Informationssicherheit in Echtzeit-Ethernet Bordnetzen

Master Seminar

Stephan Phieler
stephan.phieler@haw-hamburg.de

Hochschule für Angewandte Wissenschaften Hamburg

16. Dezember 2014

Hochschule für Angewandte Wissenschaften Hamburg
Hamburg University of Applied Sciences

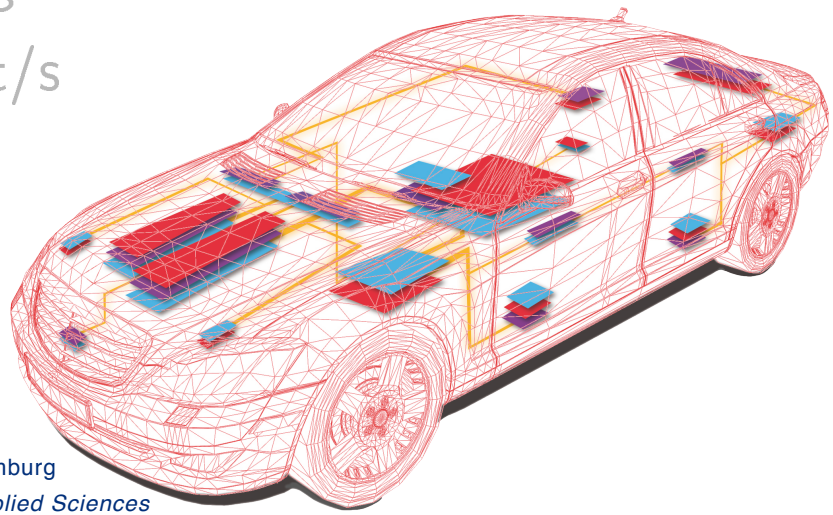
Agenda

Agenda

Motivation

- Verteilte eingebettete Systeme
- Heterogenes Netzwerk/ Bussystem
- Bandbreite $\ll$ 1Gbit/s
- Unsicher [Wol09, HAF+09, KCR+10, CMK+11, TW12, SNAD13, SNA+13]

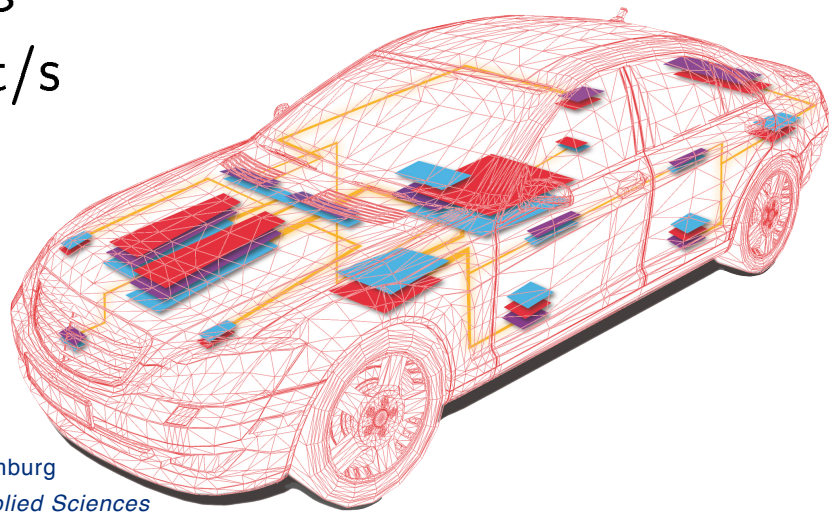
- Homogenes (Echtzeit-)Ethernet Netzwerk
- Massive Generierung von Informationen
- Bandbreite $\gg$ 1Gbit/s
- Safety und Security



Motivation

- Verteilte eingebettete Systeme
- Heterogenes Netzwerk/ Bussystem
- Bandbreite $\ll$ 1Gbit/s
- Unsicher [Wol09, HAF+09, KCR+10, CMK+11, TW12, SNAD13, SNA+13]

- Homogenes (Echtzeit-)Ethernet Netzwerk
- Massive Generierung von Informationen
- Bandbreite $\gg$ 1Gbit/s
- Safety und Security



Ziel der Arbeit

Projekt 1

- Sichere Synchronisation im Echtzeit-Ethernet Bordnetz

Projekt 2

- Sichere Kommunikation im Echtzeit-Ethernet Bordnetz

Masterarbeit

- Konzept zur Absicherung des Echtzeit-Ethernet Bordnetz

Ziel der Arbeit

Projekt 1

- Sichere Synchronisation im Echtzeit-Ethernet Bordnetz

Projekt 2

- Sichere Kommunikation im Echtzeit-Ethernet Bordnetz

Masterarbeit

- Konzept zur Absicherung des Echtzeit-Ethernet Bordnetz

Ziel der Arbeit

Projekt 1

- Sichere Synchronisation im Echtzeit-Ethernet Bordnetz

Projekt 2

- Sichere Kommunikation im Echtzeit-Ethernet Bordnetz

Masterarbeit

- Konzept zur Absicherung des Echtzeit-Ethernet Bordnetz

Agenda

Echtzeit-Ethernet

- Time Division Multiple Access (TDMA)
- Statisch konfiguriertes Netzwerk
- Virtual Links
- 3 Nachrichtenklassen (TT[1], RC[2], BE[3])
- 1 Nachrichtenklassen für Synchronisation (PCF[4])

[1] Time Triggered
[2] Rate Constrained
[3] Best Effort
[4] Protocol Control Frame

Synchronisation

Time-Triggered Ethernet [SAE09]

- Master/ Slave
- Resourcenschonend(er)
- Nur eine Nachricht (PCF)

Synchronisation

Time-Triggered Ethernet [SAE09]

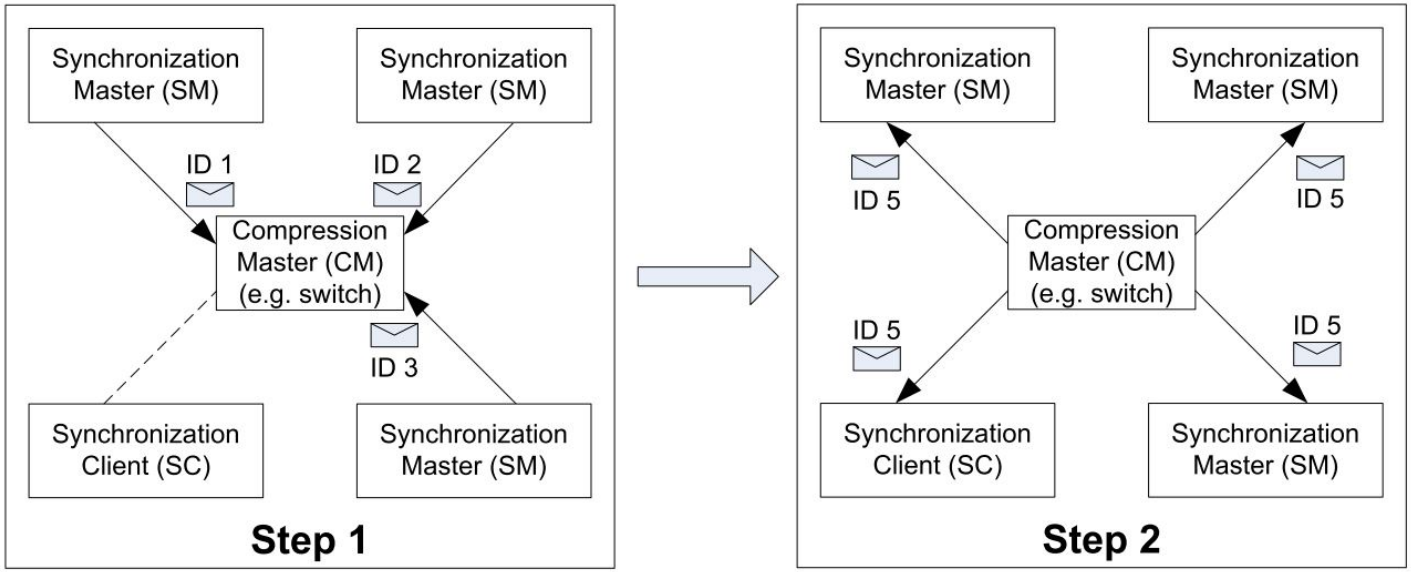


Abbildung: Synchronisation (Bildquelle: [SAE09])

Synchronisation

Precision Time Protocol (PTP) [SM08]

- Master/ Slave und Peer-to-Peer
- Hohe Genauigkeit ($2^{-16} ns$)
- Resourcenschonend
- Grundlegendes Sicherheitskonzept (Annex K)
  - Bildung von SA[5]
  - Nutzung von ICV[6]
  - Security-(Un)Aware Switch
  - Security-Capable Switch

[5] Security Assosiation

[6] Integrity Check Value

Precision Time Protocol (PTP) [SM08]

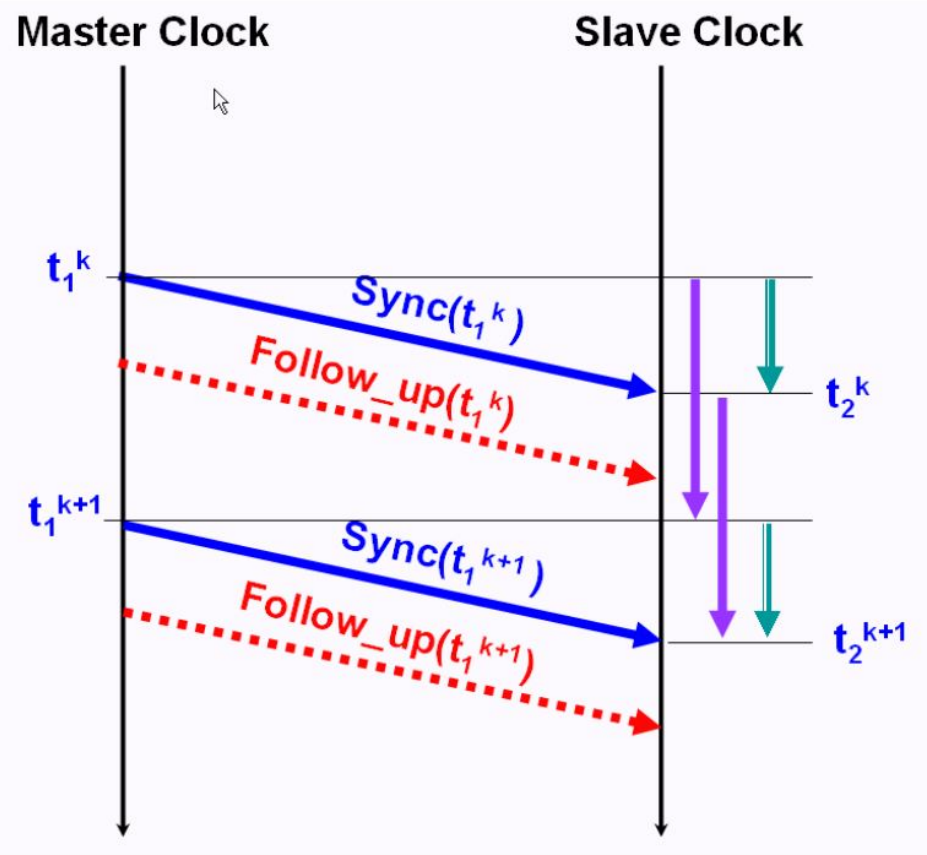


Abbildung: Syntonization (Bildquelle: [Wei09])

Precision Time Protocol (PTP) [SM08]

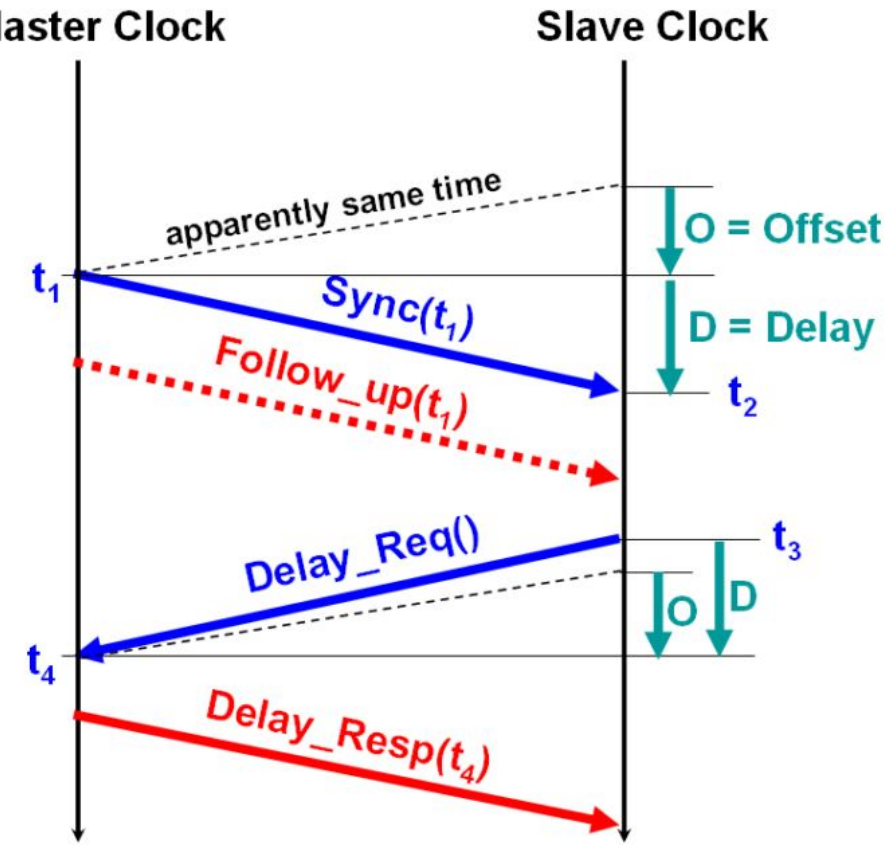


Abbildung: Offset und Delay (Bildquelle: [Wei09])

Synchronisation

Precision Time Protocol (PTP) [SM08]

- Master/ Slave und Peer-to-Peer
- Hohe Genauigkeit ($2^{-16} ns$)
- Resourcenschonend
- Grundlegendes Sicherheitskonzept (Annex K)
  - Bildung von SA[7]
  - Nutzung von ICV[8]
  - Security-(Un)Aware Switch
  - Security-Capable Switch

[7] Security Assosiation

[8] Integrity Check Value

Agenda

Entwurf eines Sicherheitskonzepts

Beachten von ...

- ... Gesetzen
- ... Normen

Vorgehensweise

1. Angriffsziele erfassen
2. Risikoanalyse
3. Bedrohungsanalyse
4. Gegenmaßnahmen erarbeiten

Entwurf eines Sicherheitskonzepts

Beachten von ...

- ... Gesetzen
- ... Normen

Vorgehensweise

1. Angriffsziele erfassen
2. Risikoanalyse
3. Bedrohungsanalyse
4. Gegenmaßnahmen erarbeiten

Konzeptphasen

3 Phasen nach [Was11]

1. Sichere Initialisierung
2. Sichere Synchronisation
3. Sichere Kommunikation

Konzeptphasen

3 Phasen nach [Was11]

1. Sichere Initialisierung
2. Sichere Synchronisation
3. Sichere Kommunikation

Konzeptphasen

3 Phasen nach [Was11]

1. Sichere Initialisierung
2. Sichere Synchronisation
3. Sichere Kommunikation

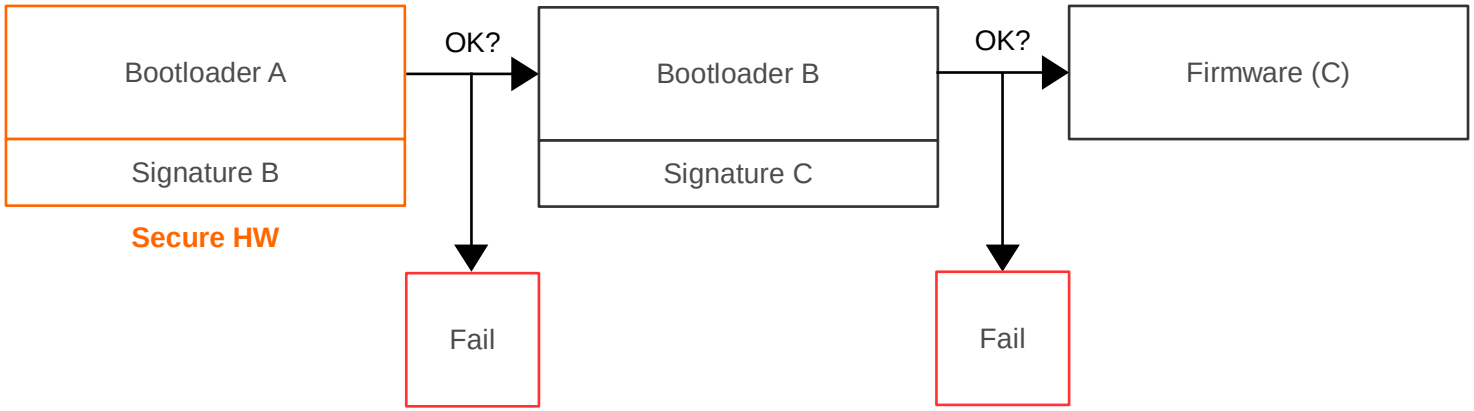
Konzeptphasen

3 Phasen nach [Was11]

1. Sichere Initialisierung
2. Sichere Synchronisation
3. Sichere Kommunikation

Sichere Initialisierung

- Basis für sicheres Netzwerk
- Authentizität und Integrität sicherstellen
- Schwerpunkt BIOS und Firmware
- Einsatz von sicherer Hardware notwendig



Sichere Synchronisation

Angriffsziel:

- Zeit (Kontrolle)

Risiko:

- Ohne Synchronisation kein TDMA

Bedrohungen:

- Übertragung: Manipulation, Delaying, Replaying, ...
- Protokoll: BMC[9]-Algorithmus, SA[10], TC[11], ...

[9] Best Master Clock
[10] Security Association
[11] Transparent Clock

Sichere Synchronisation

Angriffsziel:

- Zeit (Kontrolle)

Risiko:

- Ohne Synchronisation kein TDMA

Bedrohungen:

- Übertragung: Manipulation, Delaying, Replaying, ...
- Protokoll: BMC[9]-Algorithmus, SA[10], TC[11], ...

[9] Best Master Clock
[10] Security Association
[11] Transparent Clock

Sichere Synchronisation

Angriffsziel:

- Zeit (Kontrolle)

Risiko:

- Ohne Synchronisation kein TDMA

Bedrohungen:

- Übertragung: Manipulation, Delaying, Replaying, ...
- Protokoll: BMC[9]-Algorithmus, SA[10], TC[11], ...

[9] Best Master Clock
[10] Security Association
[11] Transparent Clock

Sichere Synchronisation

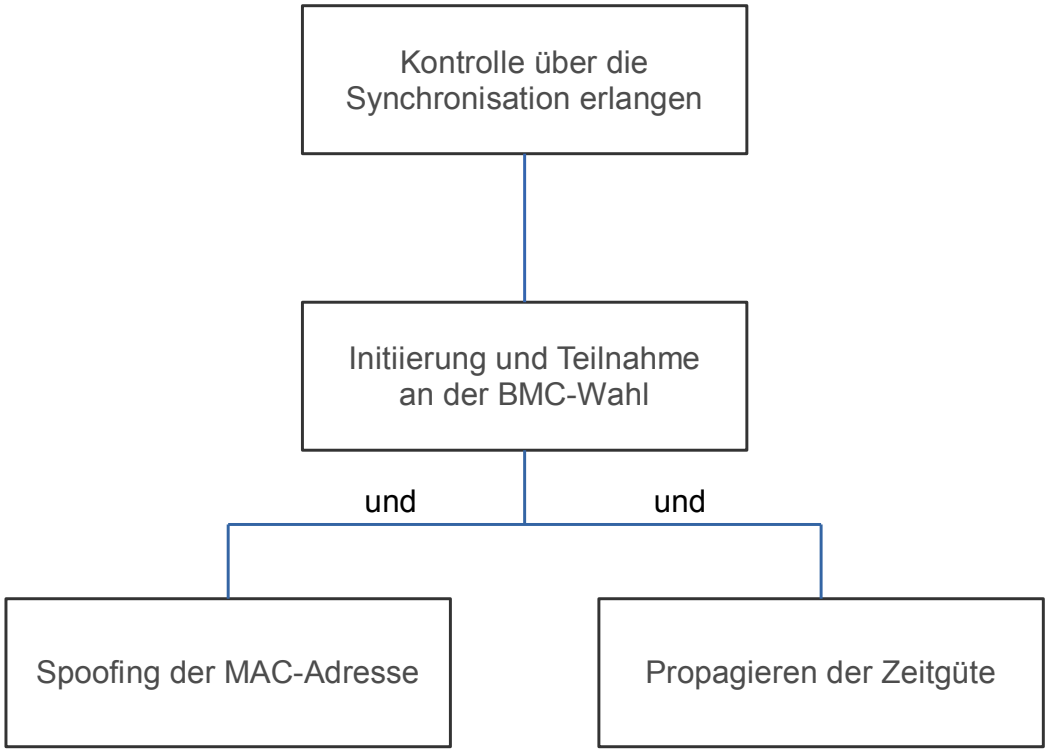
Gegenmaßnahmen:

- Statik
- Authentifizierung und Integritätschecks
- Verschlüsselung
- Monitoring
- Plausabilitätschecks
- ...

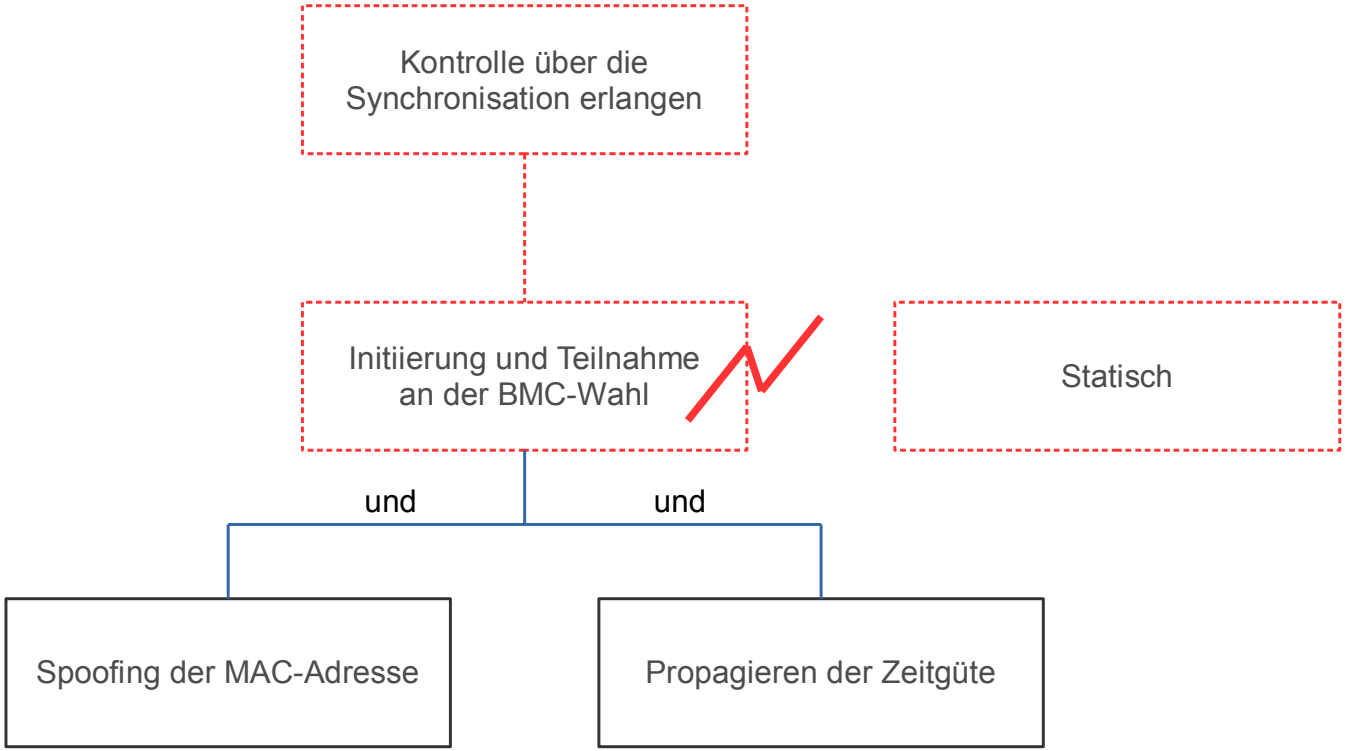
Vorraussetzungen:

- Sichere Initialisierung

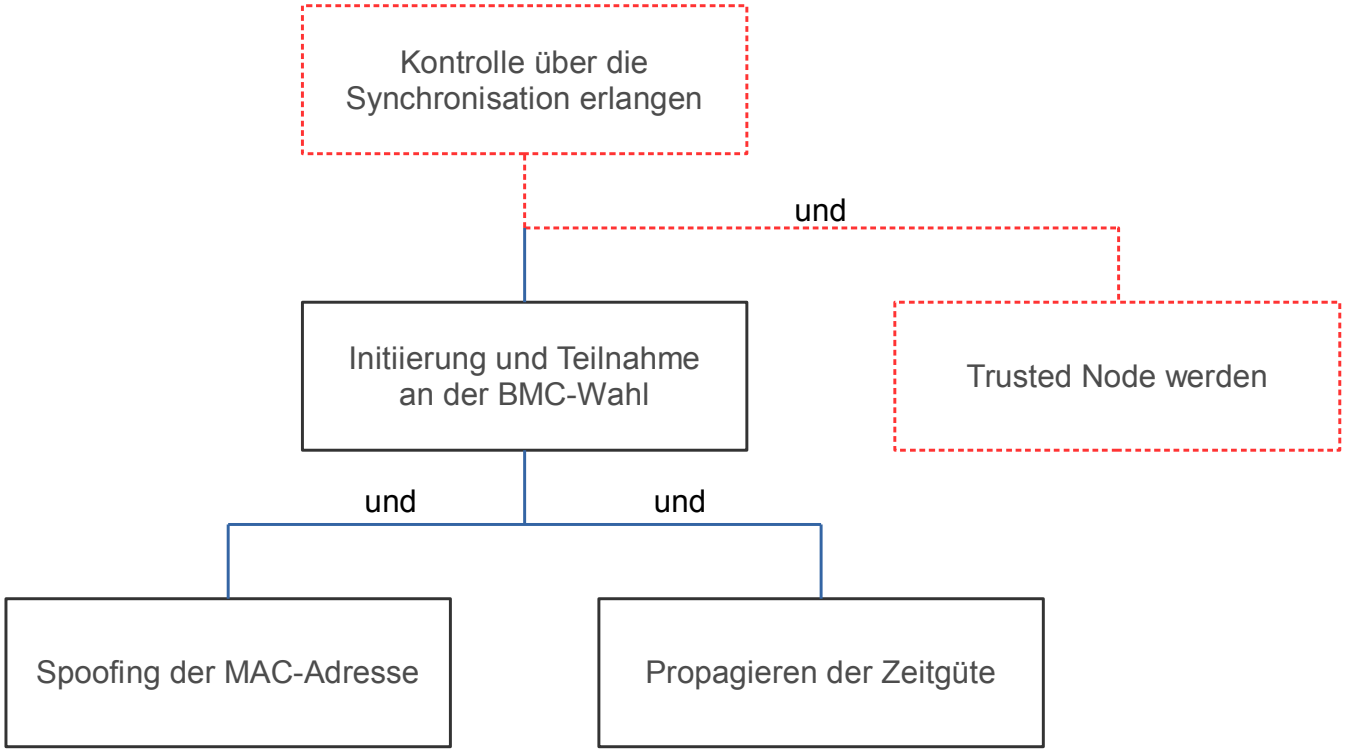
Sichere Synchronisation



Sichere Synchronisation



Sichere Synchronisation



Sichere Kommunikation

Angriffsziel:

- Hinzufügen von Funktionen
- Umgehen von Sperren

Risiko:

- Je nach Funktion/ Beschränkung

Bedrohungen:

- Übertragung: Manipulation, Delaying, Replaying, ...
- Protokoll: (work in progress)

Sichere Kommunikation

Angriffsziel:

- Hinzufügen von Funktionen
- Umgehen von Sperren

Risiko:

- Je nach Funktion/ Beschränkung

Bedrohungen:

- Übertragung: Manipulation, Delaying, Replaying, ...
- Protokoll: (work in progress)

Sichere Kommunikation

Angriffsziel:

- Hinzufügen von Funktionen
- Umgehen von Sperren

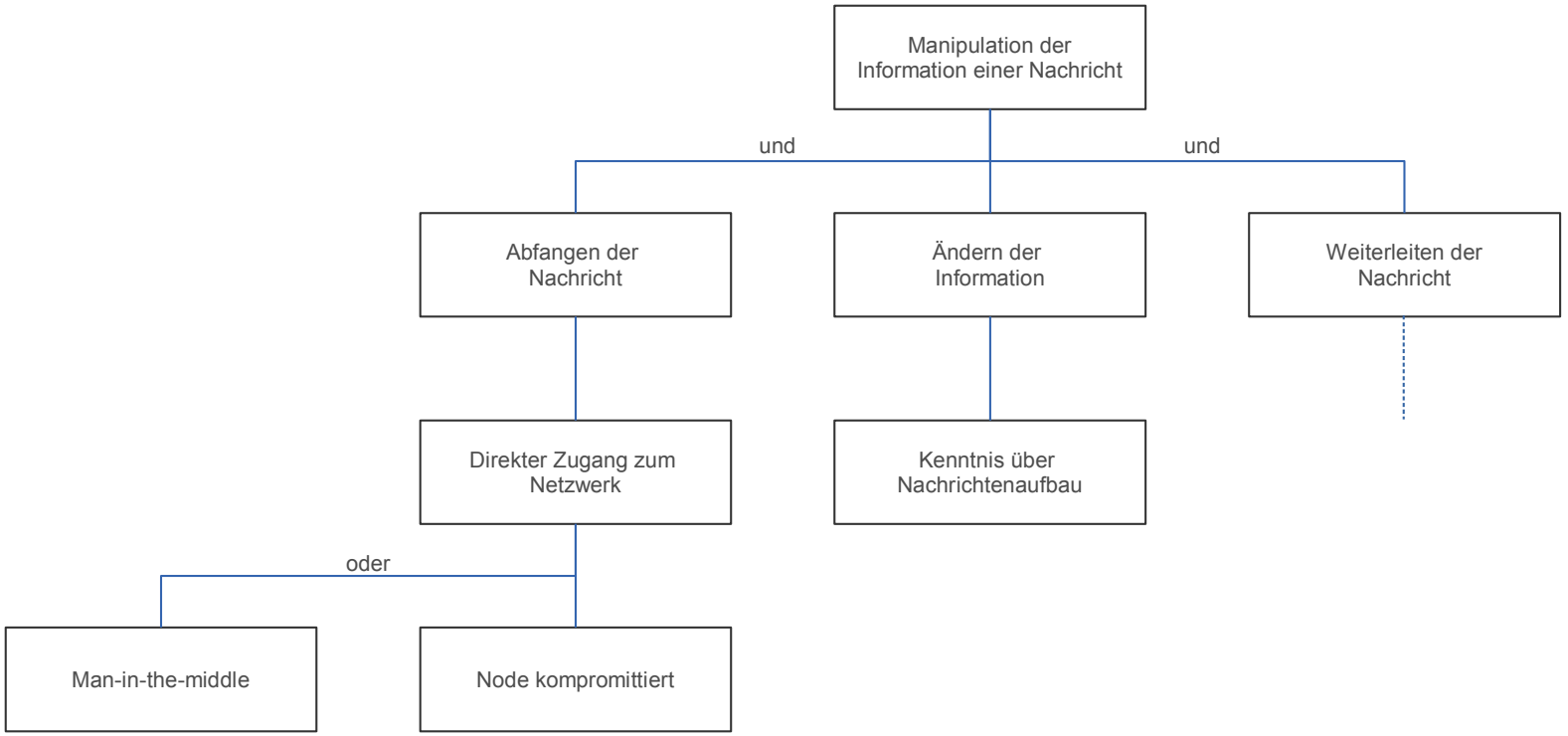
Risiko:

- Je nach Funktion/ Beschränkung

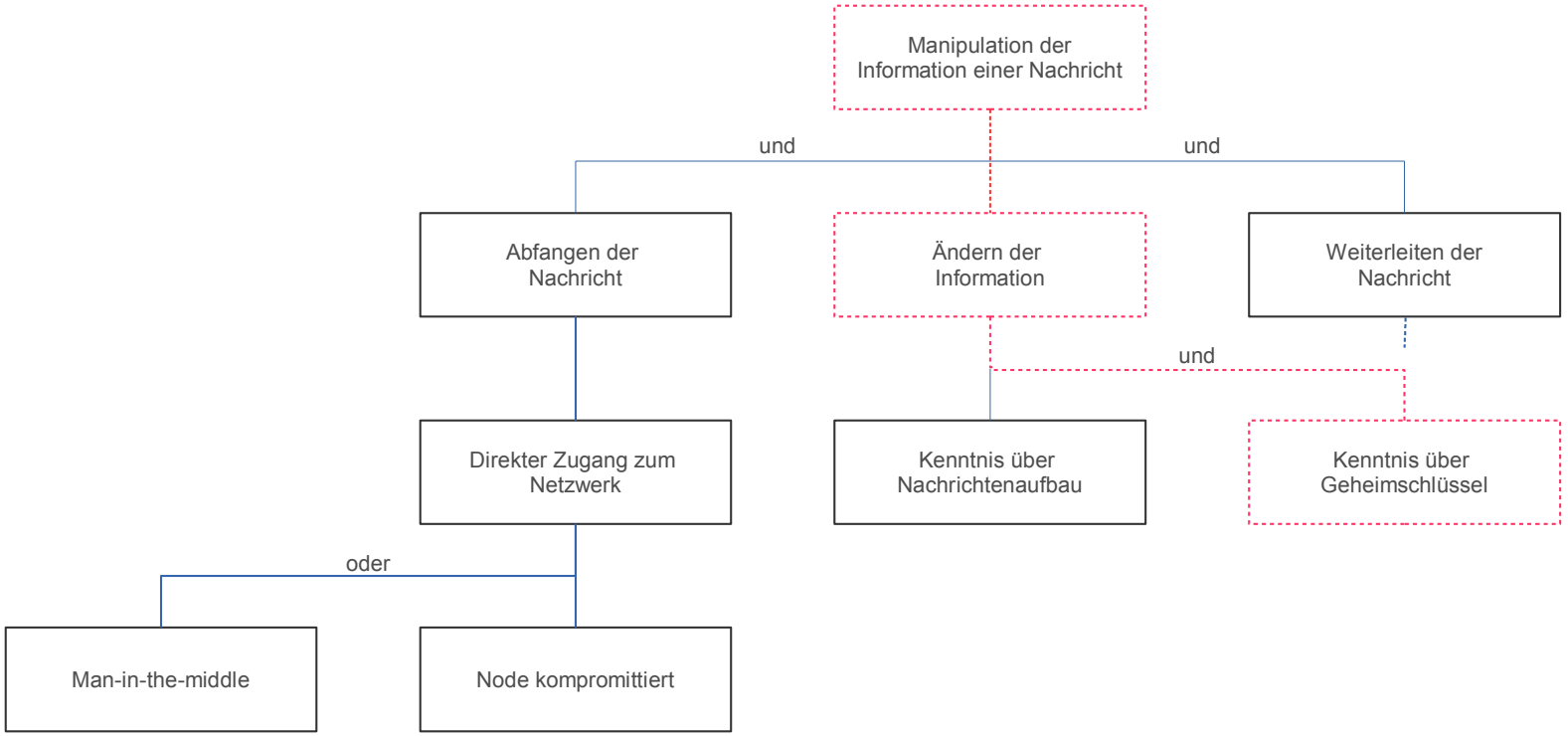
Bedrohungen:

- Übertragung: Manipulation, Delaying, Replaying, ...
- Protokoll: (work in progress)

Sichere Kommunikation



Sichere Kommunikation



Sichere Kommunikation

Gegenmaßnahmen:

- Statik
- Authentifizierung und Integritätschecks
- Verschlüsselung
- Monitoring
- Plausabilitätschecks
- ...

Vorraussetzungen:

- Sichere Initialisierung
- Sichere Synchronisierung

Sicherheitskonzept

Ziel:

- Zusammenspiel der Teilkonzepte
- Empfehlung weiterer Gegenmaßnahmen
  - Zwiebel, Honeypot, Sandboxing, ...

Prüfung:

- Sicherheitskonzepte/ -architekturen
- Publikationen
- Experten

Agenda

Risiken

- Vollständigkeit
- Umsetzbarkeit
- Erfahrung

- Beeinträchtigung der Synchronisation
- Beeinträchtigung der TT-Kommunikation

Risiken

- Vollständigkeit
- Umsetzbarkeit
- Erfahrung

- Beeinträchtigung der Synchronisation
- Beeinträchtigung der TT-Kommunikation

Risiken

- Vollständigkeit
- Umsetzbarkeit
- Erfahrung

- Beeinträchtigung der Synchronisation
- Beeinträchtigung der TT-Kommunikation

Risiken

- Vollständigkeit
- Umsetzbarkeit
- Erfahrung

- Beeinträchtigung der Synchronisation
- Beeinträchtigung der TT-Kommunikation

Agenda

Zusammenfassung & Ausblick

Zusammenfassung:

- Bedarf an Sicherheitkonzepten
- 3 Phasen (Init, Sync, Comm)
- Protokollsicherheit
- Kommunikationssicherheit

Ausblick:

- Umsetzung des Konzeptes
- Simulation

Zusammenfassung & Ausblick

Zusammenfassung:

- Bedarf an Sicherheitkonzepten
- 3 Phasen (Init, Sync, Comm)
- Protokollsicherheit
- Kommunikationssicherheit

Ausblick:

- Umsetzung des Konzeptes
- Simulation

Zusammenfassung & Ausblick

Zusammenfassung:

- Bedarf an Sicherheitkonzepten
- 3 Phasen (Init, Sync, Comm)
- Protokollsicherheit
- Kommunikationssicherheit

Ausblick:

- Umsetzung des Konzeptes
- Simulation

Vielen Dank

Vielen Dank für die Aufmerksamkeit!

[CMK+11] 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.** (2011)

[HAF+09] Henniger, Olaf ; Apvrille, Ludovic ; Fuchs, Andreas ; Roudier, Yves ; Ruddle, Alastair ; Weyl, Benjamin ; Paristech, Telecom ; Ltci, Cnrs ; Antipolis, Sophia: **Security requirements for automotive on-board networks.** (2009), S. 641–646.

ISBN 9781424453474

[KCR+10] Koscher, Karl ; Czeskis, Alexei ; Roesner, Franziska ; Patel, Shwetak ; Kohno, Tadayoshi ; Checkoway, Stephen ; McCoy, Damon ; Kantor, Brian ; Anderson, Danny ; Shacham, Hovav ; Savage, Stefan:
Experimental Security Analysis of a Modern Automobile.
In: *2010 IEEE Symp. Secur. Priv.* (2010), 447–462.
http://dx.doi.org/10.1109/SP.2010.34.
–
DOI 10.1109/SP.2010.34.
ISBN 978–1–4244–6894–2

[SAE09] SAE - AS-2D Time Triggered Systems and Architecture Committee: *Time-Triggered Ethernet (AS 6802)*. http://standards.sae.org/as6802/. Version: 2009

[SM08] Society, IEEE I. ; Measurement: *IEEE Std 1588-2008, IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems*. 2008. – ISBN 9780738154008

[SNA+13] Studnia, Ivan ; Nicomette, Vincent ; Alata, Eric ; Deswarte, Yves ; Kaâniche,

Mohamed ; Laarouchi, Youssef ; Toulouse, F:
Survey on Security Threats and Protection Mechanisms in Embedded Automotive Networks.
(2013)

[SNAD13] Studnia, Ivan ; Nicomette, Vincent ; Alata, Eric ; Deswarte, Yves:
Security of embedded automotive networks : state of the art and a research proposal.
(2013)

[TW12] Tillich, Stefan ; Wójcik, M:
Security analysis of an open car immobilizer protocol stack.

In: *Trust. Syst.* 3 (2012).
http://link.springer.com/chapter/10.1007/978-3-642-35371-0_8

[Was11] Wasicek, A:
Security in time-triggered systems.
2011 (2011).
http://www.informatik.tuwien.ac.at/dekanat/Kurzfassung-Wasicek.pdf

[Wei09] Weibel, Prof H.:
Technology Update on IEEE 1588 : The Second Edition of the High Precision Clock Synchronization Protocol.
(2009), S. 1–8

[Wol09] Wolf, Marko:
Mehr Sicherheit auf unseren Straßen.

(2009), S. 1–8