HAW HAMBURG

Masterkolloquium

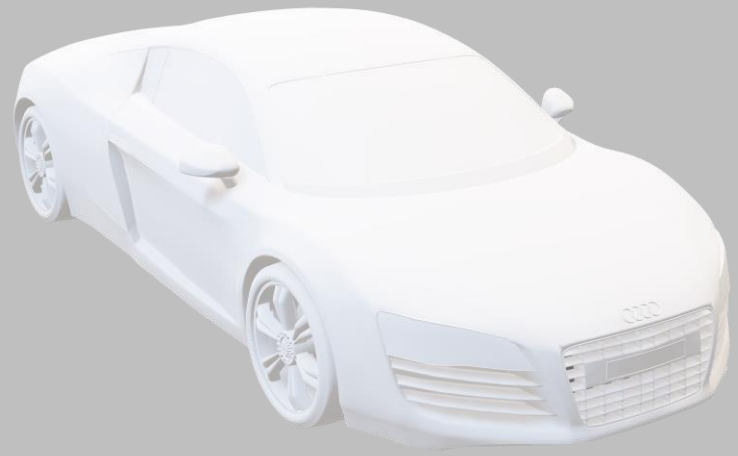
Informationssicherheit für Echtzeit-Ethernet-Fahrzeugnetzwerke

Philipp Meyer - philipp.meyer@haw-hamburg.de
Hochschule für Angewandte Wissenschaften Hamburg
13. Juni 2018

CoRE

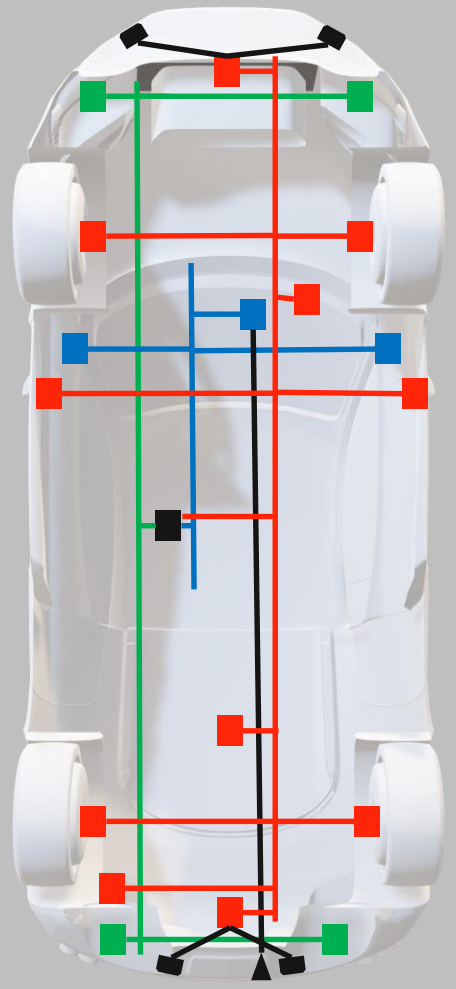
Gliederung

- **Einleitung**
- Grundlagen
- Istanalyse
- Sicherheitsanalyse
- Schutzkonzepte
- Simulation
- Fazit und Ausblick



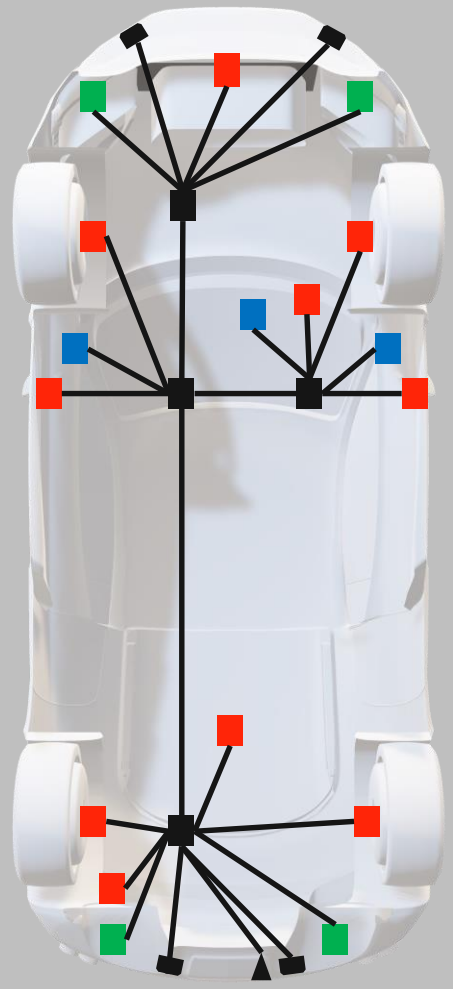
Einleitung

- Vielzahl von ECUs in aktuellen Fahrzeugen
- Kommunikation für Umsetzung von Funktionen nötig
- Aktuelle Übertragungsmedien:
  - Bustechnologien (z.B. CAN, Flexray)
  - Punkt-zu-Punkt-Verbindungen (z.B. Ethernet)
- Schritt für Schritt in die Zukunft mit Ethernet



Einleitung

- Vorteile Ethernet:
  - Simple und effiziente Kommunikationsarchitektur
  - Technologieverfügbarkeit
  - Hohe Bandbreiten
- Erfüllt jedoch keine harten Echtzeit-Anfoderungen
- Echtzeit-Ethernet-Protkolle (SERCOS-III, PROFINET, TTE, AVB, TSN)
- Öffnung des Fahrzeugs nach außen (Clouddienste, Car-to-X)
- Aktuelle Fahrzeuge sind Angreifbar (z.B Jeep[1], Tesla[2])
- Wie ist die Situation im Layer 2 mit Echtzeit-Protokollen?



1 WIRED: Hackers Remotely Kill a Jeep on the Highway—With Me in It. – URL https://www.wired.com/2015/07/ hackers-remotely-kill-jeep-highway/
2 The Verge: Car hackers demonstrate wireless attack on Tesla Model S. – URL https://www.theverge.com/2016/9/19/12985120/ tesla-model-s-hack-vulnerability-keen-labs

Gliederung

- Einleitung
- **Grundlagen**
  - **Begriff Informationssicherheit**
  - **Echtzeit-Ethernet-Protokolle**
- Istanalyse
- Sicherheitsanalyse
- Schutzkonzepte
- Simulation
- Fazit und Ausblick

Grundlagen
Definition Informationssicherheit[1]

- Funktionssicherheit (Englisch: safety)
- Informationssicherheit (Englisch: security)
  - Informationsvertraulichkeit: Geheimhaltung
  - Datenintegrität: Keine unautorisierte Modifikation
  - Systemverfügbarkeit: Kein Performance-Verlust

1 Eckert, Claudia: IT-Sicherheit Konzepte – Verfahren – Protokolle 9. aktualisierte und korr. Aufl. Muenchen : Oldenbourg, 2014

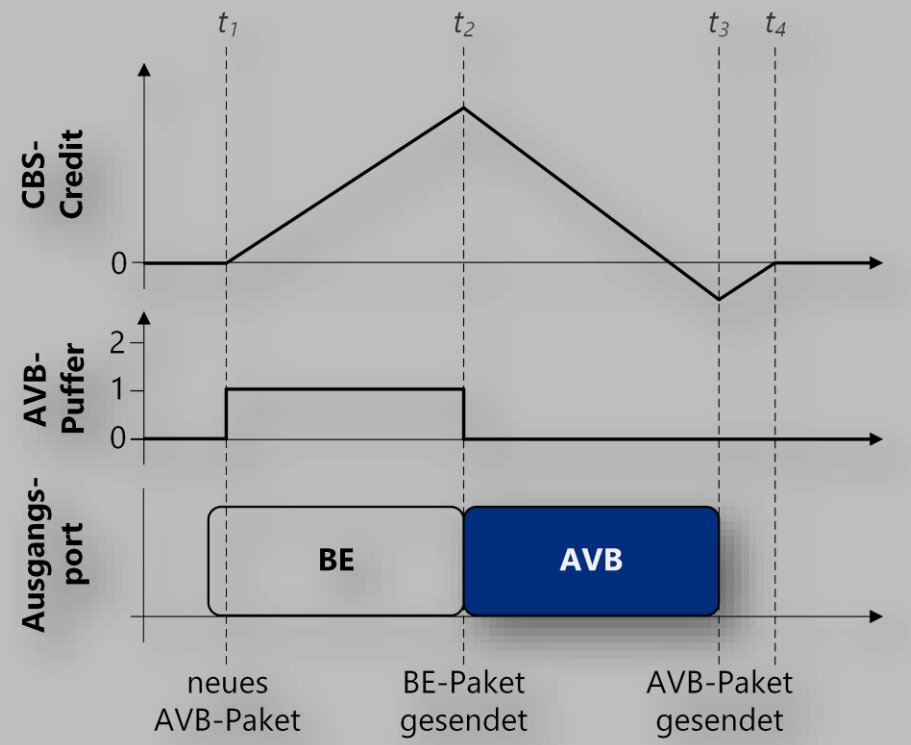
Grundlagen
Time-Triggered Ethernet (TTE)

- Standard AS6802
- Verkehrsklassen:
  - Time-Triggered (TT)
  - Rate-Constrained (RC)
  - Best-Effort (BE)
- TDMA-Verkehr benötigt verteilte Synchronisation der Zeit

Grundlagen
Audio Video Bridging (AVB)

- Standards: IEEE 802.1Q, IEEE 802.1BA, IEEE 802.1Qat, IEEE 802.1Qav
- Verkehrsklassen:
  - A
  - B
  - Best-Effort mit restlichen Q Prioritäten
- SRP für die dynamische Reservierung von Routen im Netzwerk
- CBS für Einhaltung der Bandbreite am Ausgang der Geräte verantwotlich

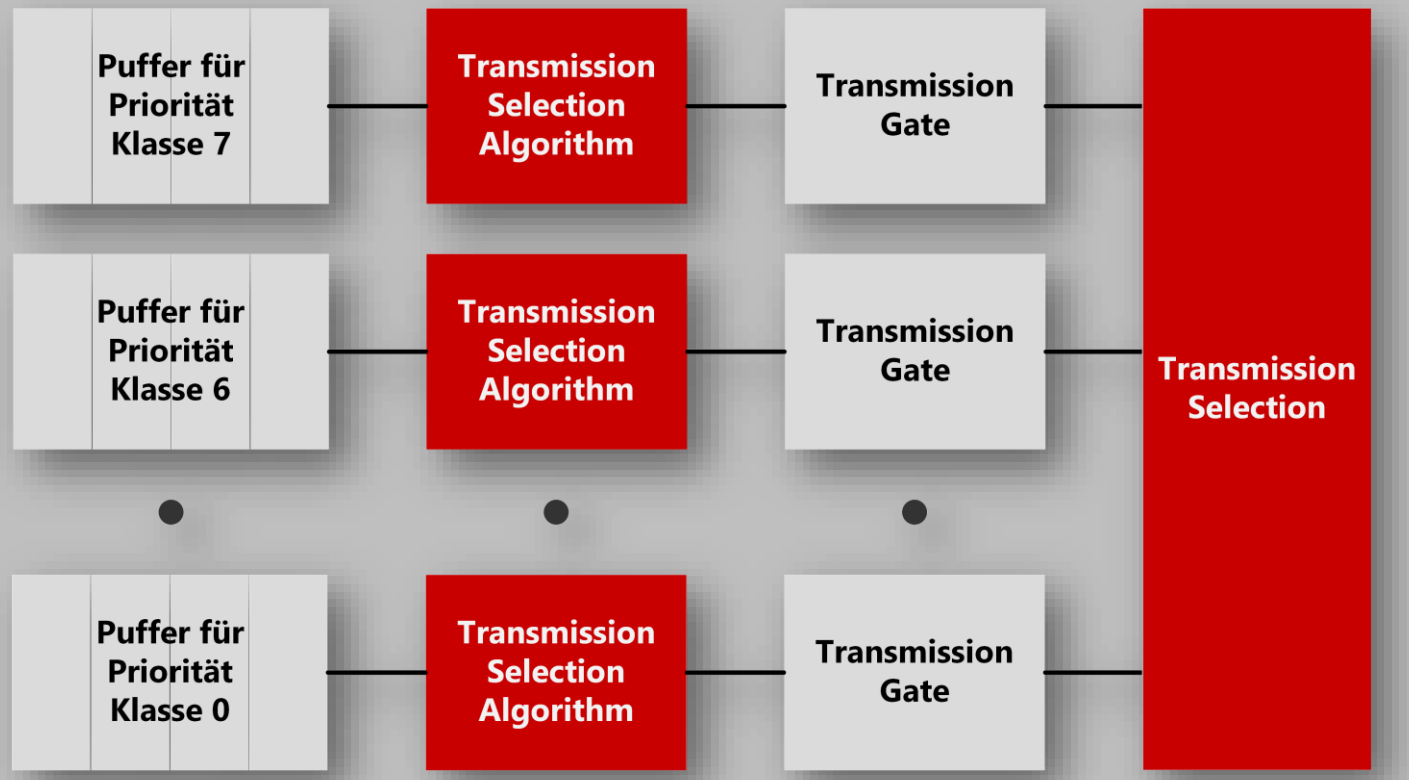
Grundlagen
Audio Video Bridging (AVB): Credit Based Shaper (CBS)



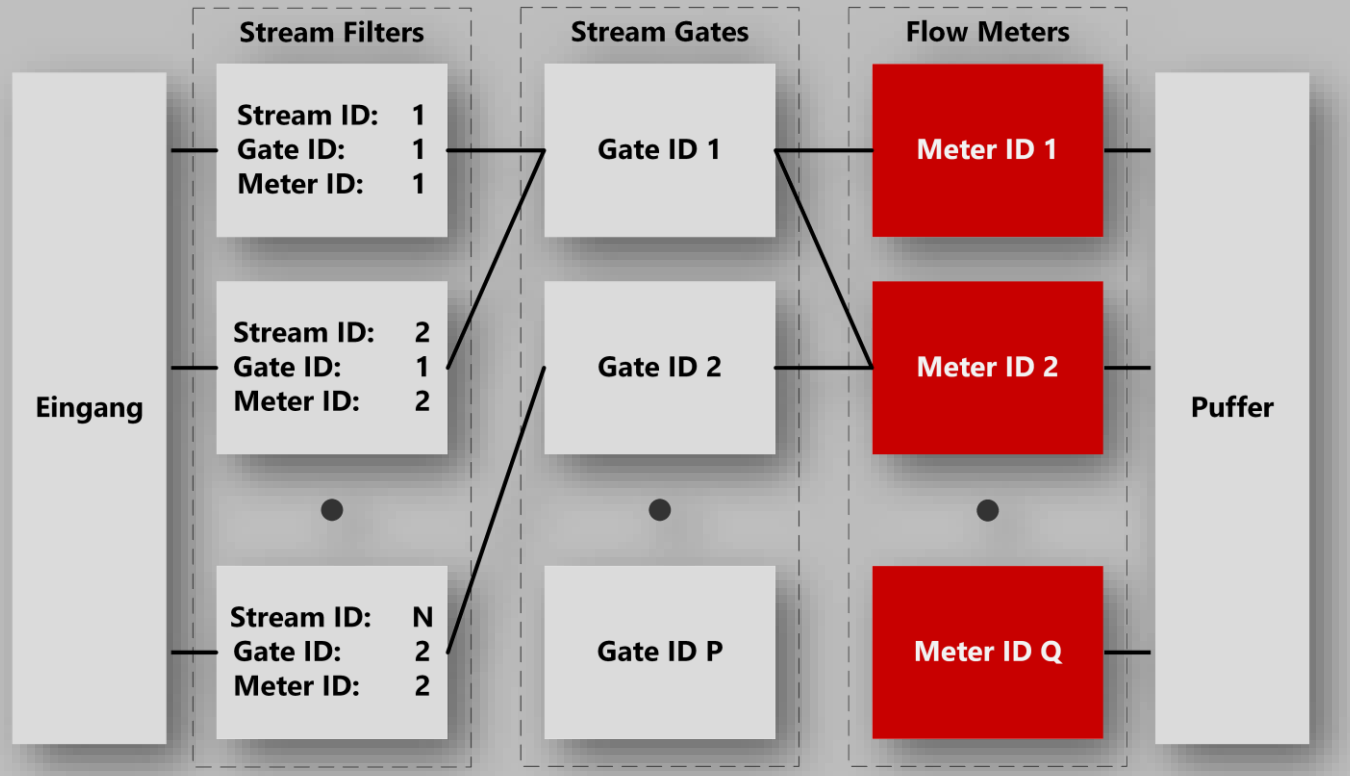
Grundlagen
Time-Sensitive Networking (TSN)

- Nachfolger AVB
- Standards: IEEE 802.1Qbv, IEEE 802.1Qci
- Verkehrsklassen:
  - Beliebiges mapping von Verkehrsklassen auf die Q Prioritäten
- TDMA-Verkehr benötigt Synchronisierung der Zeit
- Weiterhin Möglichkeit der dynamischen Reservierung von Stream-Routen
- Neu: Filtern am Eingang

Grundlagen
Time-Sensitive Networking (TSN): IEEE 802.1Qbv



Grundlagen
Time-Sensitive Networking (TSN): IEEE 802.1Qci

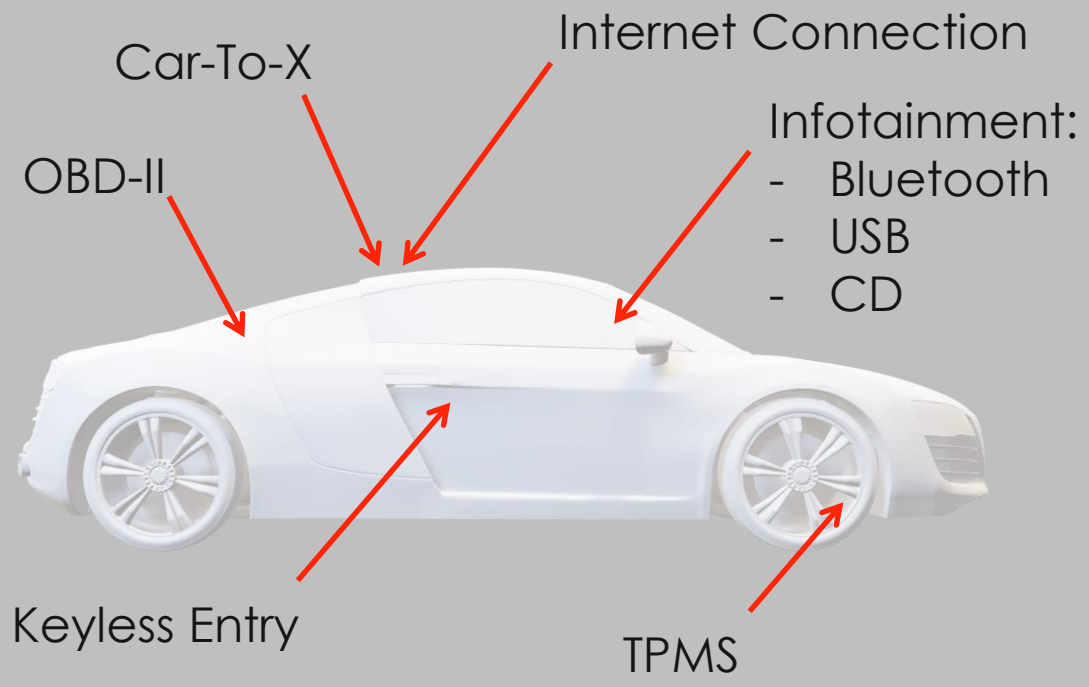


Gliederung

- Einleitung
- Grundlagen
- **Istanalyse**
  - **Angreifbarkeit aktueller Fahrzeuge**
- Sicherheitsanalyse
- Schutzkonzepte
- Simulation
- Fazit und Ausblick

Istanalyse
Angreifbarkeit aktueller Fahrzeuge[1]

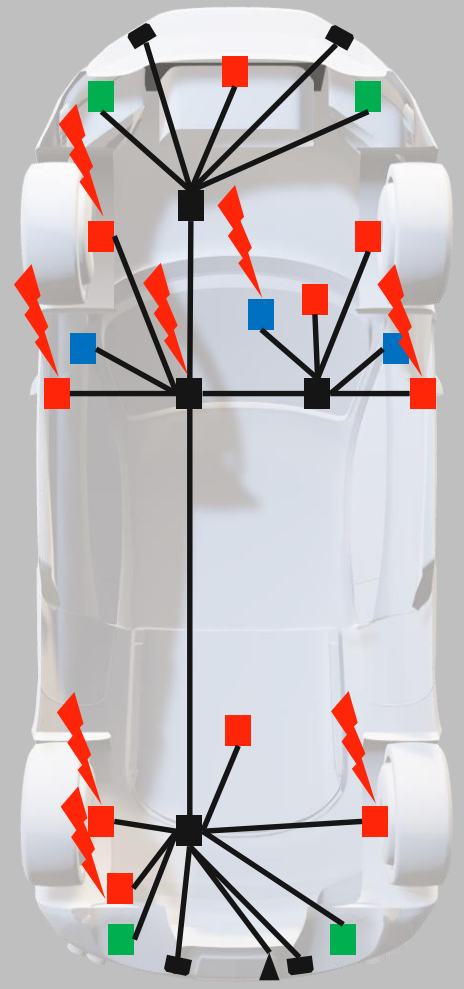
- Indirekter physikalischer Zugriff:
  - ODB-II Diagnoseschnitstelle, Infotainment, …
- Kabelloser Zugriff über kurze Distanzen:
  - Bluetooth, WiFi, Remote-Keyless-Entry, TPMS, …
- Kabelloser Zugriff über weite Distanzen:
  - GPS, Digital, Radio, TMC, Mobilfunk, …



1 Checkoway, Stephen; Mccoy, Damon; Kantor, Brian; Anderson, Danny; Shacham, Hovav; Savage, Stefan; Koscher, Karl; Czeskis, Alexei; Roesner, Franziska; Kohno, Tadayoshi: Comprehensive Experimental Analyses of Automotive Attack Surfaces In: USENIX Security (2011). – URL: http://www.autosec.org/pubs/cars-usenixsec2011.pdf

Istanalyse
Angreifbarkeit aktueller Fahrzeuge

- Schnittstellen sind Teilnehmer der Bordnetzkommunikation
- Angriffe auf das Netzwerk sind aus jeder Richtung möglich
- Angriffe können sich über das Netzwerk auf weitere Teilnehmer ausbreiten



Gliederung

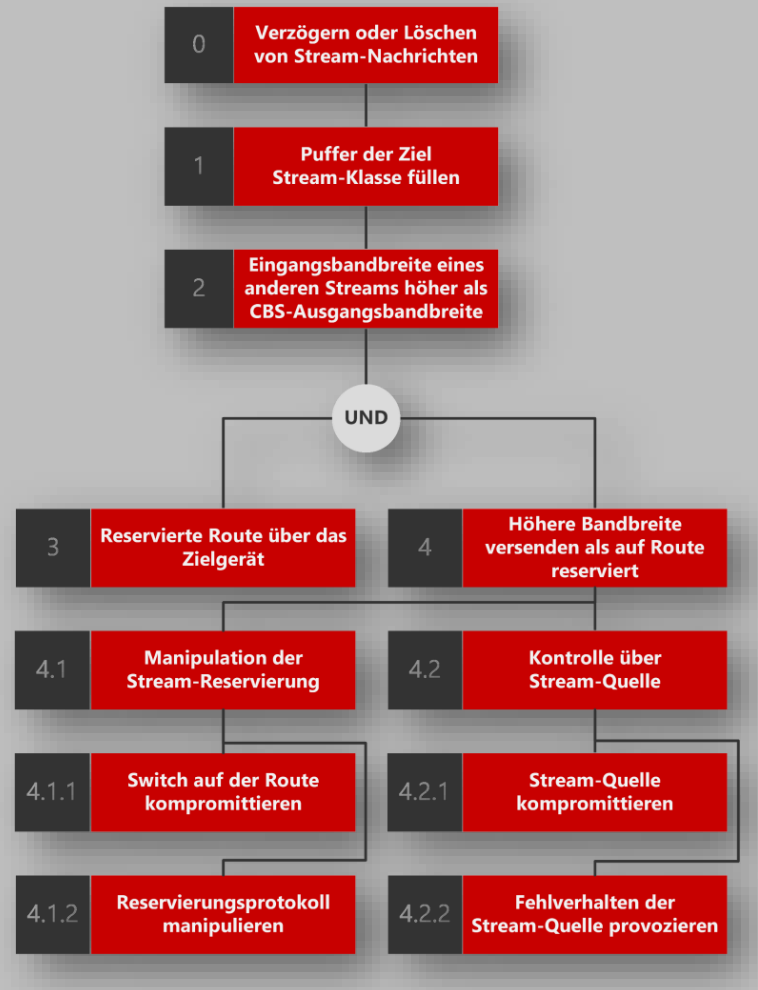
- Einleitung
- Grundlagen
- Istanalyse
- **Sicherheitsanalyse**
  - **Vorgehensweise**
  - **Beispiel einer Schwachstelle**
- Schutzkonzepte
- Simulation
- Fazit und Ausblick

Sicherheitsanalyse

- Identifikation der Schwachstellen
- Identifikation der Anforderungen
- Qualitative Bewertung der Risiken

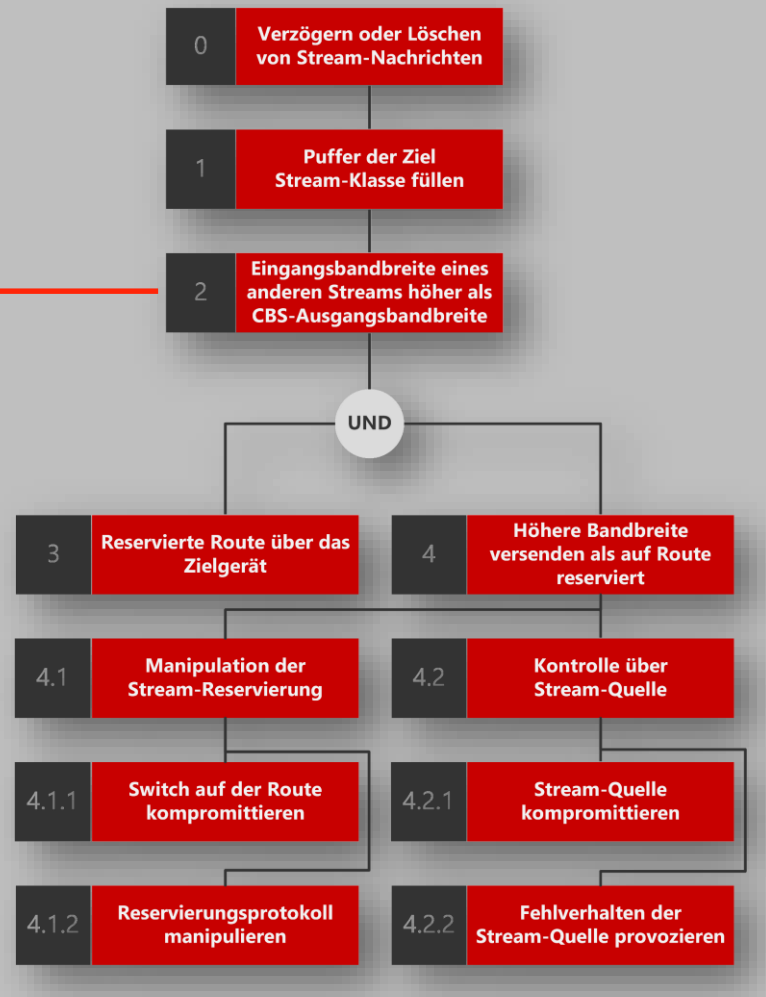
Identifikation der Schwachstellen
Verzögern oder Löschen von Stream-Nachrichten

- Einsatz von Bedrohungsbäumen
- Wurzel ist Angriffsziel
- Blätter sind Teilziele zum erreichen des Angriffsziels



Identifikation der Anforderungen

- Begrenzung der eingehenden Stream-Nachrichten
  - Aufholverhalten des CBS unbeeinflusst
- Sicherung der Switche
- Sicherung des Reservierungsprotokolls



Gliederung

- Einleitung
- Grundlagen
- Istanalyse
- Sicherheitsanalyse
- **Schutzkonzepte**
  - **Schutzmaßnahmen**
  - **Vertiefung Eingangsverkehr filtern**
- Simulation
- Fazit und Ausblick

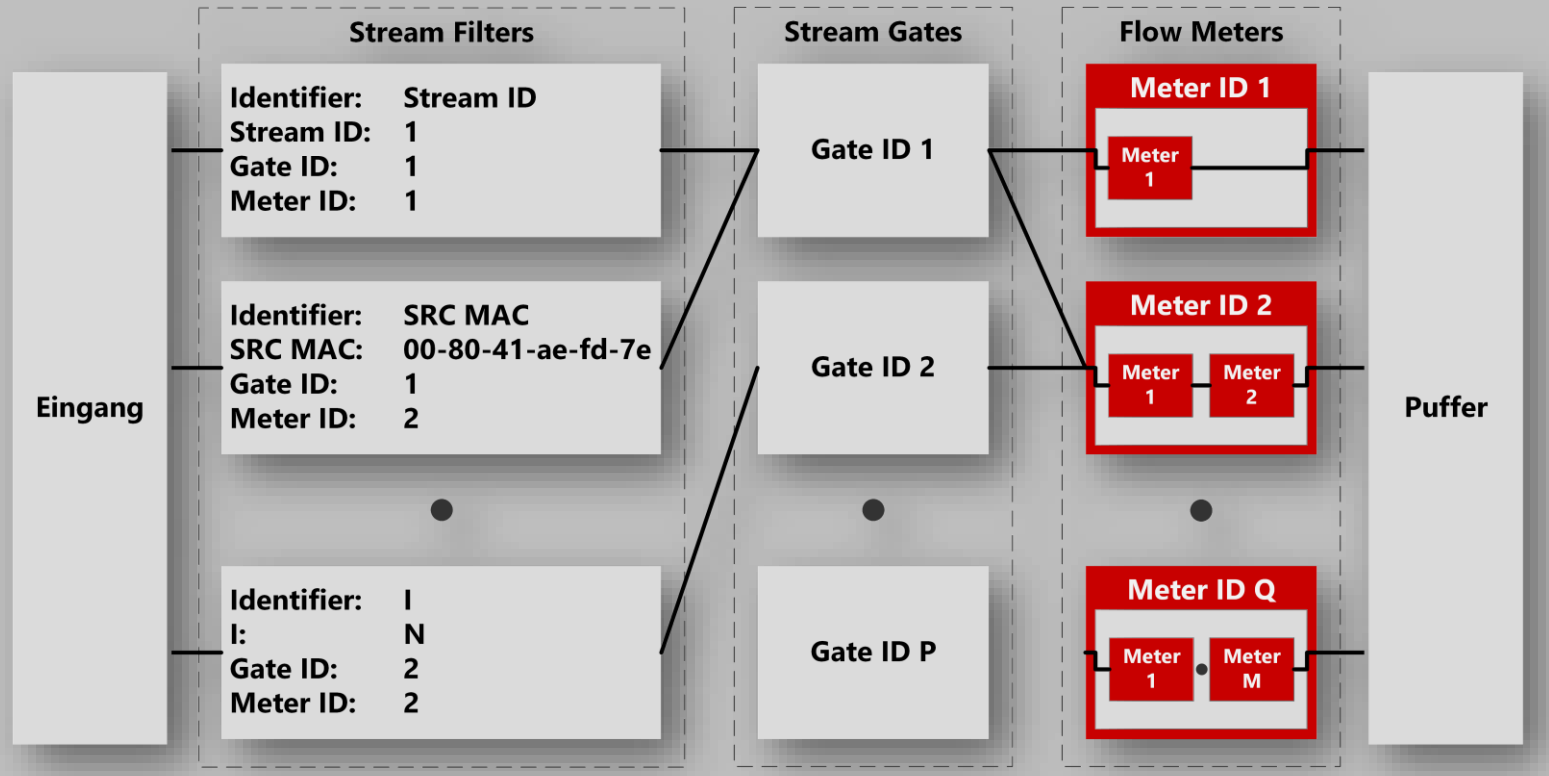
Schutzkonzepte

- Authentifizierung
- Verschlüsselung
- Schutz der Switche
- **Eingangsverkehr filtern**

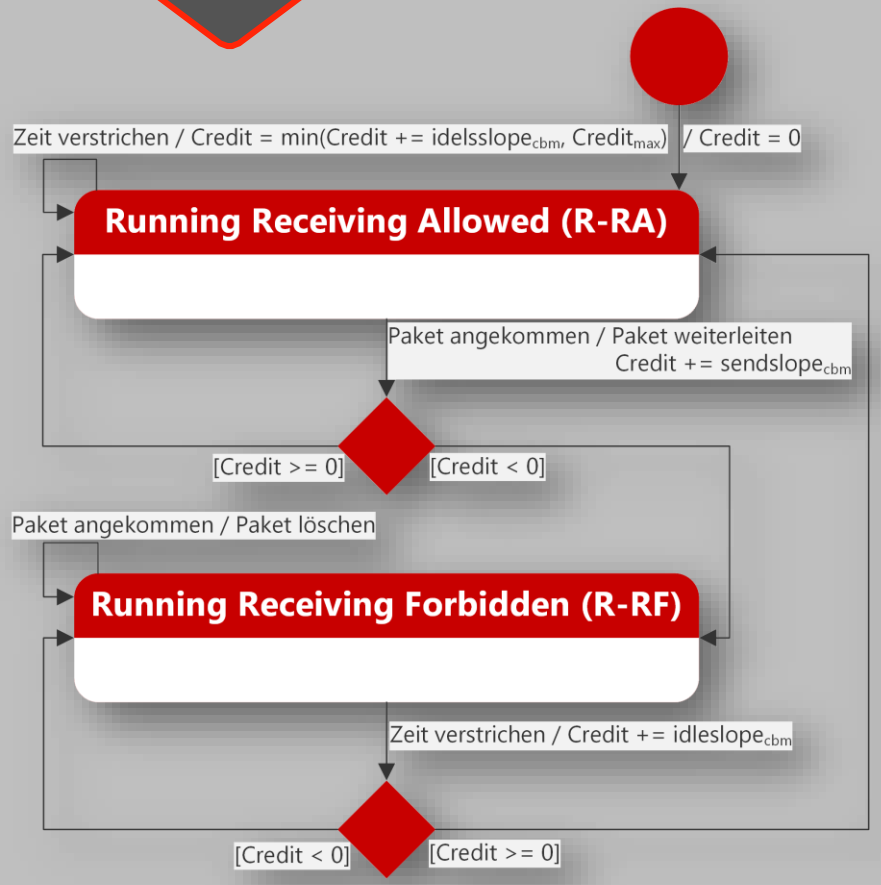
Schutzkonzepte
Eingangsverkehr filtern

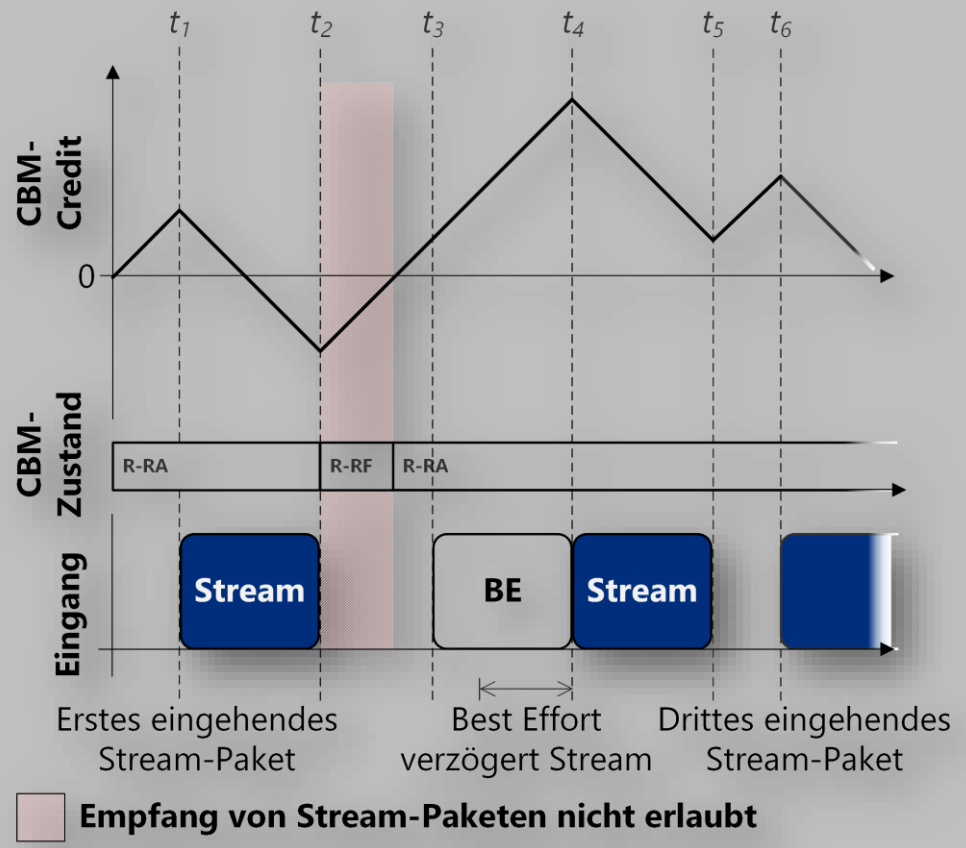
- Ziele:
  - Verteilt
  - Jede Art von Verkehr
  - Erweiterbar
  - Konfigurierbar
- Konzept orientiert sich am TSN Standard IEEE 802.1Qci
- Konkrete Lösung für die Anforderung des Filterns von Stream-Verkehr

Schutzkonzepte
Eingangsverkehr filtern



Schutzkonzepte
Eingangsverkehr filtern: Credit Based Meter



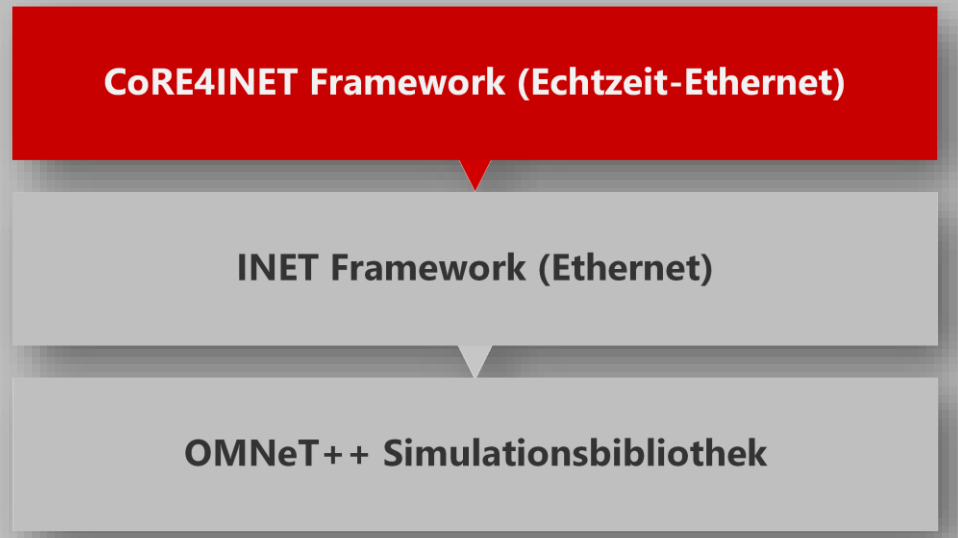


Gliederung

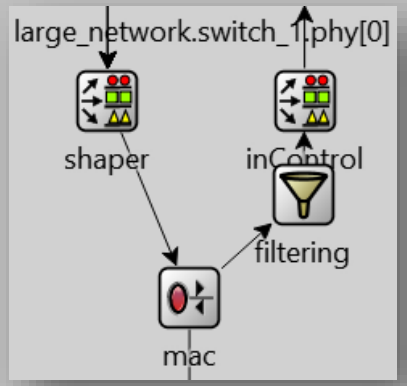
- Einleitung
- Grundlagen
- Istanalyse
- Sicherheitsanalyse
- Schutzkonzepte
- **Simulation**
  - **Erweiterung von CoRE4INET**
  - **Fallbeispiel**
- Fazit und Ausblick

Simulation
Modell

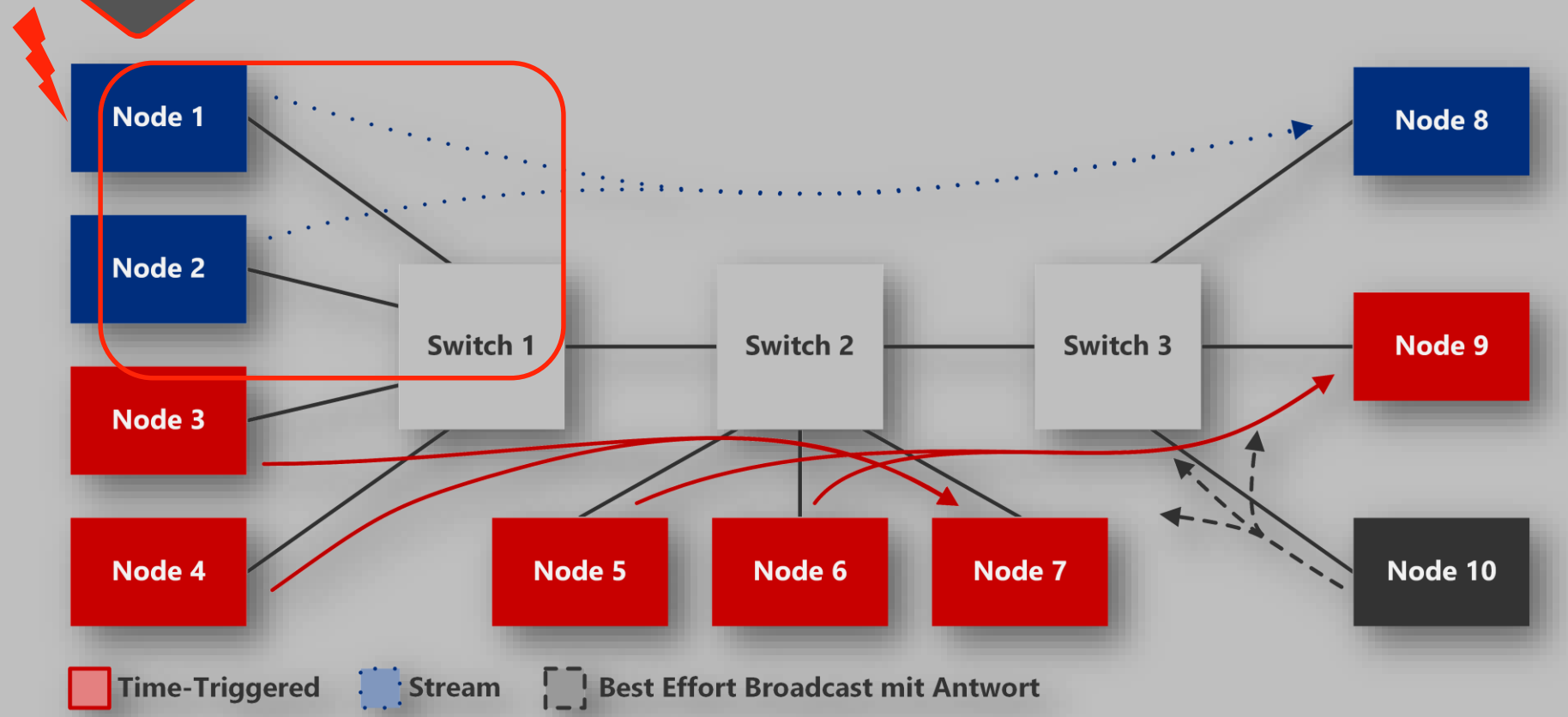
- OMNeT++: eventbasierte Simulation
- INET: Ethernet und Internettechnologien
- CoRE4INET: Echtzeit-Ethernet (TTE, AVB)



Simulation
Modell



Simulation
Fallstudie

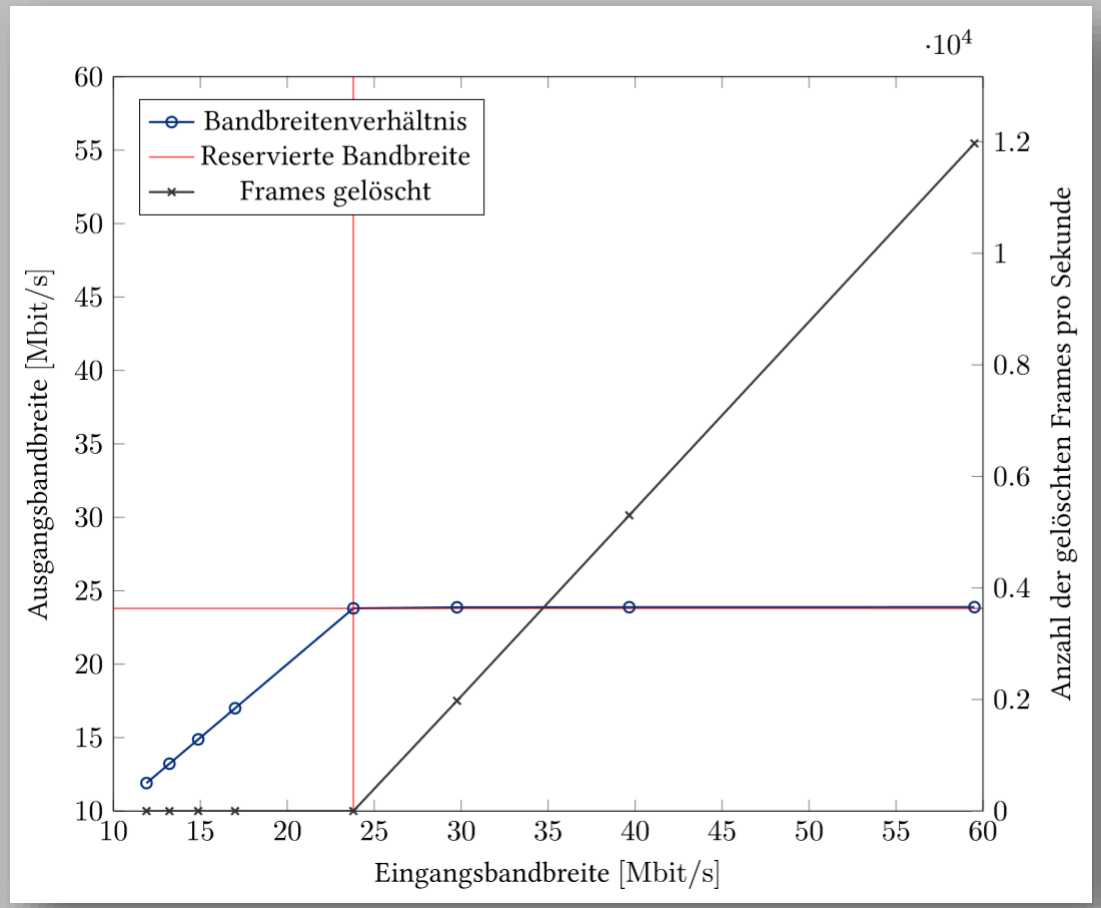


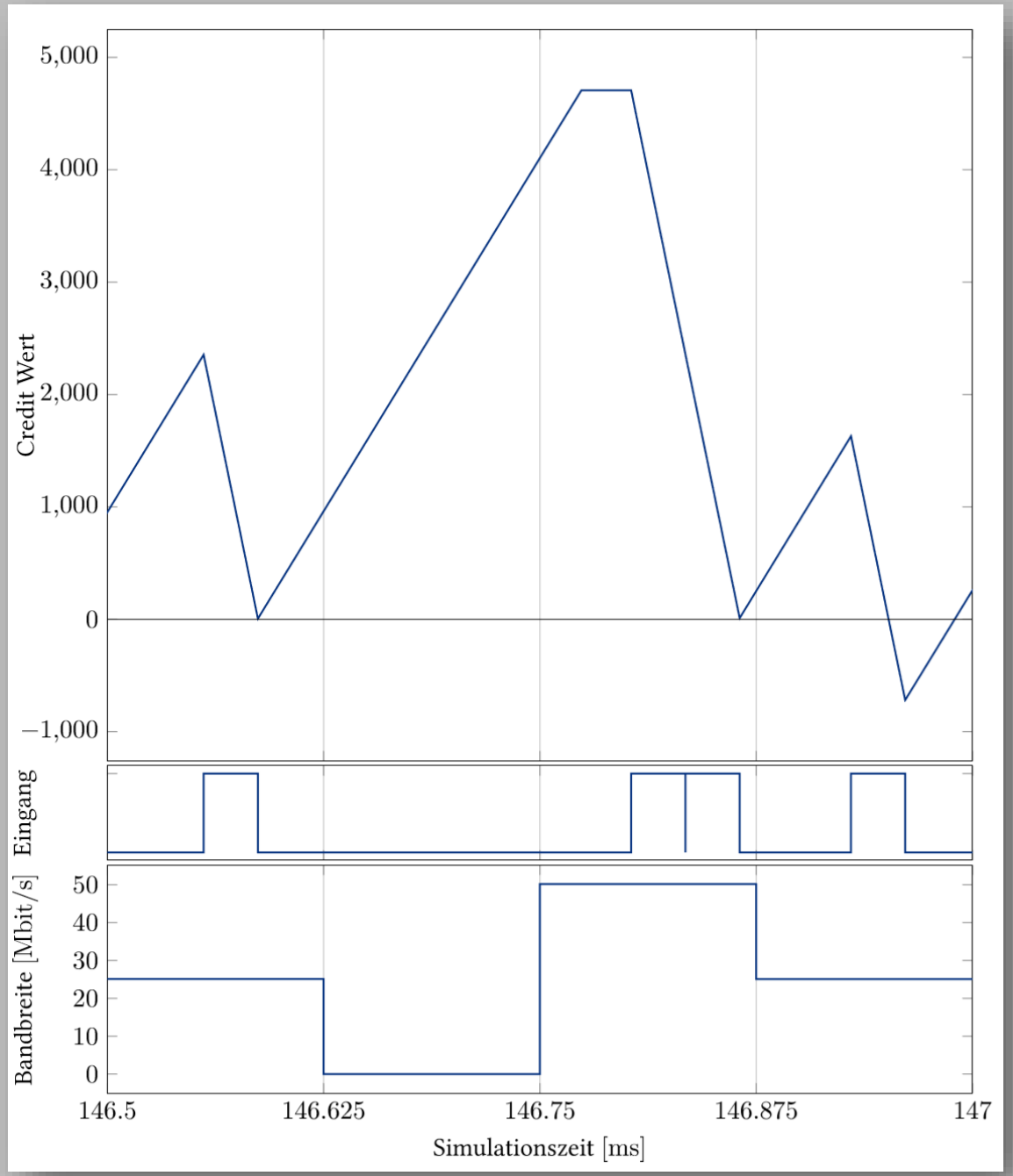
Simulation
Fallstudie

$$Burst_{maxswitch1port0} = Burst_{outnode1} + 1$$
$$= 2 + 1 = 3$$

$$Credit_{maxswitch1} = |sendslope| * T_{duration} * (Burst_{max} - 1)$$
$$\approx 75Mbit/s * 31\mu s * (3-1) = 4650$$

Simulation
Fallstudie




5,000
4,000
3,000
2,000
1,000
0
−1,000
Credit Wert
Eingang
50
40
30
20
10
0
Bandbreite [Mbit/s]
146.5
146.625
146.75
146.875
147
Simulationszeit [ms]

Gliederung

- Einleitung
- Grundlagen
- Istanalyse
- Sicherheitsanalyse
- Schutzkonzepte
- Simulation
- **Fazit und Ausblick**

Fazit

- Eingesetzte Layer 2 „Service“ Protokolle müssen gesichert werden (SRP, Sync, ARP)
  - Authentifizierung für Datenintegrität. Für Informationsvertraulichkeit sogar Verschlüsselung nötig.
- Hardware der Switche vor Manipulation schützen
- Layer 2 „Transport“ Protokolle müssen auf Schwachstellen analysiert werden (TSN)
  - Einfache „Verschlüsselung“ auf höheren Schichten reicht nicht aus
- Verteilte Eingangsfilter notwendig
  - Nicht nur Firewall an Schnittstelle
- CBM verhindert Auswirkungen von DoS-Angriffen mit CBS-Streams im Netzwerk

Ausblick

- Analyse weiterer Echtzeit-Ethernet-Protokolle
- Authentifizierung und Verschlüsselung der Layer 2 „Service“ Protokolle
- Fallstudien mit weiteren Metern
- Interferenz mit weiteren Schutzmechanismen (auch auf höheren Schichten)

Masterkolloquium
Informationssicherheit für Echtzeit-Ethernet-Fahrzeugnetzwerke