Anwendungen 2

Informationssicherheit in IEEE 802.1 Time Sensitive Networking Bordnetzen

Philipp Meyer
philipp.meyer@haw-hamburg.de

Hochschule für Angewandte Wissenschaften Hamburg

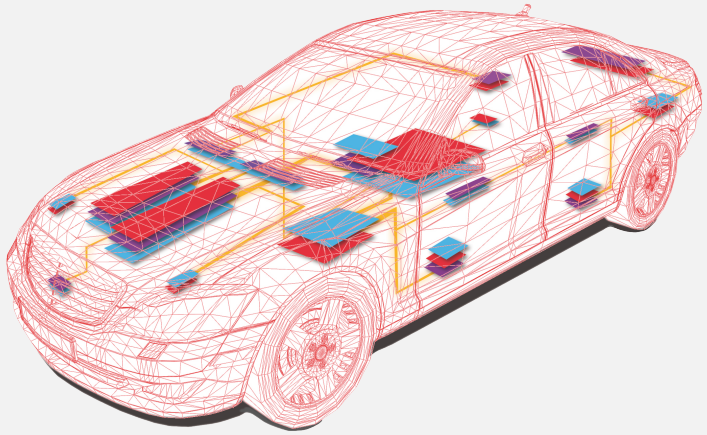
15. Januar 2015

Hochschule für Angewandte Wissenschaften Hamburg
Hamburg University of Applied Sciences

Agenda

Einleitung & Motivation

Das moderne Fahrzeug



- Vielzahl an Sensoren und Steuergeräten(ECUs)
- Von proprietären Bustechnologien zu Ethernet
- Gegenwärtige Infrastrukturen sind angreifbar
- Informationssicherheit für die nächste Bordnetzgeneration in den Fokus rücken

Einleitung & Motivation

Einsatz von Ethernet

Vorteile

- Erprobte Technologie
- Geordnete Infrastruktur
- Hohe Bandbreiten
- IP-basierte Dienste

Nachteile

- Keine Echtzeit
- Sicherheitsrisiken durch Verbreitung

Einleitung & Motivation

Time Sensitive Networking

- Ethernet mit Zeitgarantien:
  - Statische Protokolle
  - Dynamische Protokolle
- Eigenschaften in TSN Verbunden
- IEEE Time Sensitive Networking Task Group[1]
- Bisher kein Fokus auf Informationssicherheit

[1] IEEE 802.1 TSN Task Group: *IEEE 802.1 Time-Sensitive Networking Task Group*.

Agenda

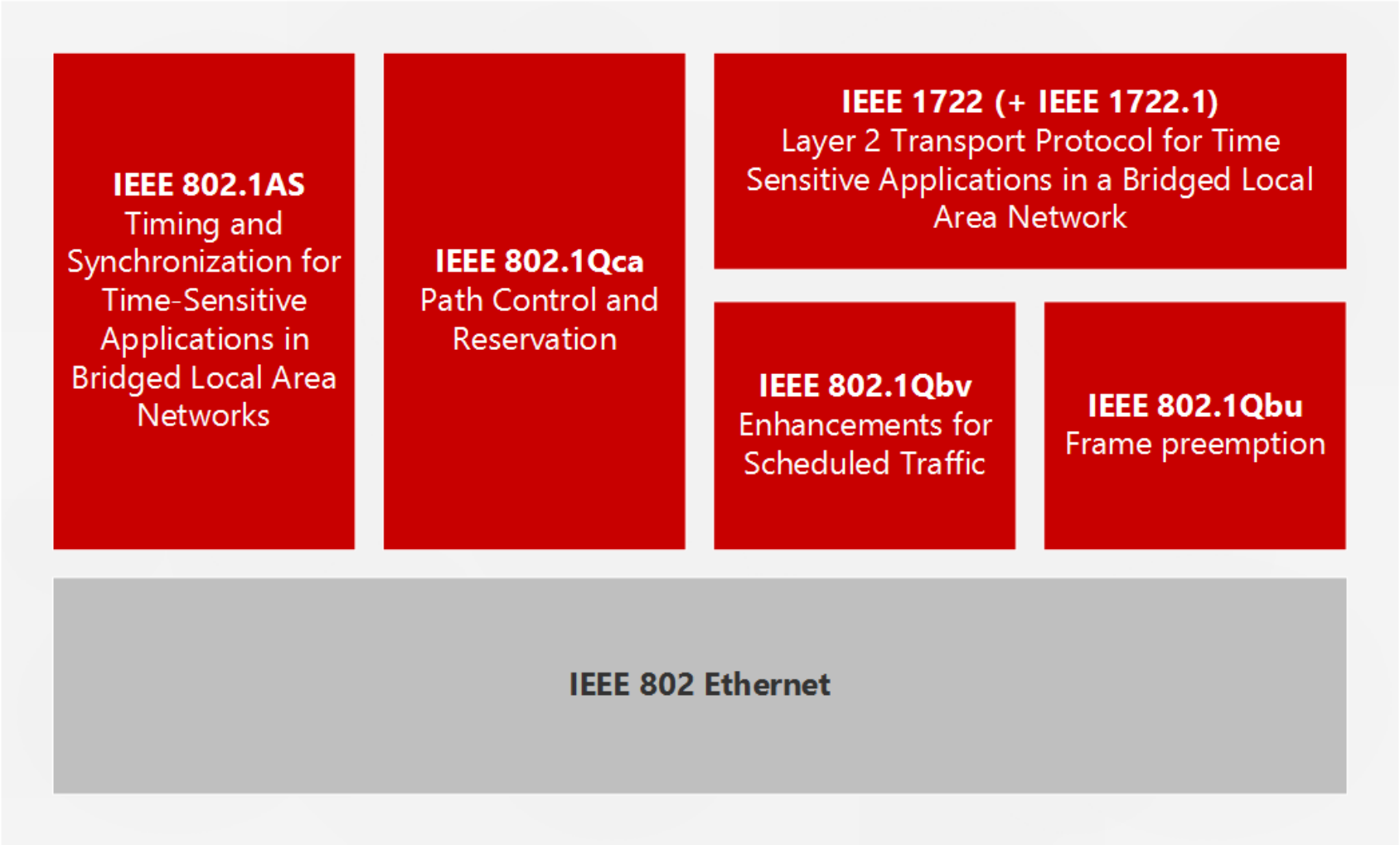
Time Sensitive Networking

Einordnung

- Ethernetprotokoll mit unterschiedlichen Zeitgarantien
- Nachfolger von Audio/Video Bridging
- Ermöglicht dynamischen und statischen Verkehr

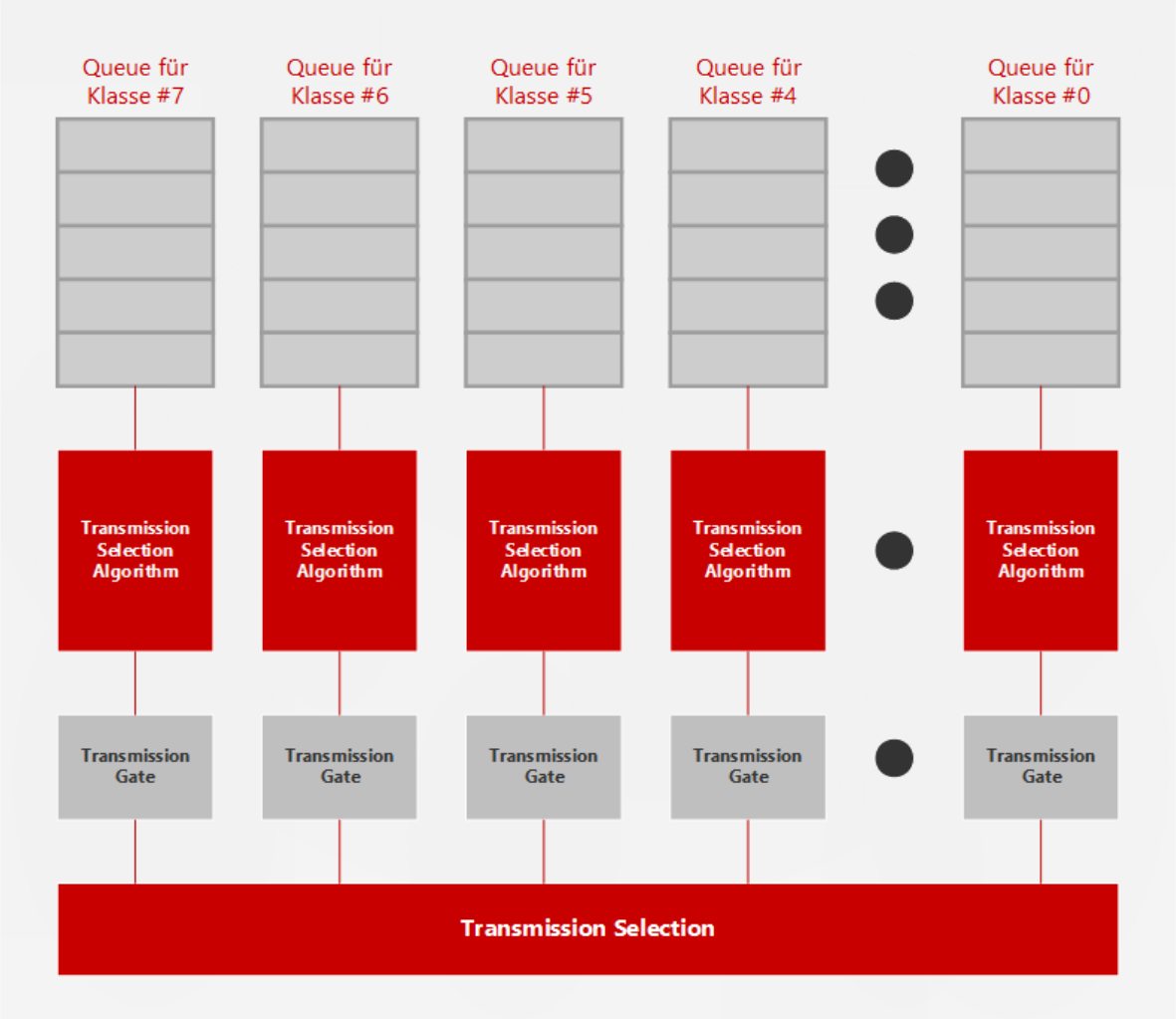
Time Sensitive Networking

Aufbau



Time Sensitive Networking

Funktion



Agenda

Zielsetzung & Problemstellung

Abgrenzung

Anwendungen 2:

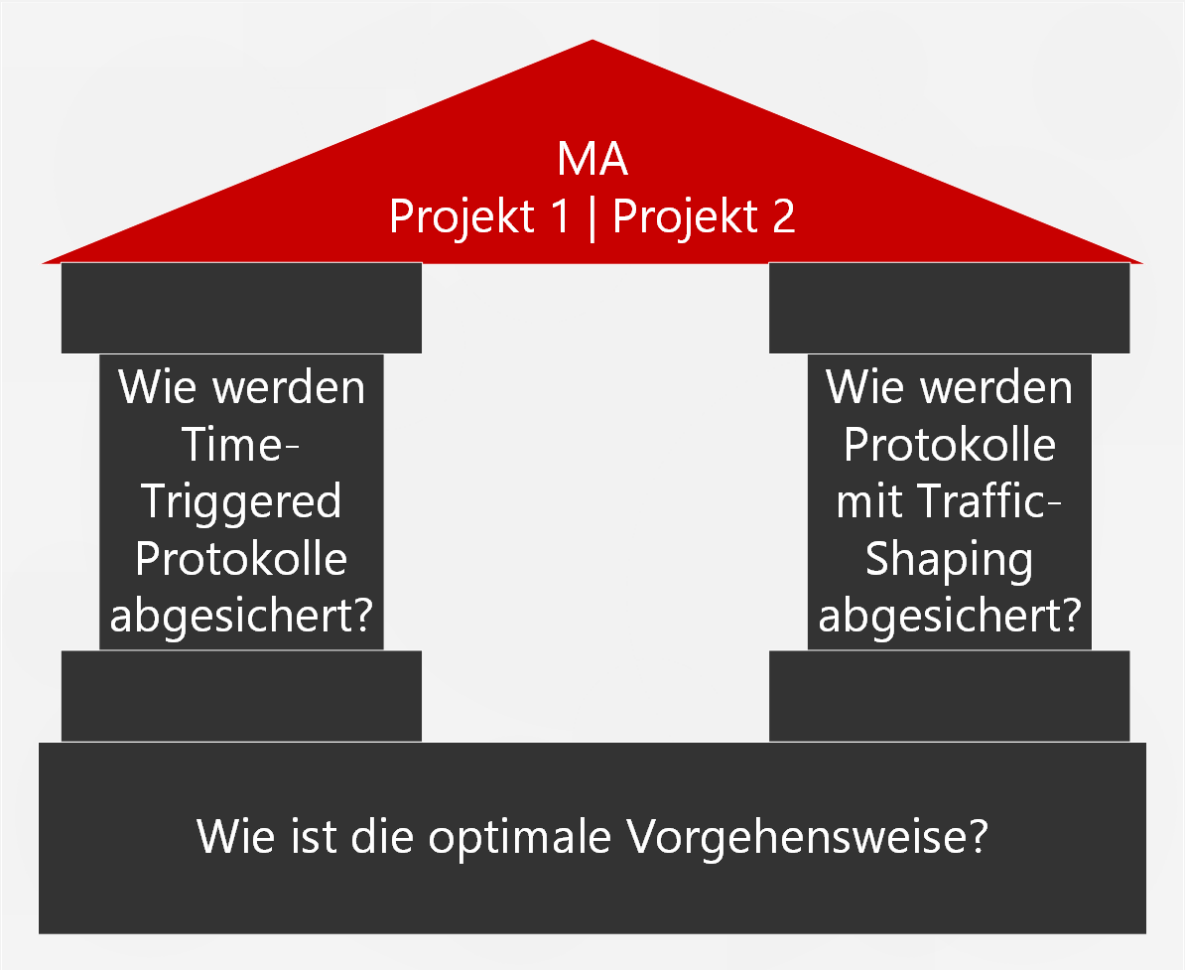
- Wie ist der Stand?
- Welche Bereiche sind abgedeckt?
- Wo sind offene Bereiche?

Masterarbeit (+ Projekt 1 & Projekt 2):

- Schwachstellen im Protokoll aufdecken
- Informationssicherheit des Protokolls verbessern

Zielsetzung & Problemstellung

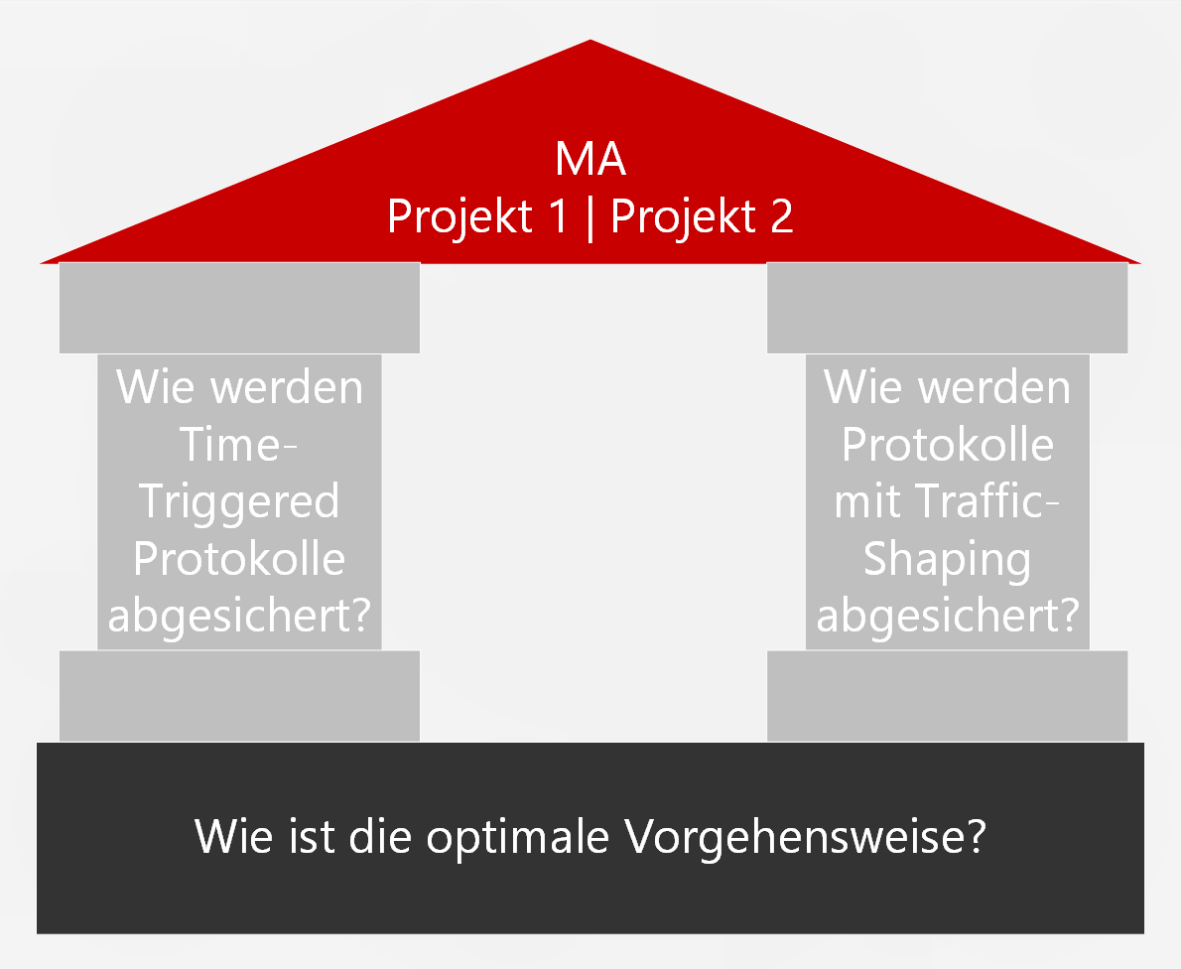
Probleme



Agenda

Vorgehensmodelle

Einordnung



Vorgehensmodelle

Überblick

- IT-Grundschutz-Kataloge[2]
- ISO 27001[3]
- IT-Sicherheit Konzepte - Verfahren - Protokolle[4]
- Security requirements for automotive on-board networks[5]

[2] Bundesamt fuer Sicherheit in der Informationstechnik: *IT-Grundschutz-Kataloge*.

[3] ISO: *Information technology – Security techniques – Information security management systems – Requirements*. 2013.

[4] Claudia Eckert: *IT-Sicherheit Konzepte - Verfahren - Protokolle*. 2013.

[5] Olaf Henniger u. a.: „Security requirements for automotive on-board networks“. 2009.

Vorgehensmodelle

Olaf Henniger u.a. [3]

Analyseprozess:

1. Bedrohungen identifizieren
2. Anforderungen zum eliminieren der Bedrohung identifitzieren
3. Risiken der Bedrohungen bewerten
4. Auf Basis der Risiken die Sicherheitsanforderungen priorisieren

Vorgehensmodelle

Bedrohungen & Anforderungen identifizieren

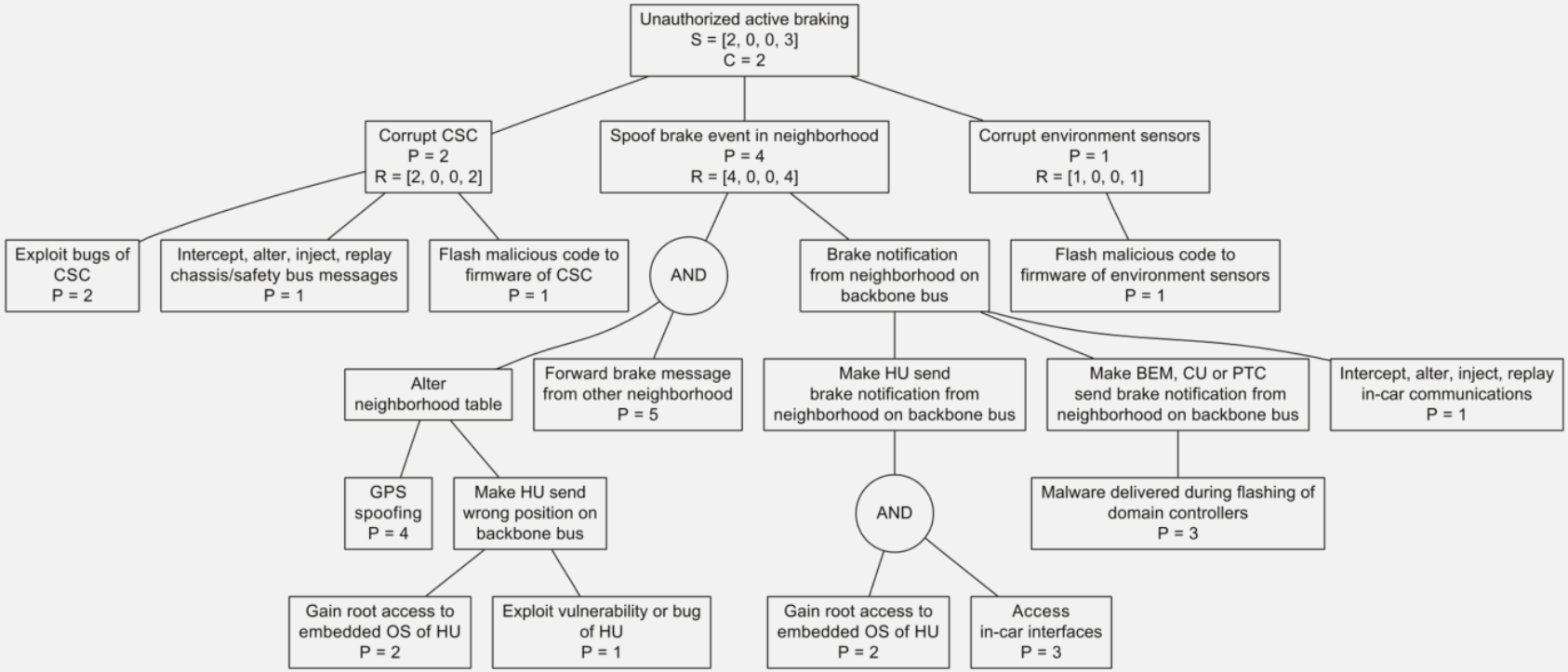


Abbildung: Bedrohungsbaum für unauthorisiertes Bremsen[6]

[6] Olaf Henniger u. a.: „Security requirements for automotive on-board networks“. 2009.

Vorgehensmodelle

Risiken bewerten

- Es ist schwierig Faktoren zu Quantifizieren die das Risiko ausmachen
- Beispiel: $\textit{Risiko} = \textit{Schaden} * \textit{Eintrittswahrscheinlichkeit}$
  - Eintrittswahrscheinlichkeit zwischen 0 und 1
  - Schaden: Finanziell? Ruf? Am Menschen? Mischung?

Vorgehensmodelle

Risiken bewerten

unauthorisiertes Bremsen: S = [2, 0, 0, 3]

Security threat severity class	Aspects of security threats			
	Safety	**Privacy**	**Financial**	**Operational**
0	No injuries	No unauthorized access to data	No financial loss	No impact on operational performance
1	Light or moderate injuries	Anonymous data only (no specific driver of vehicle data)	Low-level loss ($\approx$ €10)	Impact not discernible to driver
2	Severe injuries (survival probable); light/moderate injuries for multiple vehicles	Identification of vehicle or driver; anonymous data for multiple vehicles	Moderate loss ($\approx$ €100); low losses for multiple vehicles	Driver aware of performance degradation; indiscernible impacts for multiple vehicles
3	Life threatening (survival uncertain) or fatal injuries; severe injuries for multiple vehicles	Driver or vehicle tracking; identification of driver or vehicle for multiple vehicles	Heavy loss ($\approx$ €1000); moderate losses for multiple vehicles	Significant impact on performance; noticeable impact for multiple vehicles
4	Life threatening or fatal injuries for multiple vehicles	Driver or vehicle tracking for multiple vehicles	Heavy losses for multiple vehicles	Significant impact for multiple vehicles

Abbildung: Schadensgewichtung[7]

[7] Olaf Henniger u. a.: „Security requirements for automotive on-board networks“. 2009.

Vorgehensmodelle

Sicherheitsanforderungen priorisieren

Security risk level		$P=1$	$P=2$	$P=3$	$P=4$	$P=5$
$C=1$	$S_i=1$	0	0	1	2	3
	$S_i=2$	0	1	2	3	4
	$S_i=3$	1	2	3	4	5
	$S_i=4$	2	3	4	5	6
$C=2$	$S_S=1$	0	1	2	3	4
	$S_S=2$	1	2	3	4	5
	$S_S=3$	2	3	4	5	6
	$S_S=4$	3	4	5	6	7
$C=3$	$S_S=1$	1	2	3	4	5
	$S_S=2$	2	3	4	5	6
	$S_S=3$	3	4	5	6	7
	$S_S=4$	4	5	6	7	7+
$C=4$	$S_S=1$	2	3	4	5	6
	$S_S=2$	3	4	5	6	7
	$S_S=3$	4	5	6	7	7+
	$S_S=4$	5	6	7	7+	7+

Abbildung: Risikogewichtung[8]

Ableitung der Prioritäten aus den jeweiligen Risikogewichtungen

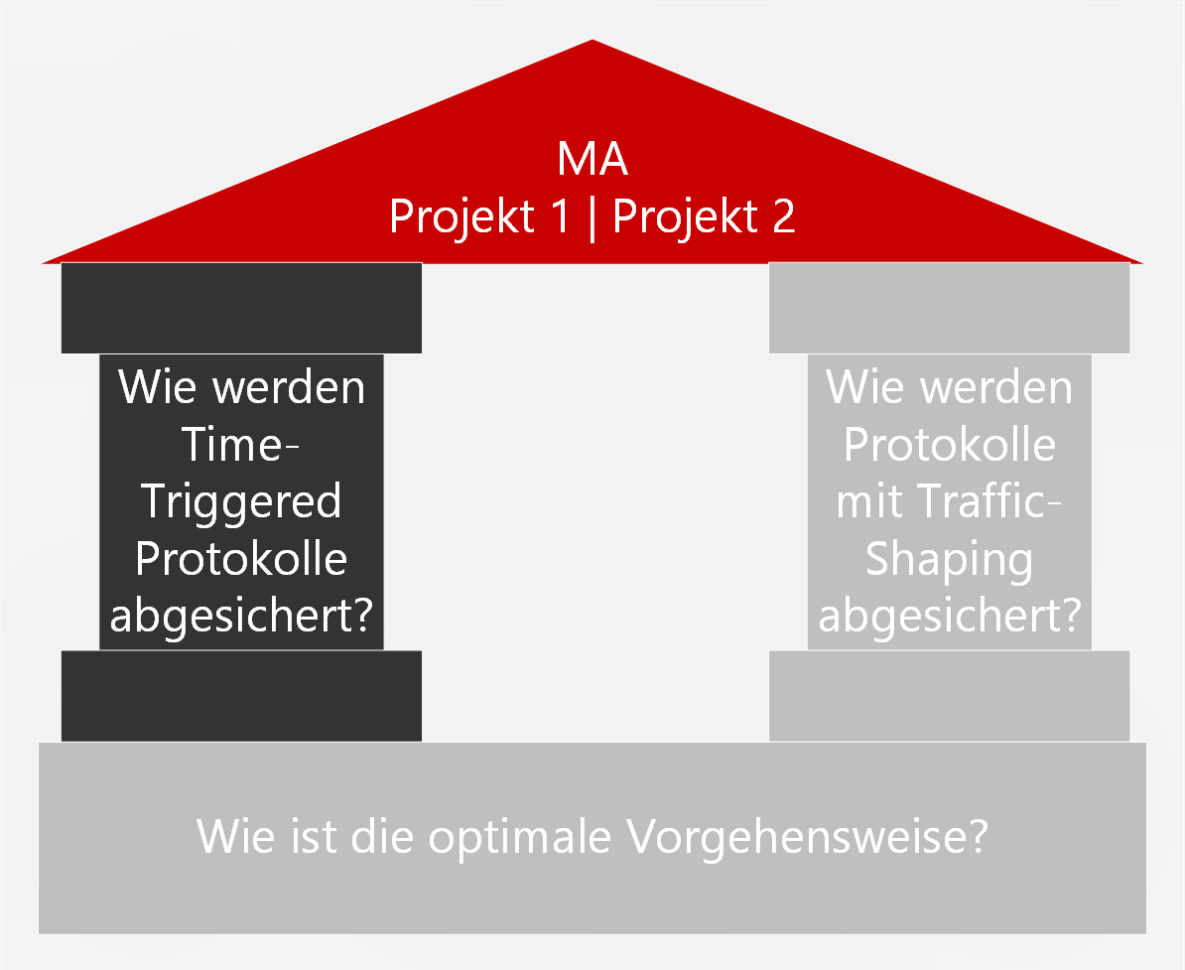
$$S = [2, 0, 0, 2]\ C = 2\ P = 4 => R = [4, 0, 0, 4]$$

[8] Olaf Henniger u. a.:„Security requirements for automotive on-board networks“. 2009.

Agenda

Sicherheit in Time-Triggered Verkehr

Einordnung



Sicherheit im Time-Triggered Verkehr

Überblick

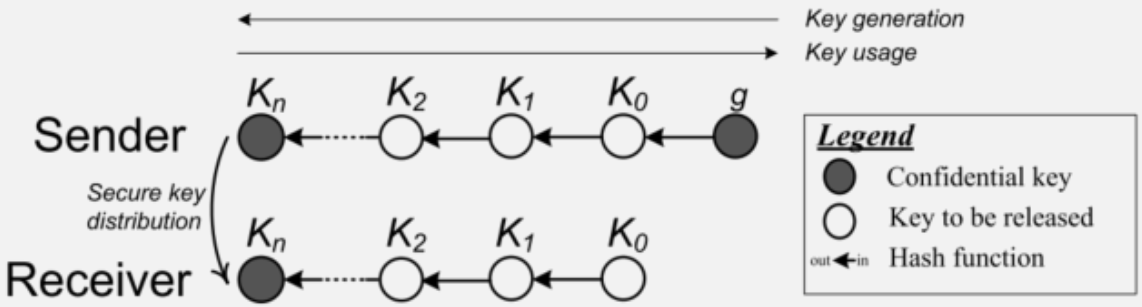
- Kommilitone aus der CoRE-Arbeitsgruppe
- Towards secure time-triggered systems[9]
- Authentication in Time-Triggered Systems Using Time-Delayed Release of Keys[10]

[9] Florian Skopik u. a.:„Towards secure time-triggered systems“. 2012.

[10] Armin Wasicek, Christian El-Salloum und Hermann Kopetz:„Authentication in Time-Triggered Systems Using Time-Delayed Release of Keys“. März 2011.

Sicherheit im Time-Triggered Verkehr

Time-Delayed Release of Keys



- Sichere Assoziation zwischen Schlüsseln
- Berechnung nur in einer Richtung möglich
- Keychain wird prekonfiguriert

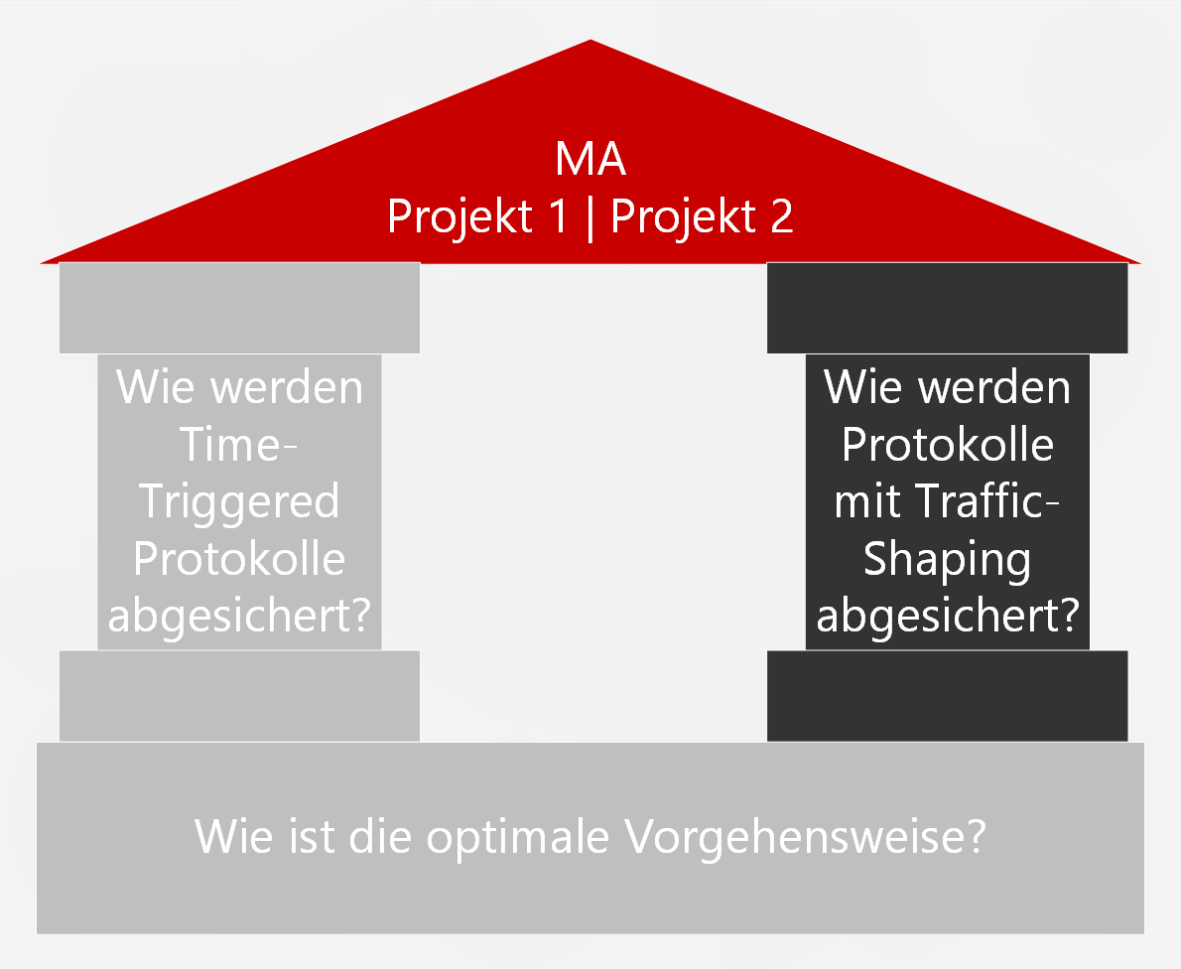
Sicherheit im Time-Triggered Verkehr

- Ein Schlüssel für Alle
- Kein Verlust der Sicherheit
- Tolerant ggb. Paketverlust
- Delay
- Hybrides Verfahren
- Speicher für Nachrichten/Schlüssel notwendig

Agenda

Sicherheit im Traffic-Shaping Verkehr

Einordnung



Sicherheit im Traffic-Shaping Verkehr

Überblick

Stellvertreter:

- Audio/Video Bridging IEEE 802.1Qav[11]
- Time Sensitive Networking IEEE 802.1Qbv Draft[12]

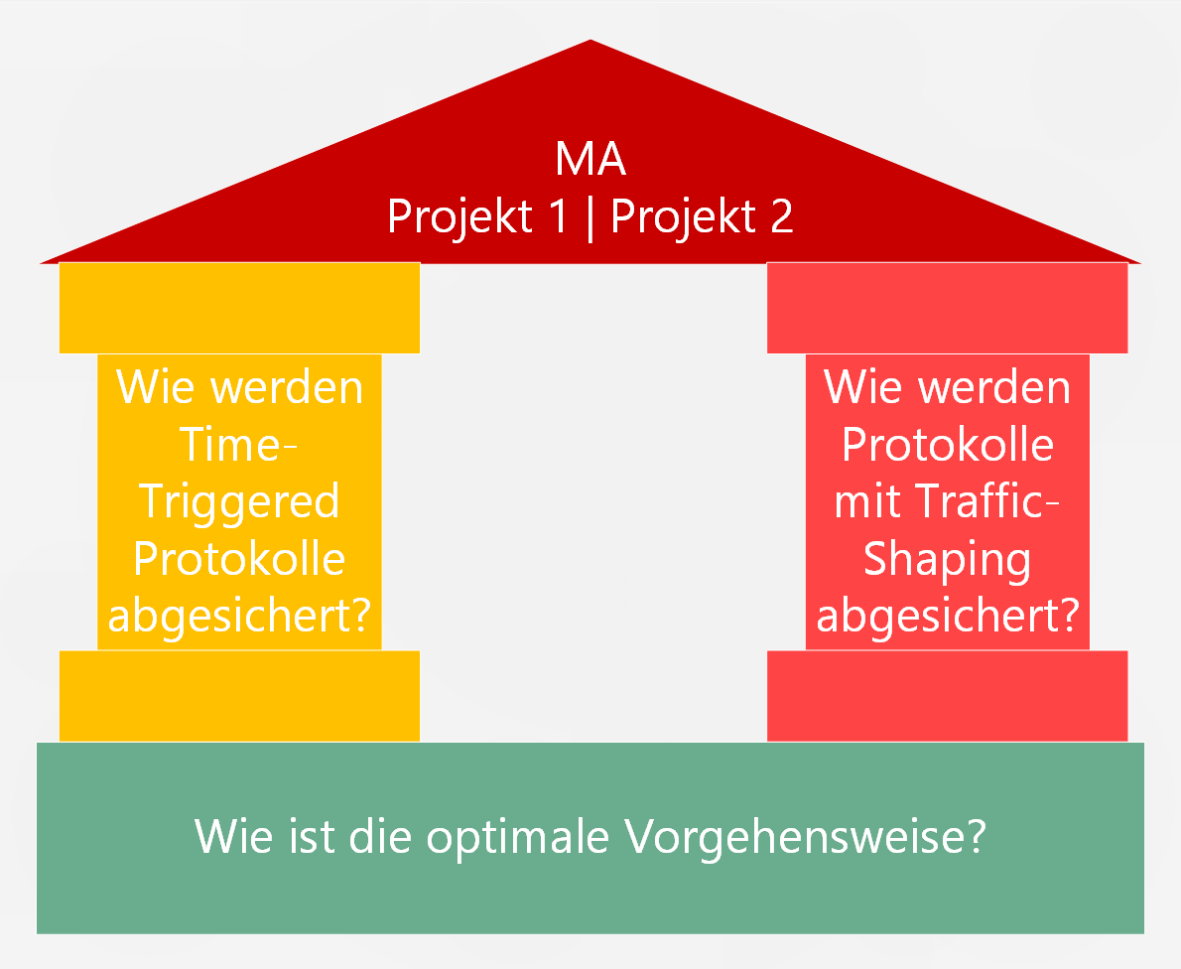
Bisher keine Arbeiten zur Informationssicherheit in diesem Gebiet veröffentlicht.

[11] Institute of Electrical and Electronics Engineers: *IEEE 802.1Qav - IEEE Standard for Local and metropolitan area networks - Virtual Bridged Local Area Networks - Amendment 12: Forwarding and Queuing Enhancements for Time-Sensitive Streams*. Dez. 2009.

[12] IEEE 802.1 TSN Task Group: *IEEE 802.1Qbv - Enhancements for Scheduled Traffic*.

Fazit

Zusammenfassung



Fazit

Risiken

- Vollständigkeit (Ist die Lösung lückenlos?)
- Umsetzbarkeit (Ist die Lösung praktisch anwendbar?)
- Erfahrung (Verlängert den Prozess?)

Fazit

Ausblick

- Projekt 1:
  - Bedrohungen identifizieren
  - Anforderungen identifizieren
  - Anforderungen klassifizieren
  - Methoden zur Absicherung der ersten Anforderungen
- Projekt 2:
  - Vollständigkeit der Anforderungen sicherstellen
  - Umgebung eines Prototypen entwickeln
- Masterarbeit:
  - Konzept für ein sicheres TSN Protokoll
  - Mit Prototyp evaluieren

Anwendungen 2

Informationssicherheit in IEEE 802.1 Time Sensitive Networking Bordnetzen

Literatur I

[1] Bundesamt fuer Sicherheit in der Informationstechnik. *IT-Grundschutz-Kataloge*. URL: www.bsi.de/gshb (besucht am 21. 07. 2014).

[2] Claudia Eckert. *IT-Sicherheit Konzepte - Verfahren - Protokolle*. 8., aktualisierte und korr. Aufl. Muenchen: Oldenbourg, 2013.

[3] Olaf Henniger u. a. „Security requirements for automotive on-board networks“. In: (2009), S. 641–646.

[4] IEEE 802.1 TSN Task Group. *IEEE 802.1 Time-Sensitive Networking Task Group*. URL: http://www.ieee802.org/1/pages/tsn.html.

[5] IEEE 802.1 TSN Task Group. *IEEE 802.1Qbv - Enhancements for Scheduled Traffic*. URL: http://www.ieee802.org/1/pages/802.1bv.html.

[6] ISO. *Information technology – Security techniques – Information security management systems – Requirements*. Norm. 2013.

Literatur II

[7] Institute of Electrical and Electronics Engineers. *IEEE 802.1Qav - IEEE Standard for Local and metropolitan area networks - Virtual Bridged Local Area Networks - Amendment 12: Forwarding and Queuing Enhancements for Time-Sensitive Streams*. Standard IEEE 802.1Qav-2009. IEEE, Dez. 2009.

[8] Florian Skopik u. a. „Towards secure time-triggered systems“. In: *. . . , Reliability, and Security* (2012), S. 1–8. URL: http://link.springer.com/chapter/10.1007/978-3-642-33675-1_33.

[9] Armin Wasicek, Christian El-Salloum und Hermann Kopetz. „Authentication in Time-Triggered Systems Using Time-Delayed Release of Keys“. In: *2011 14th IEEE International Symposium on Object/Component/Service-Oriented Real-Time Distributed Computing* (März 2011), S. 31–39. DOI: 10.1109/ISORC.2011.14. URL: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=5753589.