Securing the Future
Cybersicherheit in vernetzten Fahrzeugen und Industriesystemen

Thomas Rosenstatter

Department Information Technologies and Digitalisation
Fachhochschule Salzburg

24. November 2025

FH Salzburg

Mein Start in Cybersecurity

2015/16 Halmstad University – Grand Cooperative Driving Challenge

Sicherheit, Säkerhet, Safety und Security

Schutz vor Gefahren und Angriffen:

- Sicherheit (DE)
- Säkerhet (SE)
- Sicurezza (IT)

Sicherheit, Säkerhet, Safety und Security

Schutz vor Gefahren und Angriffen:

- Sicherheit (DE)
- Säkerhet (SE)
- Sicurezza (IT)

Schutz vor Angriffen:

- Security (EN)

Schutz vor Gefahren:

- Safety (EN)

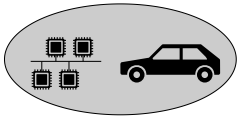
Funktionen im Fahrzeug

Funktionen im Fahrzeug

- Standard-Funktionen:
  Steuern, Beschleunigen, Bremsen

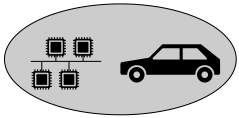
Funktionen im Fahrzeug

- Standard-Funktionen:
  Steuern, Beschleunigen, Bremsen
- Assistenz-Funktionen:
  Tempomat, Parken, Lane-Keeping
- Safety-Funktionen: ABS, Airbag, ESP



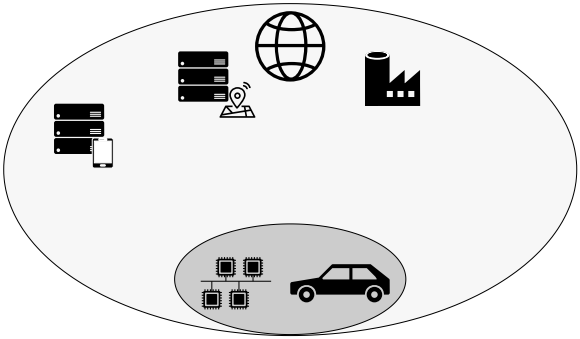
Funktionen im Fahrzeug

- Standard-Funktionen:
  Steuern, Beschleunigen, Bremsen
- Assistenz-Funktionen:
  Tempomat, Parken, Lane-Keeping
- Safety-Funktionen: ABS, Airbag, ESP
- Convenience-Funktionen:
  Klima, Radio, Navigation,
  Smartphone-App für (fast) alles



Funktionen im Fahrzeug

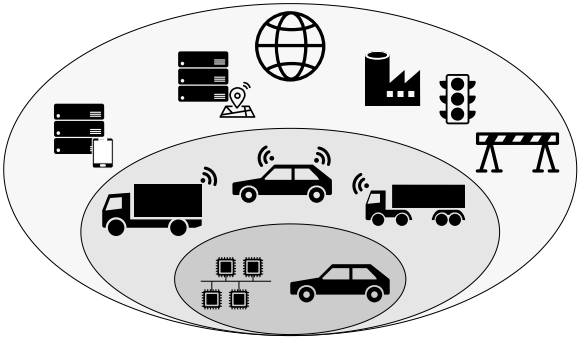
- Standard-Funktionen:
  Steuern, Beschleunigen, Bremsen
- Assistenz-Funktionen:
  Tempomat, Parken, Lane-Keeping
- Safety-Funktionen: ABS, Airbag, ESP
- Convenience-Funktionen:
  Klima, Radio, Navigation,
  Smartphone-App für (fast) alles



Funktionen im Fahrzeug

- Standard-Funktionen:
  Steuern, Beschleunigen, Bremsen
- Assistenz-Funktionen:
  Tempomat, Parken, Lane-Keeping
- Safety-Funktionen: ABS, Airbag, ESP
- Convenience-Funktionen:
  Klima, Radio, Navigation,
  Smartphone-App für (fast) alles

- Verbesserte Safety und Effizienz:
  Vehicle to Everything (V2X)
  Kommunikation



Funktionen in Industriesystemen

1. Steuerung der Aktoren (Motoren, Pumpen, ...)
2. Wahrnehmung der Umwelt (Sensoren)

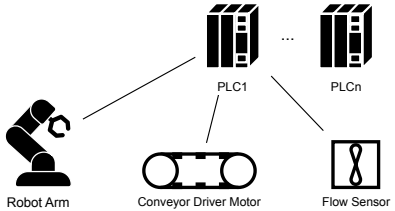

Robot Arm


Conveyor Driver Motor


Flow Sensor

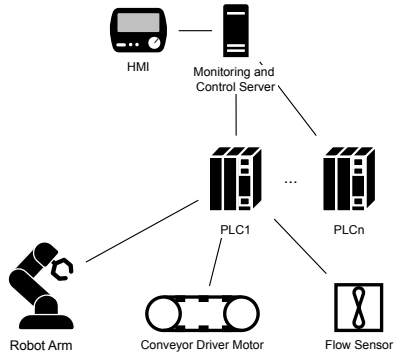
Funktionen in Industriesystemen

1. Steuerung der Aktoren (Motoren, Pumpen, ...)
2. Wahrnehmung der Umwelt (Sensoren)
3. Logik für die Steuerung



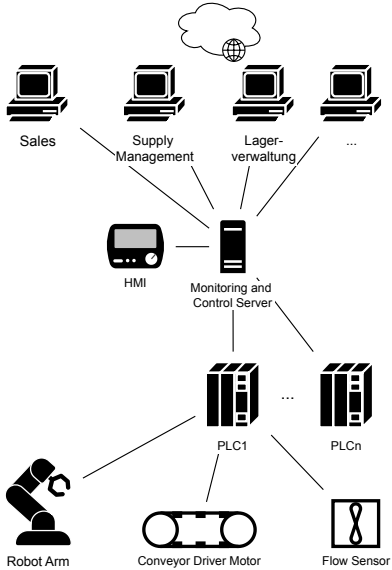
Funktionen in Industriesystemen

1. Steuerung der Aktoren (Motoren, Pumpen, ...)
2. Wahrnehmung der Umwelt (Sensoren)
3. Logik für die Steuerung
4. Überwachung und Adaption des Prozesses
5. Safety

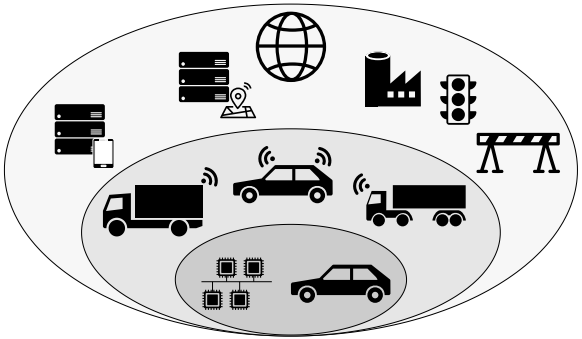


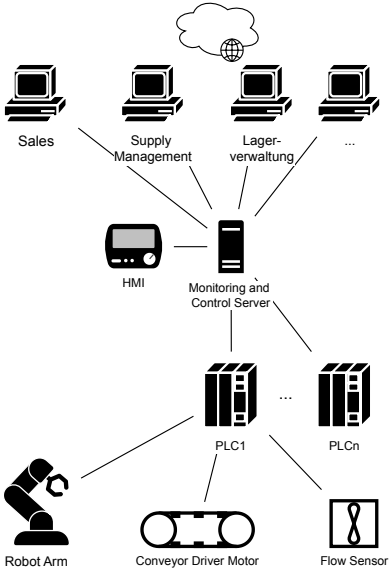
Funktionen in Industriesystemen

1. Steuerung der Aktoren (Motoren, Pumpen, ...)
2. Wahrnehmung der Umwelt (Sensoren)
3. Logik für die Steuerung
4. Überwachung und Adaption des Prozesses
5. Safety
6. Business-Planung (Lagerung, Rohstoffbeschaffung, Kundenaufträge)

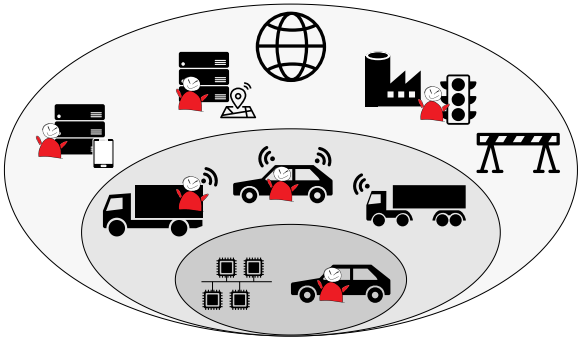


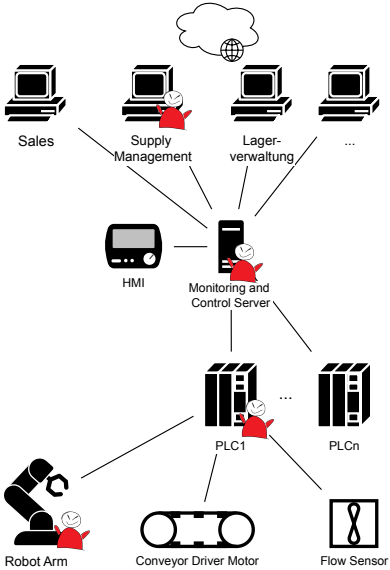
Operational Technology





Operational Technology





Attacken sind nicht nur theoretisch!

SECURITY NEWS POLICY

Sirius XM flaw could've let hackers remotely unlock and start cars

/ Security researcher Sam Curry found an exploit affecting the telematics and infotainment systems powered by Sirius XM. Curry says the company has since fixed the issue.

The Verge, 2022 [Rot22].

Attacken sind nicht nur theoretisch!

SECURITY NEWS POLICY

Sirius XM flaw could've let hackers remotely unlock and start cars

/ Security researcher Sam Curry found an exploit affecting the telematics and infotainment

The Verge, 20

Hackers take Remote Control of Tesla's Brakes and Door locks from 12 Miles Away

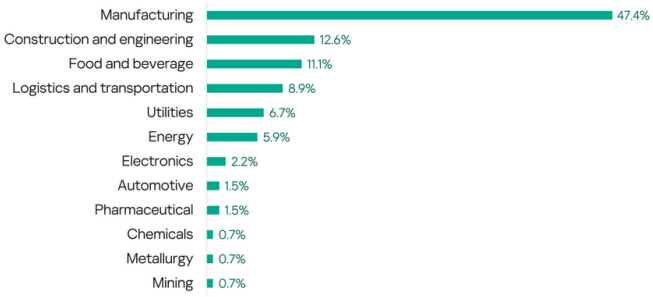
Sep 20, 2016

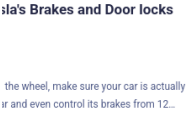
Next time when you find yourself hooked up behind the wheel, make sure your car is actually in your control. Hackers can remotely hijack your car and even control its brakes from 12...

The Hacker News, 2016 [The16].

Attacken sind nicht nur theoretisch!

In Q2 2025, 135 incidents were publicly confirmed by victims. All of these incidents are included in the table at the end of the overview, with select incidents described in detail.





Kaspersky ICS CERT, 2025 [Kas25].

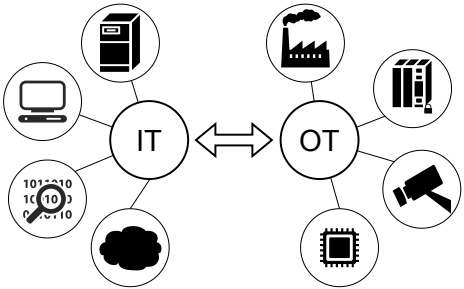
OT != IT

Informationstechnologien

- ist im "Cyberspace"
- T.ex.: PC, Bürogeräte

Operationstechnologien

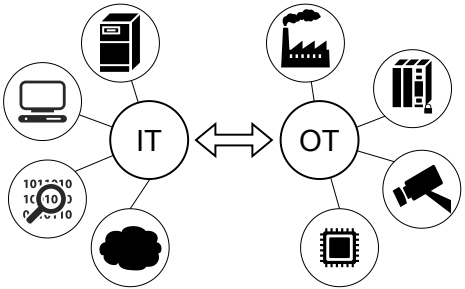
- ist im physischen Raum
- T.ex.: Produktionsanlagen, Transportsysteme



OT != IT

Informationstechnologien

- ist im "Cyberspace"
- T.ex.: PC, Bürogeräte



Operationstechnologien

- ist im physischen Raum
- T.ex.: Produktionsanlagen, Transportsysteme

- Echtzeitanforderungen
- Lebenszyklus
- Safety-kritische Natur
- Verteilte Systeme
- Integration

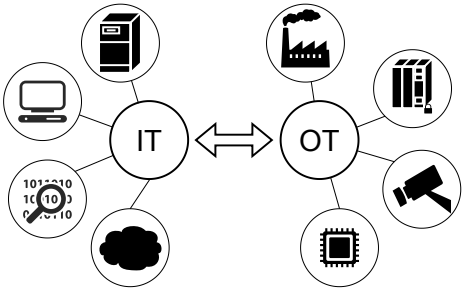
OT != IT

Informationstechnologien

- ist im "Cyberspace"
- T.ex.: PC, Bürogeräte

Operationstechnologien

- ist im physischen Raum
- T.ex.: Produktionsanlagen, Transportsysteme



- Echtzeitanforderungen
- Lebenszyklus
- Safety-kritische Natur
- Verteilte Systeme
- Integration

OT behandelt verteilte, echtzeit-kritische, embedded, cyber-physische Systeme

Threat Analyse

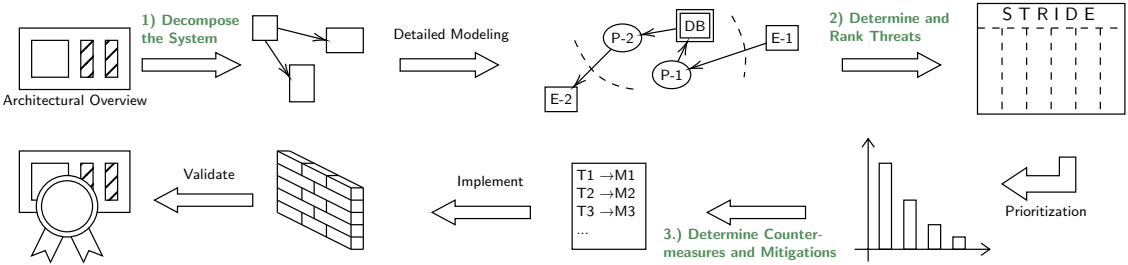


Abbildung: Threat Modeling Workflow [Ros+24].

Threat Analyse

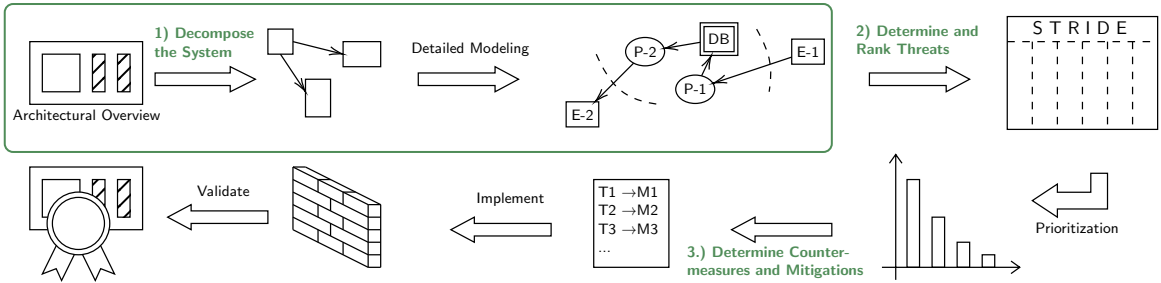


Abbildung: Threat Modeling Workflow [Ros+24].

Beispiel eines Fahrzeuges

1. Systemzerlegung

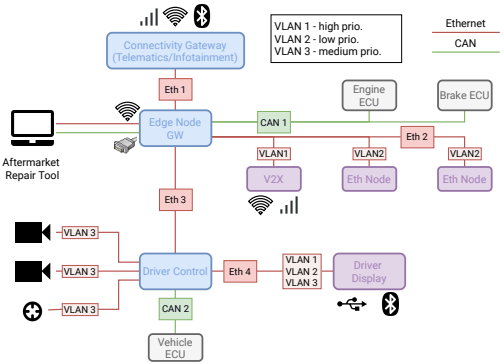


Abbildung: HoliSec Referenzarchitektur des internen Netzwerks [RO18b].

Beispiel eines Fahrzeuges

1. Systemzerlegung

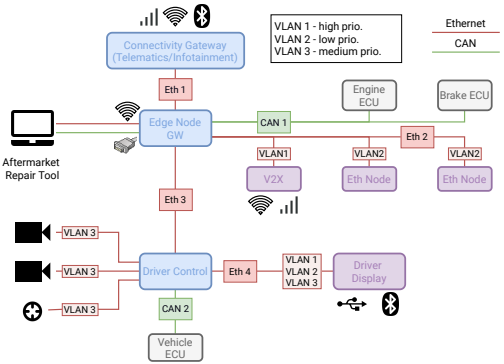
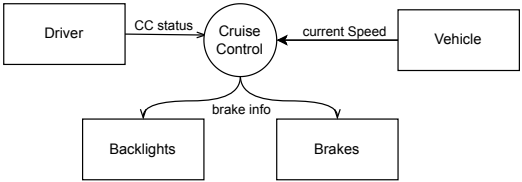


Abbildung: HoliSec Referenzarchitektur des internen Netzwerks [RO18b].



Beispiel eines Fahrzeuges

1. Systemzerlegung

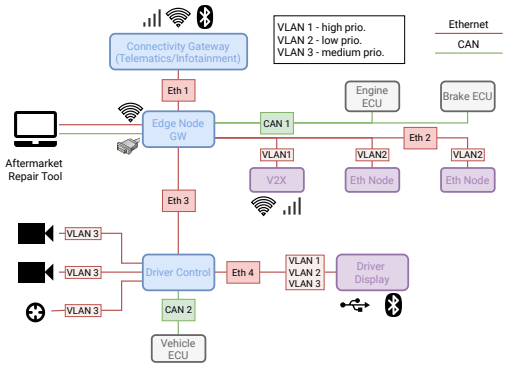
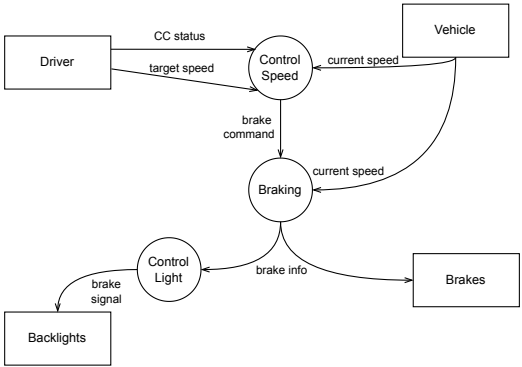
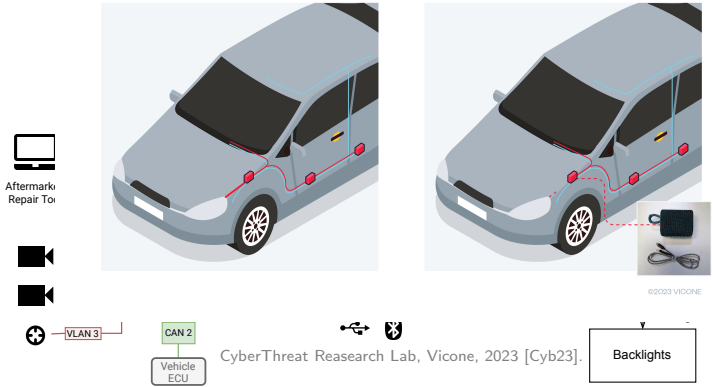


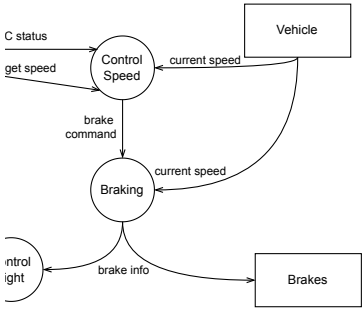
Abbildung: HoliSec Referenzarchitektur des internen Netzwerks [RO18b].



Beispiel eines Fahrzeuges

1. Syster





CyberThreat Reasearch Lab, Vicone, 2023 [Cyb23].

Abbildung: HoliSec Referenzarchitektur des internen Netzwerks [RO18b].

Forschung

Physische Schnittstellen brauchen besondere Beachtung!

- Neue Methode zur Identifikation von Assets [Ros+24]
- Fokus auf Modellierung von physischen und virtuallen Schnittstellen
- "Interface-Trees" zur Visualisierung von Abhängigkeiten

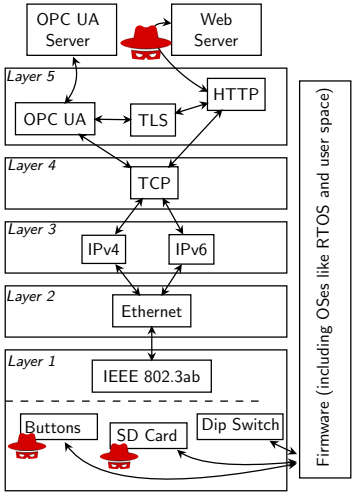


Abbildung: Vereinfachter Aslf Interface Tree.

Threat Analyse

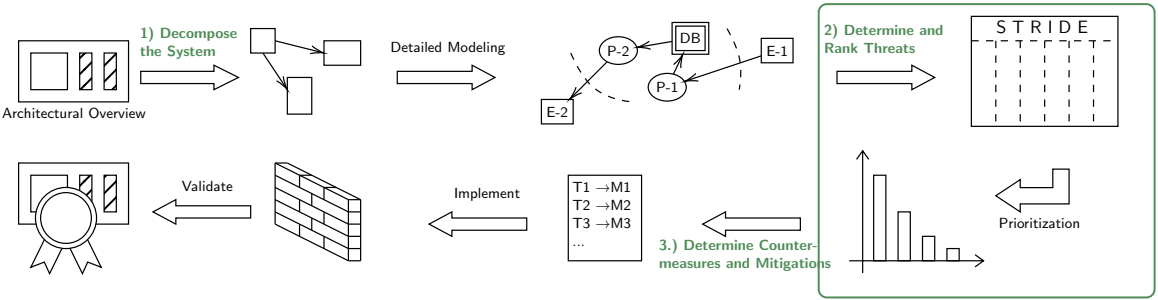
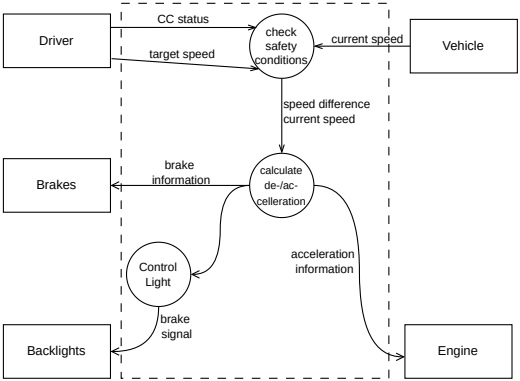


Abbildung: Threat Modeling Workflow [Ros+24].

Beispiel eines Fahrzeuges

2. Bedrohungen Identifizieren



<driver, check safety conditions, CC status>:

- **Spoofing:** *Prüfen des Sicherheitszustands* glaubt, Daten vom *Fahrer* erhalten zu haben.
- ...
- **Denial of Service:** *Prüfen des Sicherheitszustands* stürtzt aufgrund der Interaktion mit dem *Fahrer* ab
- ...

< driver, check safety conditions, target speed >
< vehicle, check safety conditions, current speed >
...

Beispiel eines Fahrzeuges

2. Bedrohungen Einstufen und Priorisieren

- Schwere
  - Safety Auswirkung
  - Finanzielle Auswirkung
  - Operationelle Ausirkung
  - ...
- Wahrscheinlichkeit
  - Sehr wahrscheinlich
  - Wahrscheinlich
  - Möglich
  - Nicht wahrscheinlich
  - Sehr unwahrscheinlich
- Security-Level
  - Hoch
  - Mittel-Hoch
  - Mittel
  - Mittel-Niedrig
  - Niedrig

Beispiel eines Fahrzeuges

2. Bedrohungen Einstufen und Priorisieren

Table B.1 – Example of a 3 x 5 risk matrix

		Severity		
		A	B	C
Likelihood	5	High	High	Med-high
	4	High	Med-high	Medium
	3	Med-high	Medium	Med-low
	2	Medium	Med-low	Low
	1	Med-low	Low	Low

Abbildung: IEC 62443-3-2 Annex B

- Schwere
  - Safety Auswirkung
  - Finanzielle Auswirkung
  - Operationelle Ausirkung
  - ...
- Wahrscheinlichkeit
  - Sehr wahrscheinlich
  - Wahrscheinlich
  - Möglich
  - Nicht wahrscheinlich
  - Sehr unwahrscheinlich
- Security-Level
  - Hoch
  - Mittel-Hoch
  - Mittel
  - Mittel-Niedrig
  - Niedrig

Forschung

Bedeutung und Struktur von Security-Levels? [RO18a]; [RO18b]

- Was bedeutet Security-Level medium-low in der Praxis?
- Wieviele Level ist notewendig?

→ Seit 2018 hat sich einiges getan

- Mehr Leitfäden
- Auch ein Cybersecurity Standard für die automotive Domäne

Forschung

Bedeutung und Struktur von Security-Levels? [RO18a]; [RO18b]

- Was bedeutet Security-Level medium-low in der Praxis?
- Wieviele Level ist notewendig?

→ Seit 2018 hat sich einiges getan

- Mehr Leitfäden
- Auch ein Cybersecurity Standard für die automotive Domäne

STRIDE Methoden in OT [Saß+24]

- Nur wenige Domänen mit Safety-Bezug
- Nur drei Adaptionen mit extra Fokus auf physische Bedrohungen
- Lebenszyklus wird kaum berücksichtigt

Threat Analyse

3. Bestimmen von Gegenmaßnahmen

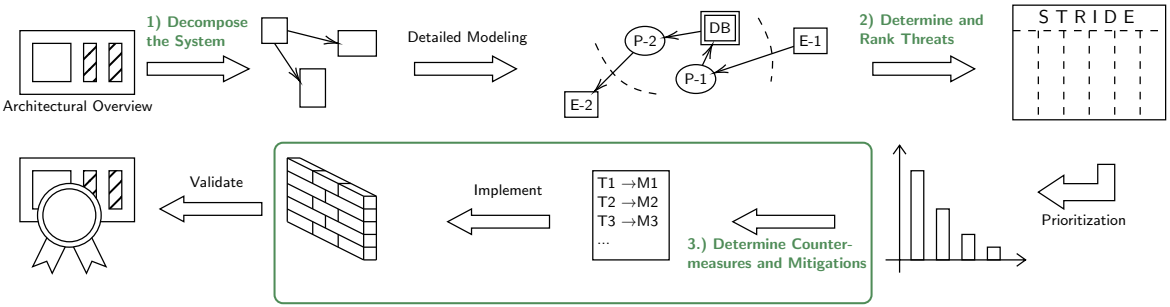


Abbildung: Threat Modeling Workflow [Ros+24].

Beispiel eines Fahrzeugs

3. Bestimmen von Gegenmaßnahmen

Auschnitt aus Industrie-Standard (IEC 62443-3-2)

- **SL 1:** Schutz vor unbeabsichtigtem oder zufälligem Missbrauch
- **SL 2:** Schutz vor vorsätzlichem Missbrauch mit einfachen Mitteln, geringen Ressourcen, allgemeinen Fähigkeiten und geringer Motivation.
- **SL 3:** Schutz vor vorsätzlichem Missbrauch mit anspruchsvollen Mitteln, moderaten Ressourcen, IACS-spezifischen Kenntnissen und mittlerer Motivation.
- **SL 4:** Schutz vor vorsätzlichem Missbrauch unter Einsatz anspruchsvoller Mittel, umfangreichen Ressourcen, IACS-spezifischen Kenntnissen und hoher Motivation.

Beispiel eines Fahrzeugs

3. Bestimmen von Gegenmaßnahmen

Auschnitt aus Industrie-Standard (IEC 62443-3-2)

- **SL 1:** Schutz vor unbeabsichtigtem oder zufälligem Missbrauch
- **SL 2:** Schutz vor vorsätzlichem Missbrauch mit einfachen Mitteln, geringen Ressourcen, allgemeinen Fähigkeiten und geringer Motivation.
- **SL 3:** Schutz vor vorsätzlichem Missbrauch mit anspruchsvollen Mitteln, moderaten Ressourcen, IACS-spezifischen Kenntnissen und mittlerer Motivation.
- **SL 4:** Schutz vor vorsätzlichem Missbrauch unter Einsatz anspruchsvoller Mittel, umfangreichen Ressourcen, IACS-spezifischen Kenntnissen und hoher Motivation.

Beispiel eines Fahrzeugs

3. Bestimmen von Gegenmaßnahmen

Auschnitt aus Industrie-Standard (IEC 62443-3-2)

- **SL 1:** Schutz vor unbeabsichtigtem oder zufälligem Missbrauch
- **SL 2:** Schutz vor vorsätzlichem Missbrauch mit einfachen Mitteln, geringen Ressourcen, allgemeinen Fähigkeiten und geringer Motivation.
- **SL 3:** Schutz vor vorsätzlichem Missbrauch mit anspruchsvollen Mitteln, moderaten Ressourcen, IACS-spezifischen Kenntnissen und mittlerer Motivation.
- **SL 4:** Schutz vor vorsätzlichem Missbrauch unter Einsatz anspruchsvoller Mittel, umfangreichen Ressourcen, IACS-spezifischen Kenntnissen und hoher Motivation.

Beispiel eines Fahrzeugs

3. Bestimmen von Gegenmaßnahmen

Auschnitt aus Industrie-Standard (IEC 62443-3-2)

- **SL 1:** Schutz vor unbeabsichtigtem oder zufälligem Missbrauch
- **SL 2:** Schutz vor vorsätzlichem Missbrauch mit einfachen Mitteln, geringen Ressourcen, allgemeinen Fähigkeiten und geringer Motivation.
- **SL 3:** Schutz vor vorsätzlichem Missbrauch mit anspruchsvollen Mitteln, moderaten Ressourcen, IACS-spezifischen Kenntnissen und mittlerer Motivation.
- **SL 4:** Schutz vor vorsätzlichem Missbrauch unter Einsatz anspruchsvoller Mittel, umfangreichen Ressourcen, IACS-spezifischen Kenntnissen und hoher Motivation.

Beispiel eines Fahrzeugs

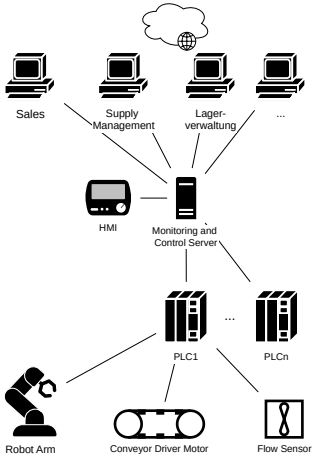
3. Bestimmen von Gegenmaßnahmen

Auschnitt aus Industrie-Standard (IEC 62443-3-2)

- **SL 1:** Schutz vor unbeabsichtigtem oder zufälligem Missbrauch
- **SL 2:** Schutz vor vorsätzlichem Missbrauch mit einfachen Mitteln, geringen Ressourcen, allgemeinen Fähigkeiten und geringer Motivation.
- **SL 3:** Schutz vor vorsätzlichem Missbrauch mit anspruchsvollen Mitteln, moderaten Ressourcen, IACS-spezifischen Kenntnissen und mittlerer Motivation.
- **SL 4:** Schutz vor vorsätzlichem Missbrauch unter Einsatz anspruchsvoller Mittel, umfangreichen Ressourcen, IACS-spezifischen Kenntnissen und hoher Motivation.

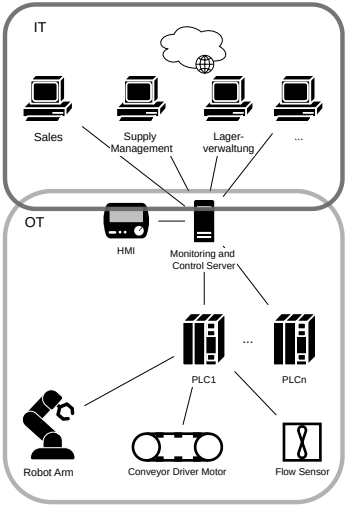
Forschung

IT-OT Konvergenz [SPR25]



Forschung

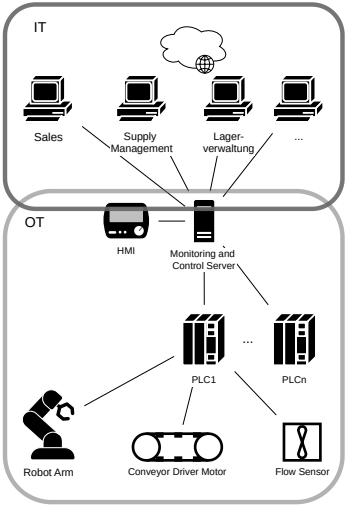
IT-OT Konvergenz [SPR25]



- Verschiedenste Sicherheitstandards und Empfehlungen
  - ISO, IEC, NIST
- Zertifizierung für die Wettbewerbsfähigkeit notwendig

Forschung

IT-OT Konvergenz [SPR25]



- Verschiedenste Sicherheitstandards und Empfehlungen
  - ISO, IEC, NIST
- Zertifizierung für die Wettbewerbsfähigkeit notwendig

PURITY Framework

- Gruppieren von Sicherheitsanforderungen
- Ausarbeiten von Maßnahmen
- Beispiele für Umsetzung in OT Netzen

Cyber-Resilienz

Benötigte Eigenschaften

- Anpassungsfähig
- Selbst-adaptiv
- Flexibel
- Widerstandsfähig
- Robust

Cyber-Resilienz

Benötigte Eigenschaften

- Anpassungsfähig
- Selbst-adaptiv
- Flexibel
- Widerstandsfähig
- Robust

Welche Strategien werden benötigt? [Ros+20]

- Erkennung
- Migration
- Wiederherstellung
- Ausdauer

→ Weitere Unterteilung in Patterns/Muster

→ Identifikation

REMIND Resilienz-Techniken

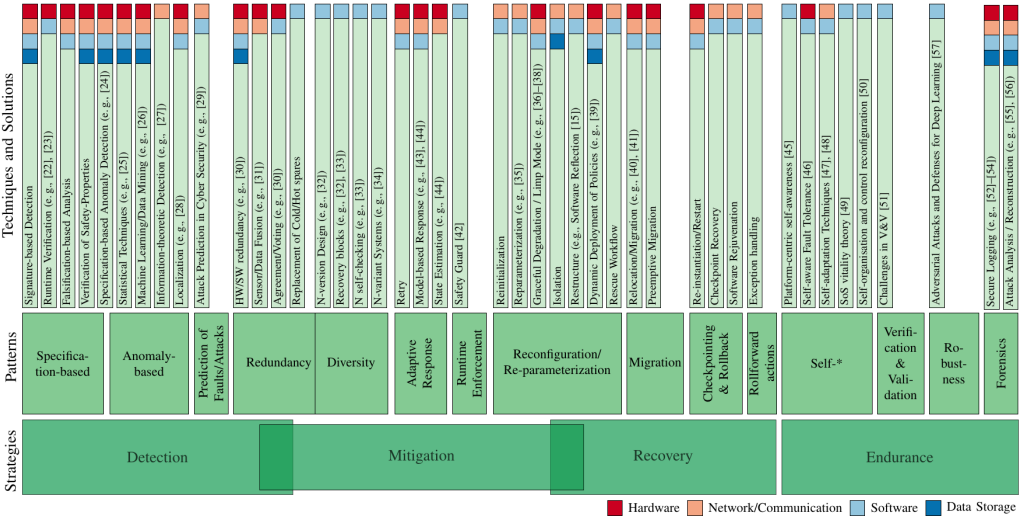


Abbildung: REMIND Resilienz-Techniken und Mechanismen [Ros+20].

Wie entscheiden Praktiker über den Mechanismus?

READY Framework [Ros+25]

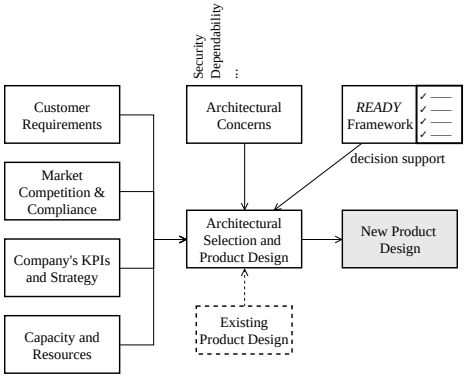


Abbildung: Verwendung von READY.

Wie entscheiden Praktiker über den Mechanismus?

READY Framework [Ros+25]

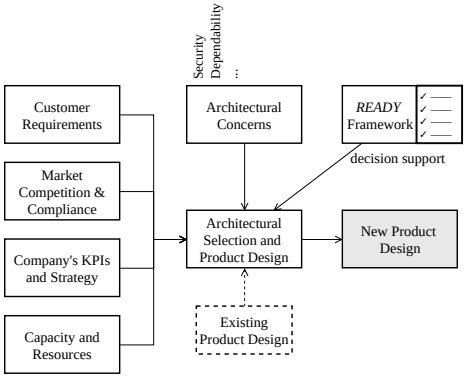


Abbildung: Verwendung von READY.

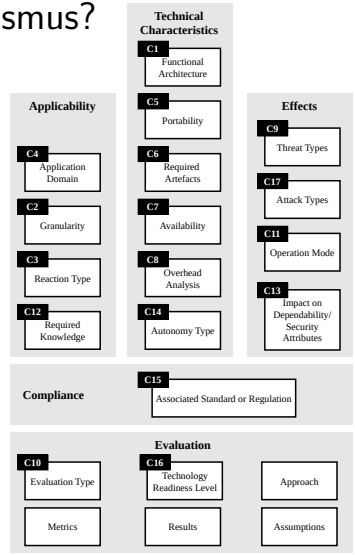


Abbildung: READY Framework.

Wie geht es weiter?

- Weitere Arbeit an Detection Mechanismen
- Automatisierte Entscheidung über Anwenden von Security-Mechanismen nicht trivial
- Safety, Echtzeitanforderungen, verteilte Systeme

Wie geht es weiter?

Detection → Mitigation → Recovery → Endurance

- Weitere Arbeit an Detection Mechanismen
- Automatisierte Entscheidung über Anwenden von Security-Mechanismen nicht trivial
- Safety, Echtzeitanforderungen, verteilte Systeme
- Reinforcment Learning zur Entscheidungsfindung?
- Unklar:
  - Aktionsraum
  - Belohnungsfunktion
  - Zustandsraum

Wie geht es weiter?

- Cyber-Resilienz “testen”?
- Validierung von Zielen nicht einfachen

Wie geht es weiter?

- Cyber-Resilienz “testen”?
- Validierung von Zielen nicht einfachen

  ➞ Security Chaos Engineering

Wie geht es weiter?

- Cyber-Resilienz “testen”?
- Validierung von Zielen nicht einfachen

  ➞ Security Chaos Engineering

- Kontinuierliche Evaluierung des Systems
- Simulation von Angriffen in Produktionsumgebung
- Automatische Überprüfung der Effektivität

  ➞ Restriktionen durch OT Eigenschaften

Securing the Future
Cybersicherheit in vernetzten Fahrzeugen und Industriesystemen

Thomas Rosenstatter

Department Information Technologies and Digitalisation
Fachhochschule Salzburg

24. November 2025

FH Salzburg

Bibliography I

[Cyb23] CyberThreat Research Lab, VicOne. *How to Get Away With Car Theft: Unveiling the Dark Side of the CAN Bus*. Blog article, updated May 8, 2023. VicOne. 2023-05. URL: https://vicone.com/blog/how-to-get-away-with-car-theft-unveiling-the-dark-side-of-the-can-bus.

[Kas25] Kaspersky ICS CERT. *A brief overview of the main incidents in industrial cybersecurity. Q2 2025*. Technical Report. Accessed: 2025-11-21. Kaspersky ICS CERT, 2025-10. URL: https://ics-cert.kaspersky.com/publications/reports/2025/10/09/a-brief-overview-of-the-main-incidents-in-industrial-cybersecurity-q2-2025/.

[RO18a] Thomas Rosenstatter und Tomas Olovsson. „Open Problems when Mapping Automotive Security Levels to System Requirements“. In: *Proceedings of the 4th International Conference on Vehicle Technology and Intelligent Transport Systems - VEHITS*. INSTICC. SciTePress, 2018, S. 251–260.

[RO18b] Thomas Rosenstatter und Tomas Olovsson. „Towards a Standardized Mapping from Automotive Security Levels to Security Mechanisms“. In: *2018 21st International Conference on Intelligent Transportation Systems (ITSC)*. 2018, S. 1501–1507.

[Ros+20] Thomas Rosenstatter, Kim Strandberg, Rodi Jolak, Riccardo Scandariato und Tomas Olovsson. „REMIND: A Framework for the Resilient Design of Automotive Systems“. In: *2020 IEEE Secure Development (SecDev)*. IEEE, 2020-09, S. 81–95.

Bibliography II

[Ros+24] Thomas Rosenstatter, Christian Schäfer, Olaf Saßnick und Stefan Huber. „AsIf: Asset Interface Analysis of Industrial Automation Devices“. In: *8th Cyber Security in Networking Conference (CSNet 2024)*. Paris, France: IEEE, 2024-12, S. 165–172.

[Ros+25] Thomas Rosenstatter, Efi Papatheocharous, Rodi Jolak, Behrooz Sangchoolie und Pierre Kleberger. „READY: Cybersecurity Resilience and Self-Adaptive Strategies Derieved from a Comprehensive Literature Review“. In: submitted. 2025.

[Rot22] Emma Roth. *Sirius XM Flaw Could've Let Hackers Remotely Unlock and Start Cars*. Accessed: 2025-11-21. 2022-12. URL: https://www.theverge.com/2022/12/3/23491259/sirius-xm-hack-remotely-unlock-start-cars.

[Saß+24] Olaf Saßnick, Thomas Rosenstatter, Christian Schäfer und Stefan Huber. „STRIDE-based Methodologies for Threat Modeling of Industrial Control Systems: A Review“. In: *2024 IEEE 7th International Conference on Industrial Cyber-Physical Systems (ICPS)*. St. Louis, USA: IEEE, 2024-05, S. 1–8.

[SPR25] Franz-Karl Schachinger, Ulrich Pache und Thomas Rosenstatter. „PURITY – An Industry-Standard-Based Security Framework for IT-OT Convergence“. In: 2025.

Bibliography III

[The16] The Hacker News. *Hackers Take Remote Control of Tesla's Brakes and Door Locks from 12 Miles Away*. Accessed: 2025-11-21. 2016-09. URL: https://thehackernews.com/2016/09/hack-tesla-autopilot.html.