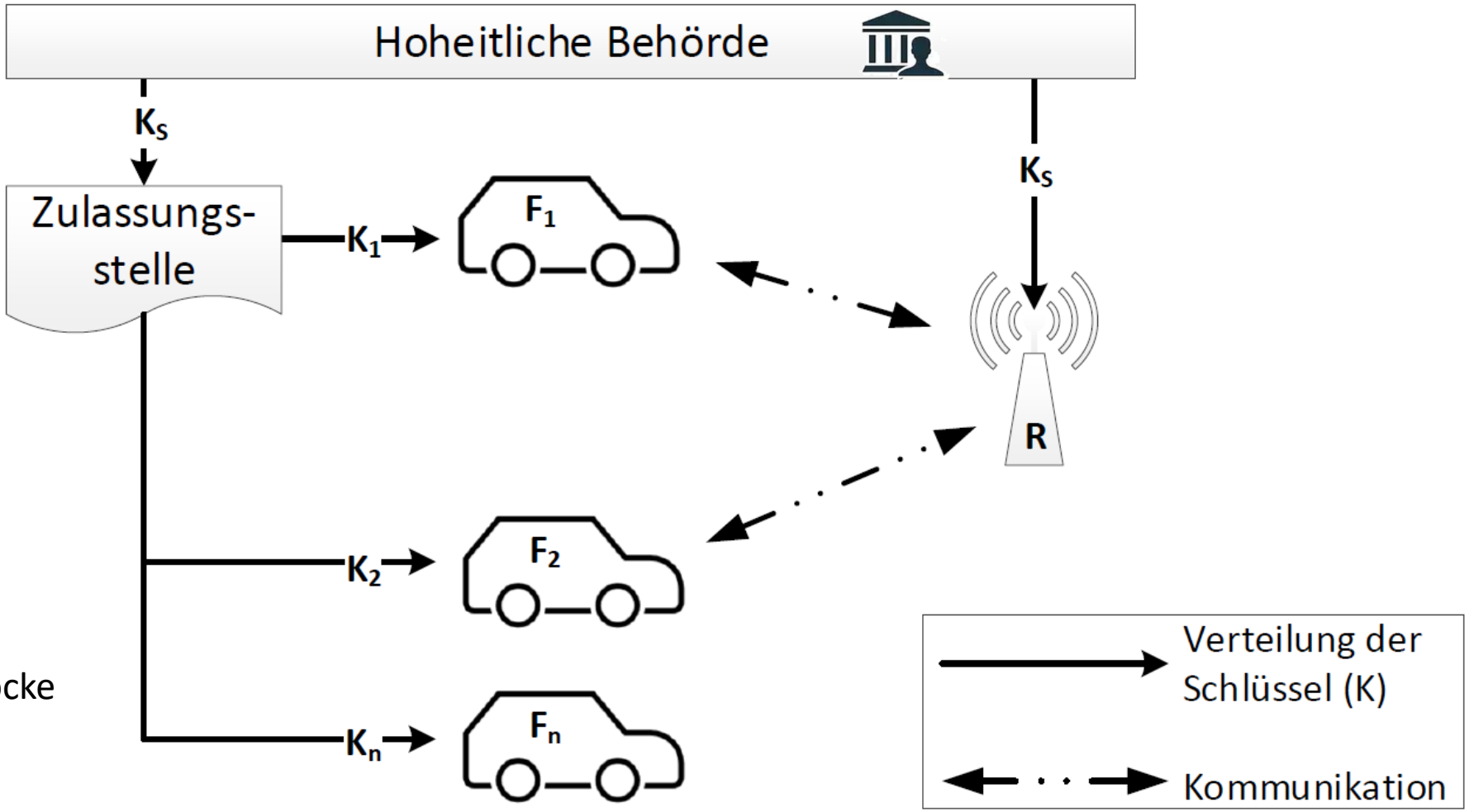
Ein Kryptosystem mit $|\mathcal{K}|=|\mathcal{P}|=|\mathcal{C}|<\infty$ und $Pr(x)>0$ für alle $x \in \mathcal{P}$ ist genau dann perfekt geheim, wenn die Schlüssel gleichverteilt sind und für alle $x \in \mathcal{P}, y \in \mathcal{C}$ genau ein Schlüssel $K \in \mathcal{K}$ mit $e_K(x)=y$ existiert

- Praktische Probleme des Schlüsselmanagements
  - Schlüsselerzeugung
  - Schlüsselverteilung
  - Schlüsselnachschub



Claude Shannon
www.wikipedia.de

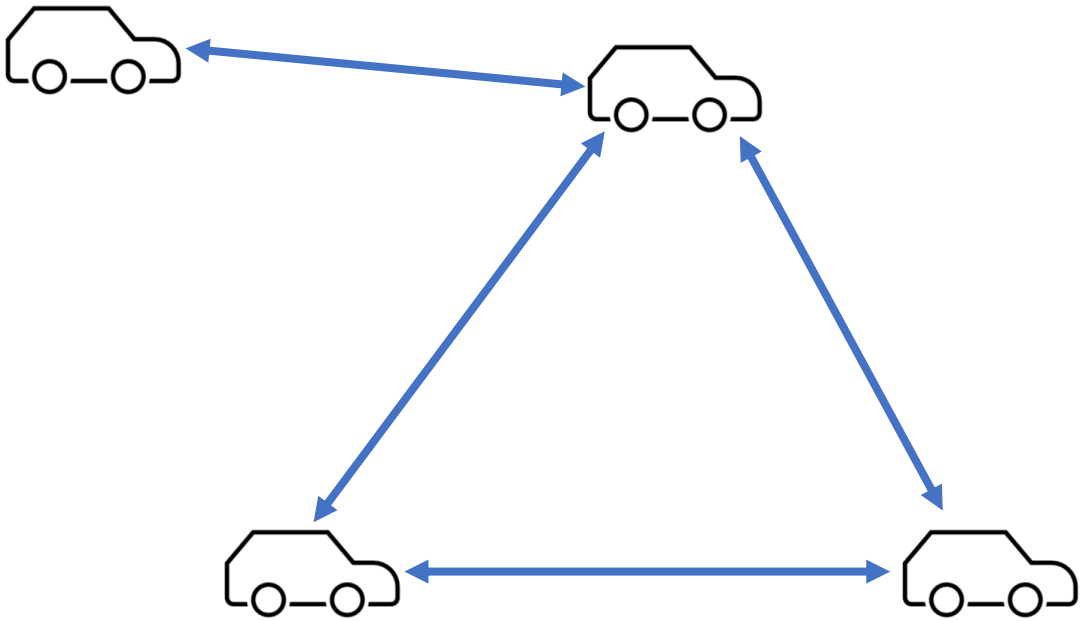
Akteure Schlüsselmanagement



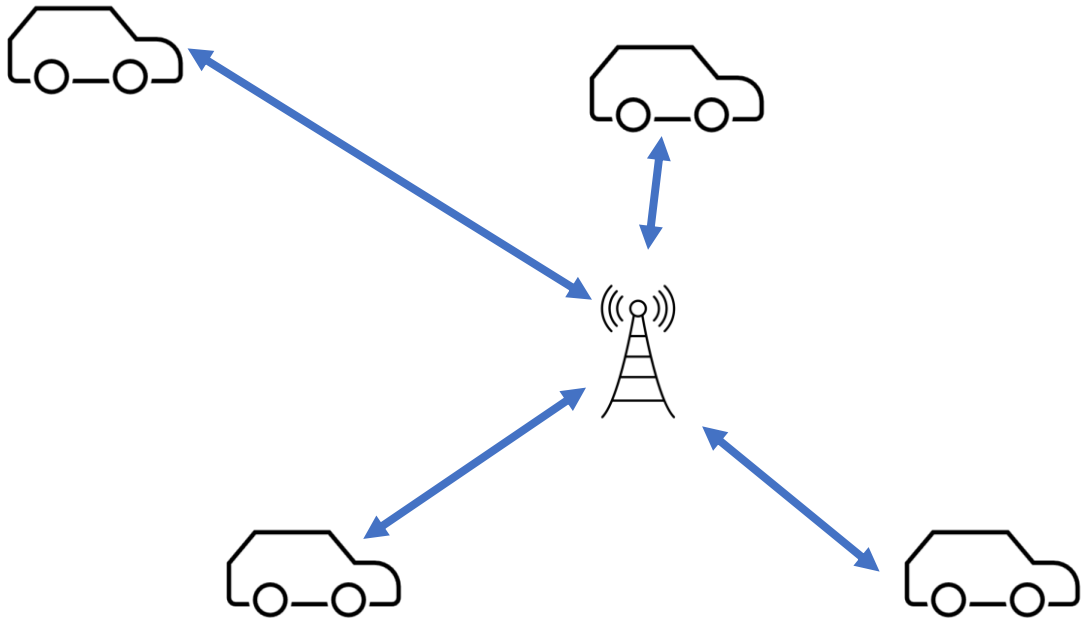
- F_n: Fahrzeug
- K_s: Saatwert / Schlüsselblöcke
- K_n: Individueller Schlüssel

Aspekte der Netzwerktopologie

Ohne Relais („Peer-to-Peer“)



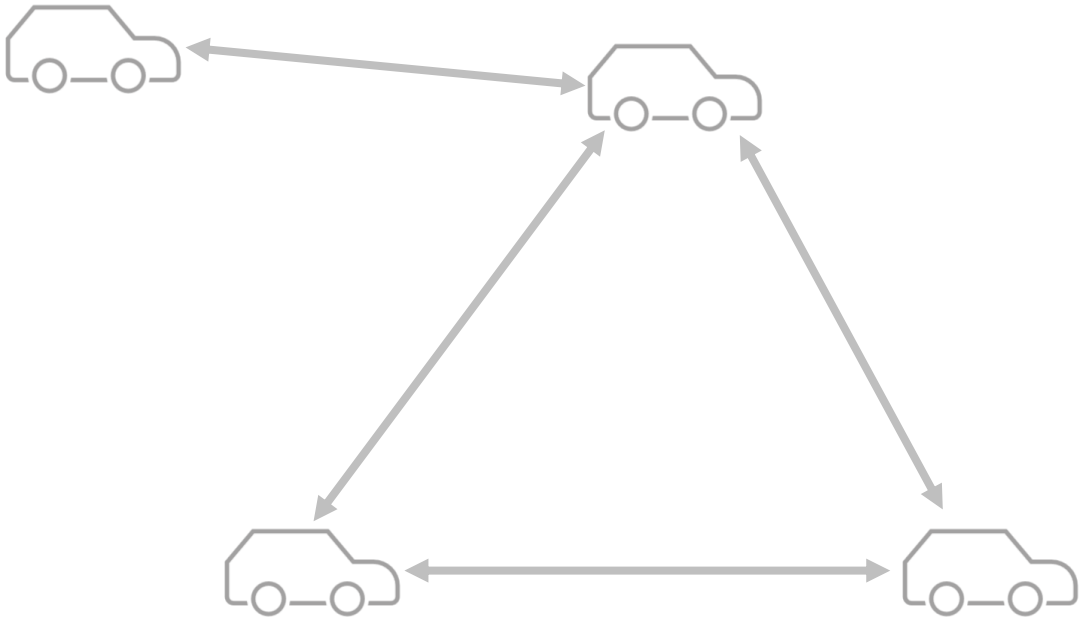
Mit Relais („Client-Server”)



Auswahl der Netzwerktopologie

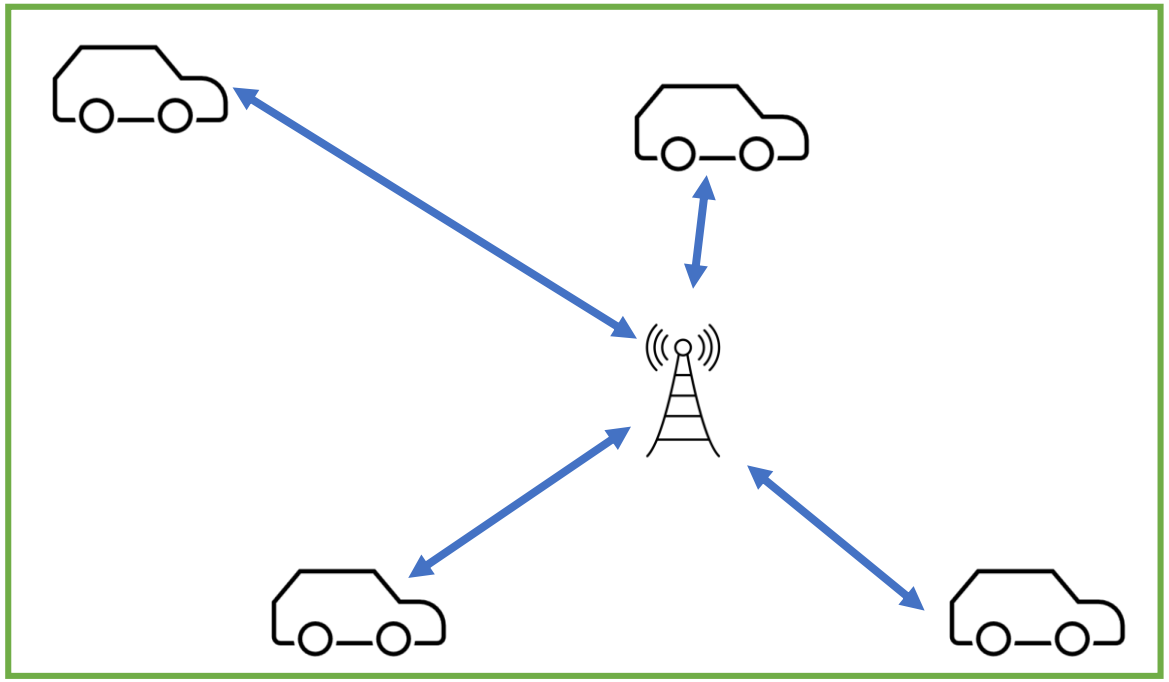
Ohne Relais („Peer-to-Peer“)

(-) Unvorhersehbare Anzahl an Übertragungsstrecken



Mit Relais („Client-Server“)

(+) Skalierbarkeit



Größe der Nutzdaten

- Spezifikation: ETSI TS 102 637-2 V1.2.1 (s. u.)
- Annahme: Nutzdaten in einem Paket gem.
  - „Cooperative Awareness Message (CAM)“
  - „Decentralized Environmental Notification Message (DENM)“

Use Case	min Frequency (Hz)	min Latency (ms)
Emergency Vehicle Warning	10	100
Slow Vehicle Indication	2	100
Intersection Collision Warning	10	100
Motorcycle Approaching Indication	2	100
Collision Risk Warning	10	100
Speed Limits Notification	1 to 10	100
Traffic Light Optimal Speed Advisory	2	100

Benötigte Schlüssellänge

- Mindestens gleicher Umfang wie Nutzdaten
- Benötigter Umfang somit Funktion von
  - Nutzdaten
  - Sendefrequenz
  - Sendeintervall

Paketgröße	Einheit	Frequenz	Einheit	Byte pro h	MB pro h	MB pro 24h
2.304	Byte	10	Hz	82.944.000,00	79,10	1.898,44
250	Byte	5	Hz	4.500.000,00	4,29	103,00
1	Byte	1	Hz	3.600,00	0,00	0,08

Aktuelle Datenspeicher

- USB-Stick: ~Terabyte

Kingston DataTraveler Ultimate GT

Smartcard: ~Kilobyte

MIFARE DESFIRE EV1 4K

Datenreduktion durch Codebücher (LUT)

Dynamisch

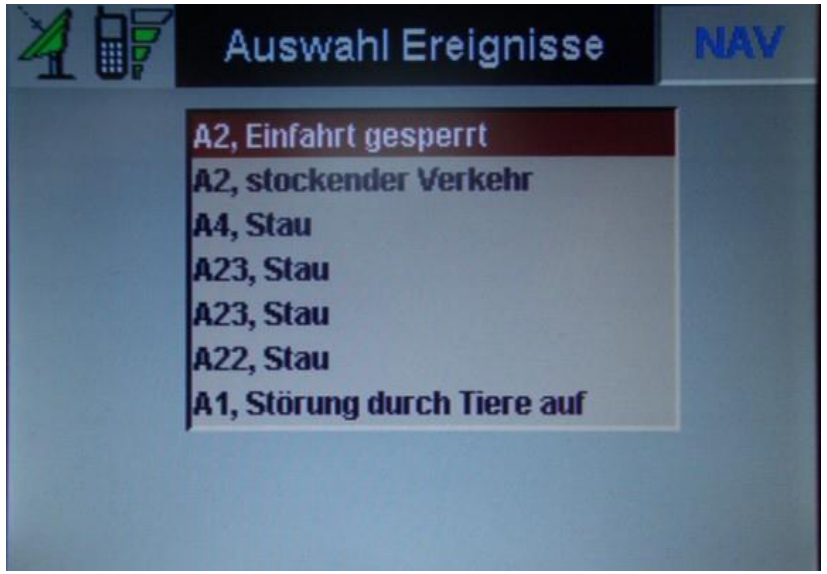
- Stetige Größen, z. B.
  - Fahrzeugabstand
  - Geschwindigkeit
  - Stauende
- Nicht vordefinierbar

Statisch

- Diskrete Größen, z. B.
  - Infrastruktur
  - Baustellen
- vordefinierbar

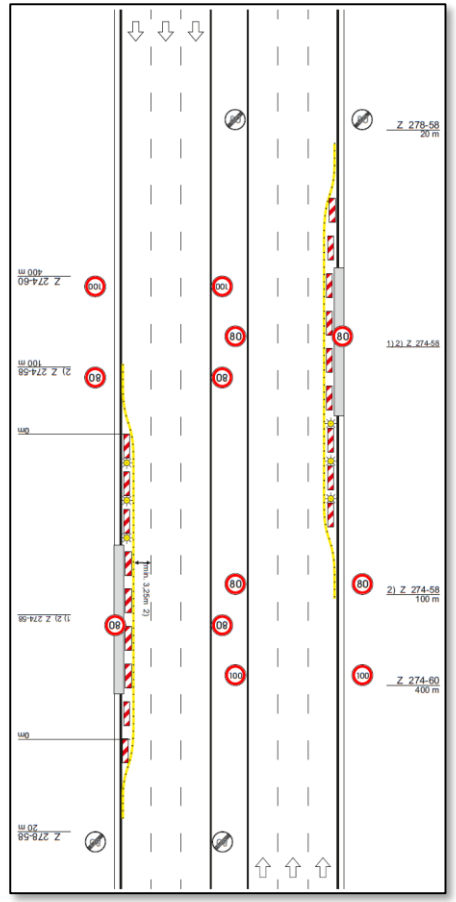
Beispiele für vordefinierbare Nachrichten

- Traffic Message Channel (TMC)

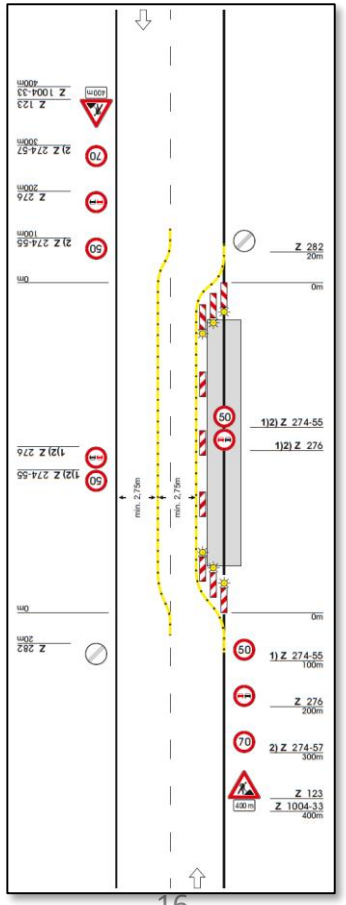


Aufbereitete Verkehrsnachricht im Fahrzeug

- Streckenführung Baustelle



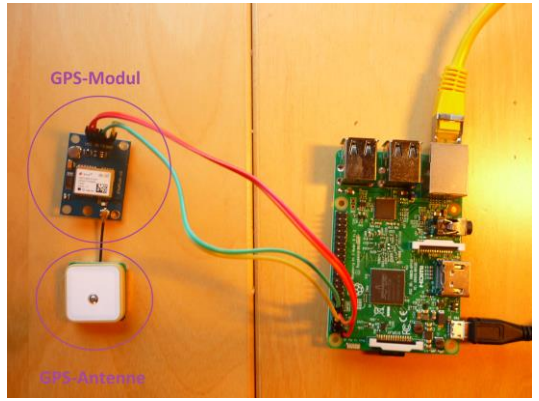
Regelplan D1-1



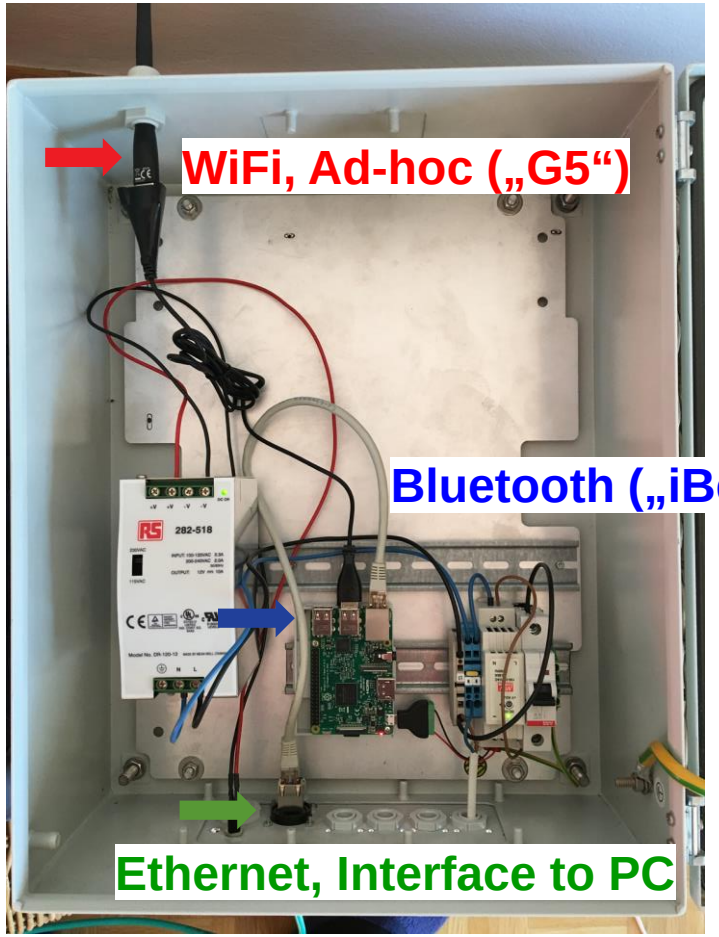
Regelplan C1-3

Weitere Schritte

- Laufender Praxistest
- Datenmodell
- Geschäftsmodell



Mobileinheit



Stationäre Einheit

Fazit und Ausblick

- Notwendige Bausteine zur perfekt sicheren Kommunikation sind seit langem bekannt
- Bisher bestehende technische Hürden können mit moderner Datenhaltung und –verarbeitung überwunden werden
- Durch korrekte Implementierung lassen sich Anforderungen nach Automotive Safety Integrity Level (ASIL) gem. ISO 26262 erfüllen

Danke für die Aufmerksamkeit

christoph.maget@studium.fernuni-hagen.de