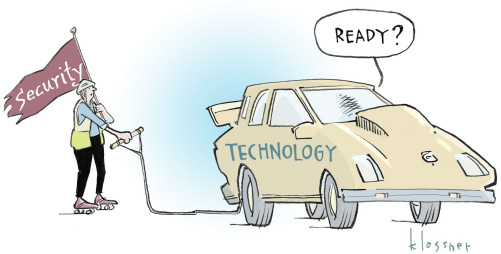
IT-Security in Transportation Systems

DRSS

Dr.-Ing. Christine Jakobs

TU Chemnitz, Professur Betriebssysteme

19.09.2023



Wer bin ich und warum stehe ich hier?

- **Dr.-Ing. Christine Jakobs**
  - Ausbildung zur technischen Assistentin für Informatik
  - Berufserfahrung als Consultant bei Teamix GmbH
  - Bachelor in Betriebswirtschaftslehre und Master in Informatik
  - Ph.D. in Zusammenarbeit mit der AUDI AG
  - Industrieprojekte im Automotivbereich, darunter:
    - Middleware technologies for high integration
    - Modern automotive middleware's for high integration
    - Doktorandenprojekt zur Optimierung des Security-Entwicklungsprozesses bei der AUDI AG
  - Und Forschungsprojekte im Bahnbereich, darunter:
    - Flexible, digitale Systeme für den schienengebundenen Verkehr in Wachstumsregionen
    - KI-bezogene Test- und Zulassungsmethoden

Unsere Zukunft?

Folgen für die Fahrzeugindustrie

- Früher waren die Systeme geschlossene Systeme
  - ➡ keine Kommunikation nach außen
- Heute bzw. zukünftig:
  - Das System ist immer online
  - Kurzstrecken ad hoc Kommunikation zwischen Systemen
  - Kurzstreckenkommunikation mit der Infrastruktur/dem Fahrzeug
  - Langstreckenkommunikation mit dem Backend
- Keine *Closed-World* Annahmen mehr

1 Prozessor

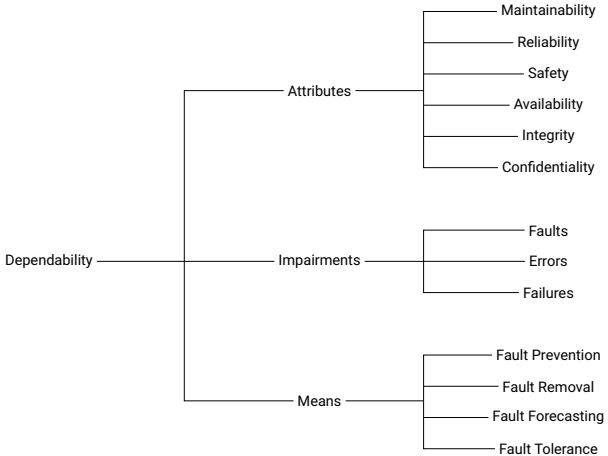
0 Prozessoren

60 Prozessoren
Million Zeilen Code

- ➡ Höhere Anforderungen an die Sicherstellung meta-funktionaler Eigenschaften (Verlässlichkeit)
- Automotive muss Infrastuktur mit beachten, Railway muss Fahrzeuge mit beachten
- ➡ Die Welten wachsen mehr und mehr zusammen

Das Problem der Verlässlichkeit

- Sog. *cross-cutting concerns*
  - ➡ Kein *divide-and-conquer* möglich
- Diverse Terminologien, Forschung folgt meist Laprie
- In Fahrzeugen primär Safety und Security
- Security relativ neues Gebiet (Veröffentlichung Standard Automotive 2021)
  - Früher „nur“ Wegfahrsperre und Diebstahlwarnanlage

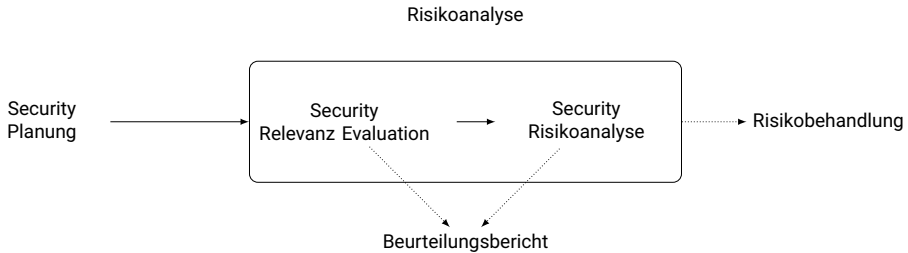


Safety vs. Security

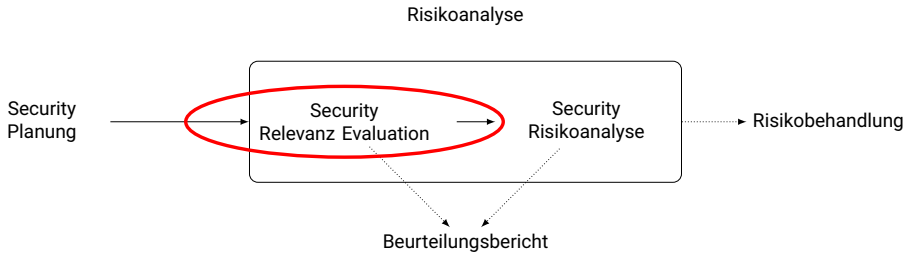
- Eigene Forschungsfelder
  - Eigene Methoden
  - Teilweise konkurrierend
- Gemeinsamkeiten:
  - Begriff des Risikos (Wahrscheinlichkeit, Auswirkungen)
  - Problem des *cross-cutting concerns*
- Safety: Fahrzeug hat keine unerwünschten Auswirkungen auf Fahrer und Umwelt
- Security: Fahrer und Umwelt haben keine unerwünschten Auswirkungen auf das Fahrzeug
- Car2X forciert die Kooperation beider Welten
- Sichere Architekturen erfordern Security-by-design

Bildquelle: *Cyberscurity Ventures*

Security Prozess (linker Schenkel V-Modell)

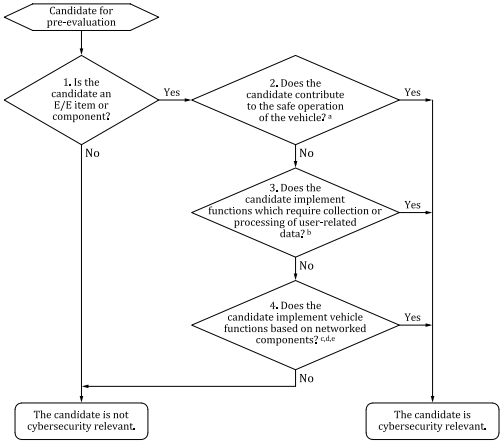


Security Prozess (linker Schenkel V-Modell)



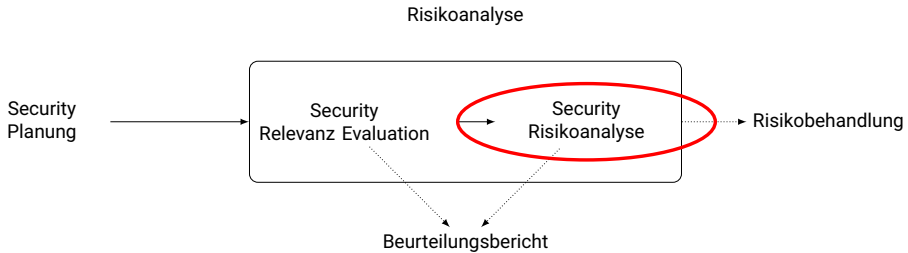
SRE

- Zwei Möglichkeiten: Fragenkatalog oder „rule of thumb“
- Scharfes draufschauen ist meist nicht objektiv
- Analyse muss aber reproduzierbar und nachvollziehbar sein
- ➡ Besser den Fragebogen nutzen



Bildquelle: *ISO/SAE 21434:2021.*

Security Prozess (linker Schenkel V-Modell)



Struktur der Risikoanalyse

Item Definition: Worum geht es?

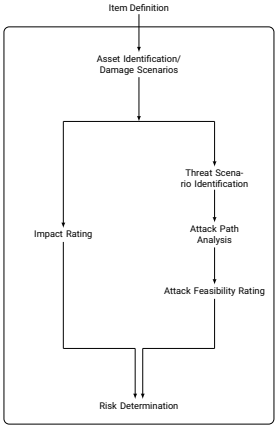
Asset Identification/Damage Scenario: Was kann schief gehen?

Impact Rating: Wie schlimm ist das?

Attacks: Wie kann das passieren?

Feasibility: Wie wahrscheinlich ist das?

Risk: Wie hoch ist das resultierende Risiko?



Struktur der Risikoanalyse

Item Definition: Worum geht es?

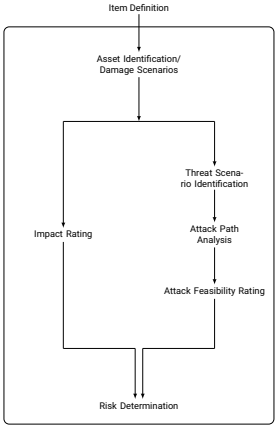
Asset Identification/Damage Scenario: Was kann schief gehen?

Impact Rating: Wie schlimm ist das?

Attacks: Wie kann das passieren?

Feasibility: Wie wahrscheinlich ist das?

Risk: Wie hoch ist das resultierende Risiko?



Struktur der Risikoanalyse

Item Definition: Worum geht es?

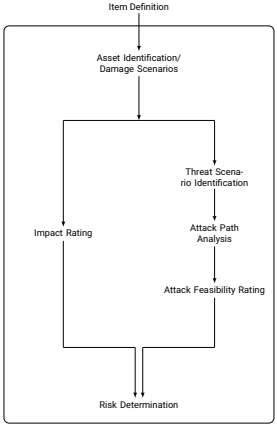
Asset Identification/Damage Scenario: Was kann schief gehen?

Impact Rating: Wie schlimm ist das?

Attacks: Wie kann das passieren?

Feasibility: Wie wahrscheinlich ist das?

Risk: Wie hoch ist das resultierende Risiko?



Struktur der Risikoanalyse

Item Definition: Worum geht es?

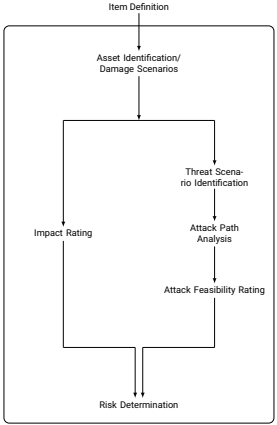
Asset Identification/Damage Scenario: Was kann schief gehen?

Impact Rating: Wie schlimm ist das?

Attacks: Wie kann das passieren?

Feasibility: Wie wahrscheinlich ist das?

Risk: Wie hoch ist das resultierende Risiko?



Struktur der Risikoanalyse

Item Definition: Worum geht es?

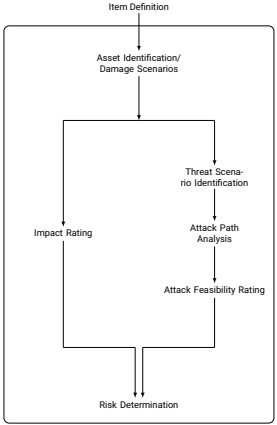
Asset Identification/Damage Scenario: Was kann schief gehen?

Impact Rating: Wie schlimm ist das?

Attacks: Wie kann das passieren?

Feasibility: Wie wahrscheinlich ist das?

Risk: Wie hoch ist das resultierende Risiko?



Struktur der Risikoanalyse

Item Definition: Worum geht es?

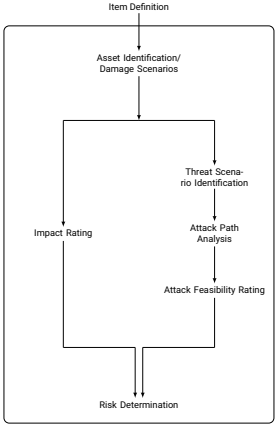
Asset Identification/Damage Scenario: Was kann schief gehen?

Impact Rating: Wie schlimm ist das?

Attacks: Wie kann das passieren?

Feasibility: Wie wahrscheinlich ist das?

Risk: Wie hoch ist das resultierende Risiko?



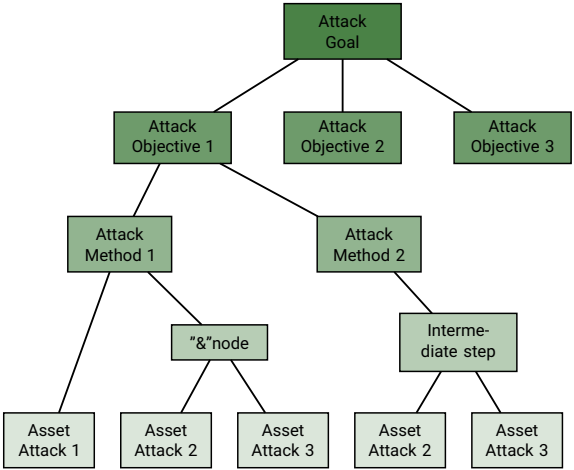
Beispielmethode: Angriffsbäume

Level 0: Attack Goal

Level 1: Attack Objectives

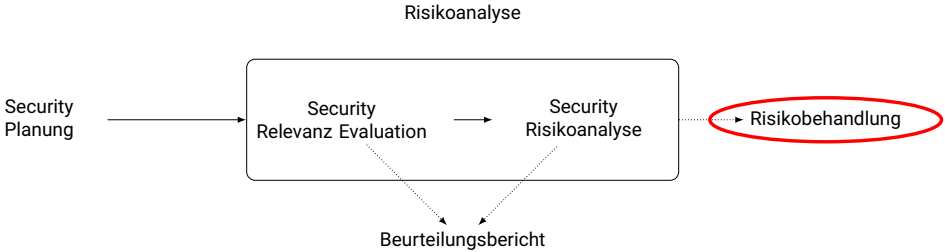
Level 2: Attack Methods

Intermediate or "dummy"nodes



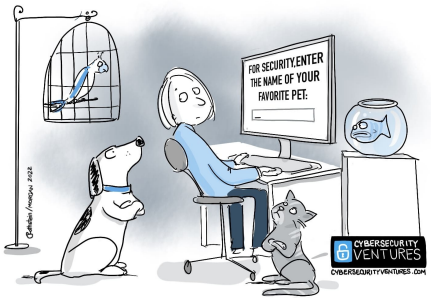
Bildquelle: *Ruddle, Alastair. „Deliverable D2.3: Security requirements for automotive on-board networks based on dark-side scenarios". Project Report. EVITA - E-safety vehicle intrusion protected applications, 30. September 2009.*

Security Prozess (linker Schenkel V-Modell)



Risikobehandlung

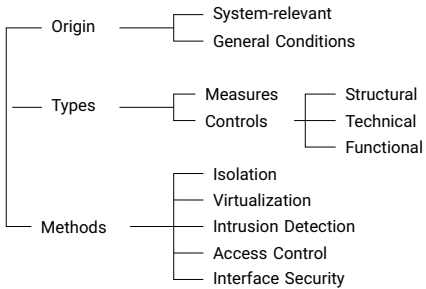
- Basierende auf: Item definition, Angriffspfade und Risiko
- Möglichkeiten:
  - Vermeidung: z.B. Coding Conventions, Datenflüsse verbieten
  - Reduzierung: Einbringen von Maßnahmen
  - Teilung/Akzeptanz: z.B. Versicherung, Ignorieren
- ➡ **Problem:** Manches wird schon vorher eingebracht
- ➡ **Problem:** Ressourcenbeschränkungen



Bildquelle: *Cyberscurity Ventures*

Risikoreduzierung

- Herkunft der Forderungen:
  - Normative Vorgaben z.B. Netzwerksegmentierung
  - Identifizierte Risiken
- Typen von Maßnahmen:
  - Allgemeines Verhalten, Kategorien von Maßnahmen
  - Verschiedene Ebenen
- Maßnahmen:
  - Verschiedene Kategorien und Maßnahmen



Lessons Learned

- Security-Entwicklungsprozesse in Automotive stecken in den Teenagerschuhen
  - Methodik funktioniert
  - Verständnis, Streamlining und Traceability fehlen oft noch
- Standards teilweise wenig hilfreich
  - Methodik
  - Effizienz
- Security-Entwicklungsprozesse und Standards in Railway hinken noch hinterher
- Security-Entwicklung konkurriert mit der funktionalen Entwicklung
  - Zeitlich
  - Funktional
- Gemeinsame Betrachtung Safety und Security fehlt meist gänzlich