EDOH
Consulting: Safety & IT-Security
Aviation Theory: ATPL / CPL / IR

Informationssicherheit (IT-Sicherheit)

Autorecht 2015 – Autonomes Fahren

Gliederung

EDOH
Consulting: Safety & IT-Security
Aviation Theory: ATPL / CPL / IR

- Einführung in die Informationssicherheit in Systemen der funktionalen Sicherheit
  - Grundlegendes und Ziele, Erweiterungen der IT-Sicherheit
- Anwendungen des automatisierten Fahrens
  - Assistentensysteme, Teil- u. Vollautomatisierung
- Vorstellung eines typischen Szenarios für automatisiertes (autonomes) Fahren
  - Beispiel „Staupilot“
- Prozesse und Daten - Gefahren und Schutzbedarf
  - Am Beispiel Staupilot
- Ausblick und Zusammenfassung

Einführung Informationssicherheit

EDOH
Consulting: Safety & IT-Security
Aviation Theory: ATPL / CPL / IR

- Informationssicherheit (Schutz von Informationen) ist eine alte Disziplin und wird seit langer Zeit angewendet.
  - Codebücher, Caesar …
- Seit Beginn des 20. Jahrhunderts wird sie technisch angewendet (ab ca. 1927)
  - Enigma (Rotor-Verschlüsselungsmaschine)
- Das ursprüngliche Ziel der Informationssicherheit war die Vertraulichkeit der Daten

  ➧ Vertraulichkeit durch Verschlüsselung

Einführung Informationssicherheit

EDOH
Consulting: Safety & IT-Security
Aviation Theory: ATPL / CPL / IR

- Ende der 80er-Jahre erfährt die Informationssicherheit einen grundlegenden Wandel (Computertechnik)
  - Orange Book (TCSEC, USA 1983), Green Book (ITSK, Deutschland 1989)
  - ITSEC (Information Technology Security Evaluation Criteria, 1990)
  - Common Criteria (IEC 15408, 1996)
- Die grundlegenden Sicherheitsziele sind (für Daten und Anwendungen)
  - Integrität (Unverfälschtheit)
  - Vertraulichkeit
  - Verfügbarkeit

Einführung Informationssicherheit

EDOH
Consulting: Safety & IT-Security
Aviation Theory: ATPL / CPL / IR

> Mit zunehmender Durchdringung des täglichen Lebens mit Informationstechnik wurden die Sicherheitsziele im Jahr 1994* erweitert (Beispiel elektronische Signaturen → Signaturgesetz)

- Integrität (Integrity)
- Vertraulichkeit (Confidentiality)
- Verfügbarkeit (Availability)
- **Rechtsverbindlichkeit (Liability)**
- **Rechtsverträglichkeit (Justice Compatibility)**

* Eingeführt von Harald Hauff in der Veröffentlichung „Chipkarten im Gesundheitswesen“, Band 5 der Schriftenreihe zur IT-Sicherheit des Bundesamtes für Sicherheit in der Informationstechnik (ISSN 0947-093X, 1994) → Exkurs: Grenzen der Anwendung digitaler Signaturen

Anwendungen

EDOH
Consulting: Safety & IT-Security
Aviation Theory: ATPL / CPL / IR

- Wie kommt die Automobiltechnik zur Informationssicherheit?
  - Gesetze und Vorschriften verlangen funktionale Sicherheit mit einem akzeptablen Restrisiko für die Zulassung
  - Bisher waren die Steuer- und Regelsysteme in den Fahrzeugen eingebettete Systeme ohne Vernetzung und der Fahrer wurde nicht aus der Verantwortung entlassen (Fahrer muss das technische System jederzeit kontrollieren und die Kontrolle übernehmen können → Wiener Abkommen)
  - Zunehmende Automatisierung zur Entlastung des Fahrers
    - Fahrer wird aus der „Regelschleife“ entlassen
    - Der Fahrer kann nicht mehr schnell genug die Kontrolle übernehmen

➧ Funktionale Sicherheit ist zwingend erforderlich

Anwendungen

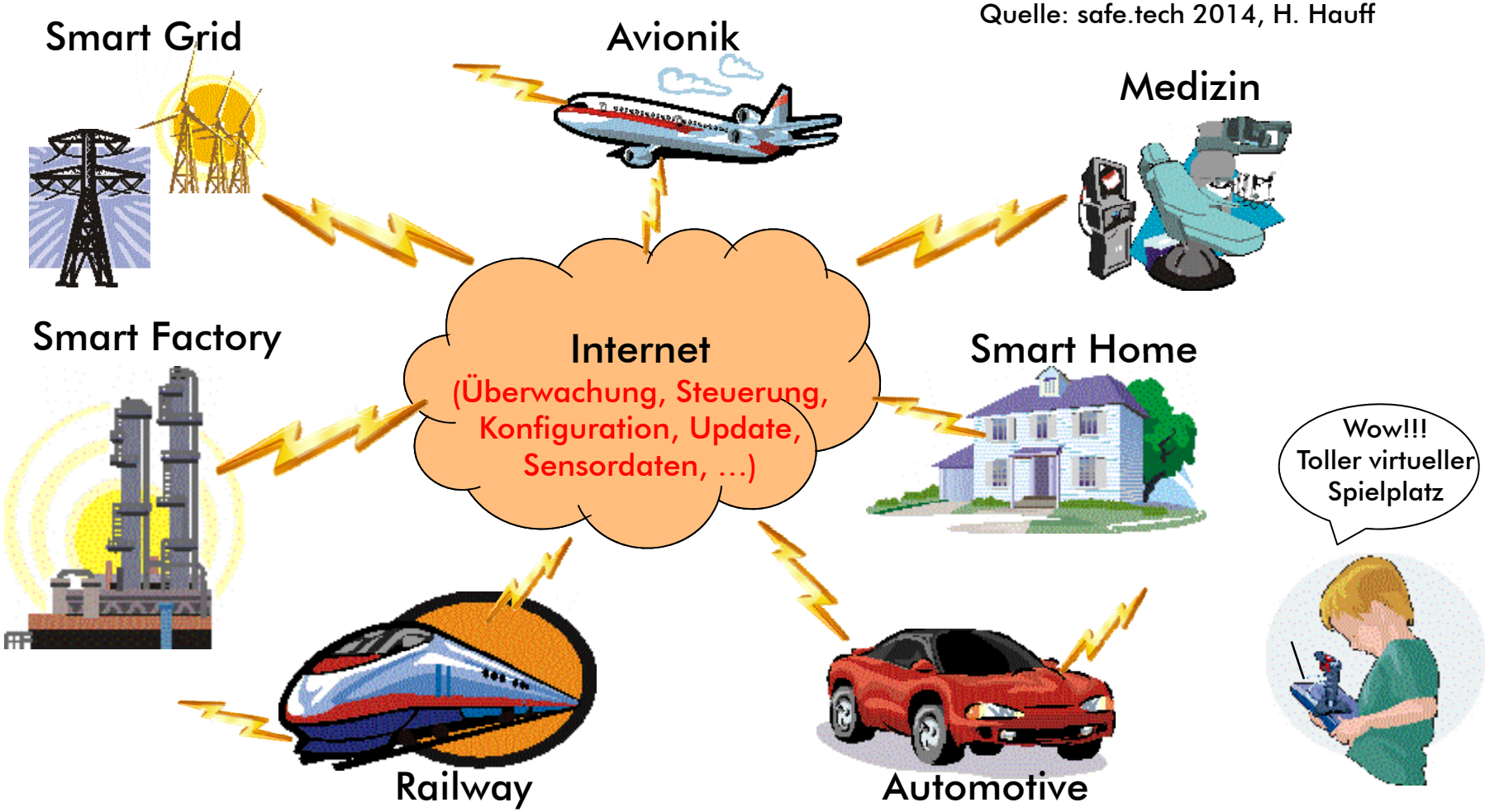
EDOH
Consulting: Safety & IT-Security
Aviation Theory: ATPL / CPL / IR

> Neu in der Fahrzeugelektronik mit Teil- und Vollautomatisierung

- Vernetzung der Steuer- und Regelsysteme im Fahrzeug zur Ermöglichung neuer Funktionen (ca. 70 pro Fahrzeug)
- Hohe Komplexität der Aufgaben u. Funktionen
- Abhängigkeit der Steuer- und Regelsysteme untereinander (Lenkung, Bremse, Motor)
- Hohe Zuverlässigkeit (und Robustheit)
- Verschiebung der Funktionalität auf software-gestützte Systeme (mehr Flexibilität, auch später noch erweiterbar mit zusätzlichen Funktionen)

Anwendungen

Quelle: safe.tech 2014, H. Hauff



Anwendungen

EDOH
Consulting: Safety & IT-Security
Aviation Theory: ATPL / CPL / IR

- Automatisiertes Fahren oder autonomes Fahren?
  - Mit Fahrer oder ohne?
- Anwendungen des automatisierten Fahren
  - Assistenzsysteme (ABS, ESP, EPS, ACC …)
    - Anti-blockier System (Bremse) – anti-lock braking system
    - Elektronisches Stabilisierungs-Programm – electronic stabilization program (Bremse)
    - Servolenkung – electric power steering
    - Tempomat (Antrieb)
    - Einparkhilfe (Lenkung, Bremse u. Antrieb)
    - Spurhalteassistent
    - Rangierassistent für Anhänger (Lenkung)
    - Adaptive Cruise Control (Antrieb, Bremse)

Anwendungen

EDOH
Consulting: Safety & IT-Security
Aviation Theory: ATPL / CPL / IR

- Anwendungen des automatisierten Fahren
  - Teilautomatisierung / Vollautomatisierung
    - Staupilot
    - Parkhauspilot
    - Einparkpilot
    - …
- Ob Assistenzsystem oder Teil-/Vollautomatisierung, alle Systeme müssen die funktionale Sicherheit erfüllen
  - Es gibt zahlreiche Normen zur funktionalen Sicherheit, die Basisnorm ist die IEC 61508 und die automotive spezifische Norm die ISO 26262
  - Beide Normen behandeln jedoch keine Informationssicherheit mit Ausnahme der Sicherheitsintegrität → SIL, ASIL

Anwendungen

EDOH
Consulting: Safety & IT-Security
Aviation Theory: ATPL / CPL / IR

> Postulat:

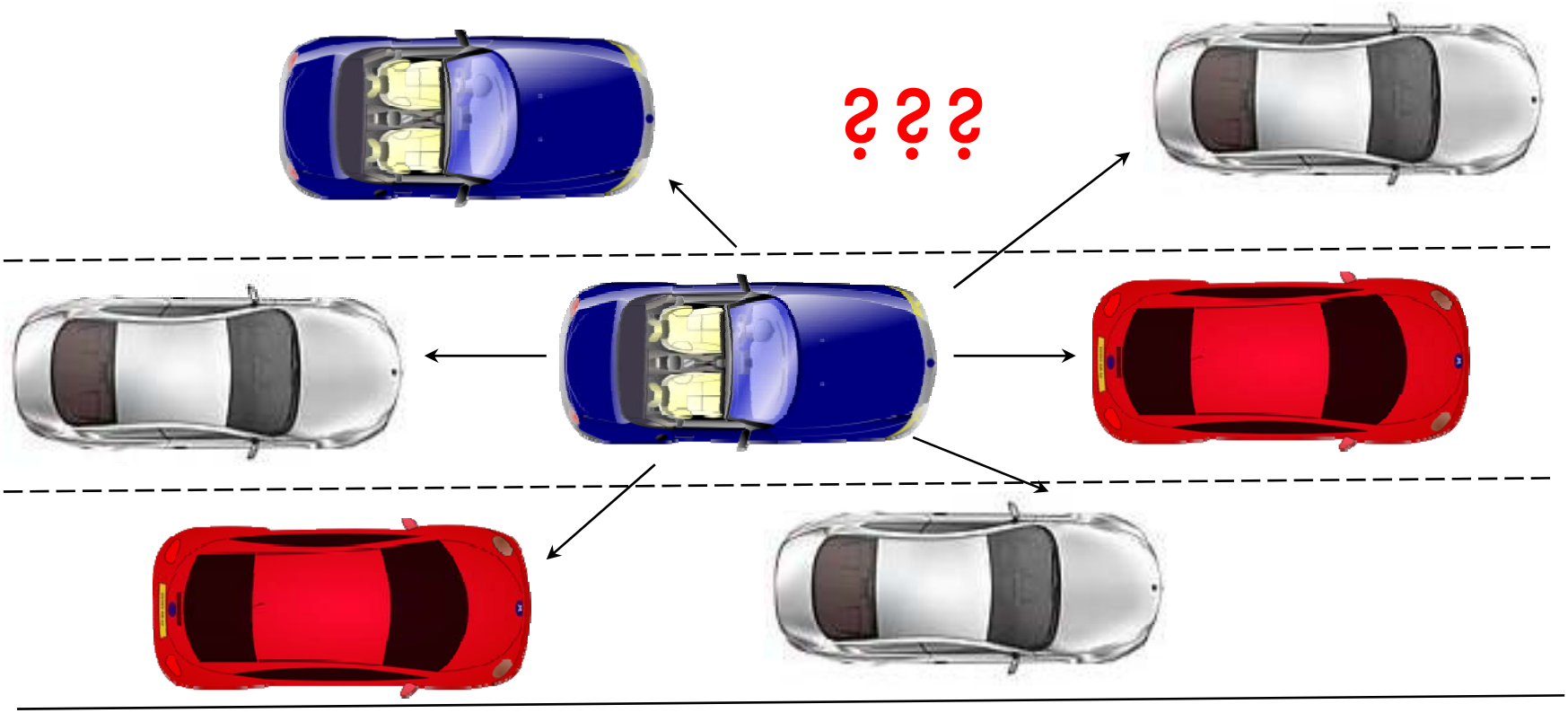
- Zur Aufrechterhaltung und Gewährleistung der funktionalen Sicherheit vernetzter, software-gestützter Systeme (Sicherheitsintegrität) ist die Informationssicherheit eine Grundvoraussetzung

> Die Sicherheitsintegrität für die Daten und die Anwendungen, für Hardware und Software kann nur gewährleistet werden, wenn Daten und Anwendungen, Hardware und Software nicht manipuliert werden können und jede Manipulation entdeckt wird und das System in den sicheren Zustand wechselt
(Fahrzeug darf durch eigene Mittel nicht mehr bewegt werden können).

Typisches Szenario - Staupilot

EDOH
Consulting: Safety & IT-Security
Aviation Theory: ATPL / CPL / IR

Autobahn mit drei Fahrstreifen pro Richtung



Quelle für Autos: http://all-free-download.com/free-vector

Prozesse u. Daten - Staupilot

EDOH
Consulting: Safety & IT-Security
Aviation Theory: ATPL / CPL / IR

- Prozesse und Daten
  - Abstandsbestimmung zum vorausfahrenden Fahrzeug in Abhängigkeit von der Geschwindigkeit
  - Bestimmung des Fahrstreifens (rechts, mitten, links)
  - Mit oder ohne Ausweichmanöver (Objektdetektion u. -Unterscheidung auf Fahrstreifen in Fahrtrichtung)
  - Detektion der umgebenden Fahrzeuge (hinten, links, rechts)
  - Erkennung des Verhaltens der umgebenden Fahrzeuge
    - Spurwechsel, Bremsmanöver, Notbremsung, Beschleunigung …
  - Situationserfassung und Entscheidung
  - …

Sicherer Zustand?

Sensoren - Staupilot

EDOH
Consulting: Safety & IT-Security
Aviation Theory: ATPL / CPL / IR

- Mit oder ohne Car-2-Car Kommunikation?
  - Car-2-Car Kommunikation
    - Wer ist vorausfahrendes Fahrzeug?
    - Wer ist seitlich oder hinter dem Fahrzeug?
    - Ad-hoc Kommunikation ohne Vorkenntnisse
    - Internationaler Standard für alle OEM verbindlich
    - Fälschungs- und Missbrauchssicherheit für die Kommunikation
      - Ansatz ähnlich Bahnnorm, CENELEC EN 50159

Problem stellt der Mischverkehr dar, der Verkehr der autonom/automatisiert fahren kann und welcher der es nicht kann (also auch keine Daten durch Car-2-Car Kommunikation)

Sensoren - Staupilot

EDOH
Consulting: Safety & IT-Security
Aviation Theory: ATPL / CPL / IR

- Autonom? → Sensoren für weitreichende Autonomie zur Situationserfassung, Objekterkennung und Entscheidung
  - Ultraschall → Entfernung eines Objektes
  - Videokamera → Entfernung, Objekterkennung
  - Radar (Doppler) → Geschwindigkeit (longitudinal) zu einem Objekt
  - Radar (FMCW) → Entfernung (Größe) eines Objektes
  - LIDAR (oder Laser-Scanner) → Entfernung, Objektkonturen
  - Photonic Mixing Device (PMD) → Entfernung, Objektgestalt (3D)
    - **Zuverlässigkeit, Täuschungsmöglichkeiten, Fälschungsmöglichkeiten, Verbindlichkeit der Informationen?**

Datenaggregation u. Datenfusion - Staupilot

EDOH
Consulting: Safety & IT-Security
Aviation Theory: ATPL / CPL / IR

- Situationserfassung, Situationserkennung und Entscheidung/Reaktion in Echtzeit?
  - Mindestanforderungen an die Daten
    - Frequenz, Verfügbarkeit, Integrität, Qualität … ???
    - Minimaler Satz an Daten für die Nutzung des Staupiloten?
    - Datenmenge die verarbeitet werden muss???
    - Schutz der Daten bei Car-2-Car Kommunikation oder Car-2-Infrastuktur Kommunikation???
    - Ad-hoc Netze ohne Vorkenntnis über den Kommunikationspartner
    - Kombination mit Navigationssystemen
      - Aktualität und Korrektheit der Navigationsdaten???
    - Gültigkeitszeitraum für die Daten
    - Beweissicherung (Logging)

Gefahren und Schwachstellen - Staupilot

EDOH
Consulting: Safety & IT-Security
Aviation Theory: ATPL / CPL / IR

- Manipulation von Steuergeräten (Tuning)
  - Algorithmen für Staupilot verlieren die Gültigkeit und Korrektheit (Motorleistung, Bremsleistung, Lenkwinkel, Fahrdynamik)
- Störanfälligkeit der Sensoren
  - Verschmutzungen (besonders im Winter, Nebel, Starkregen)
  - Falsche Sensordaten durch zufällige Fehler
  - Vorgetäuschte Daten (Car-2-Car Kommunikation oder Car-2-Infrastruktur Kommunikation)
  - Interferenz von Sensorsignalen …
- Direkter Remote-Eingriff in die Fahrzeugfunktionen
  - Car-Hacking (Zugang über drahtlose Netzwerke und Infotainment-Systeme)

Gefahren und Schwachstellen - Staupilot

EDOH
Consulting: Safety & IT-Security
Aviation Theory: ATPL / CPL / IR

- Es besteht eine große „Angriffsfläche“, um die automatisierte Funktion zu stören oder versagen zu lassen
  - Direkte Eingriffe in das System (autorisiert oder nicht - Tuning)
  - Fehleranfälligkeit durch falsche/fehlerhafte Wartung
  - Indirekte Eingriffe durch Täuschung von Sensoren
  - Übernahme der Funktion aus der Ferne (Remote)
  - …

Gefahren und Schwachstellen - Staupilot

EDOH
Consulting: Safety & IT-Security
Aviation Theory: ATPL / CPL / IR

- Mischverkehr (mit/ohne Staupilot)
- Internationale Nutzbarkeit von automatisierten Funktionen
  - China???
  - Indien???
  - Rechts- / Linksverkehr ???

Eine Straßenkreuzung in Indien
https://youtu.be/nuvHtCai0BI
oder
https://youtu.be/pm8OEEd7u00

Ausblick und Zusammenfassung

EDOH
Consulting: Safety & IT-Security
Aviation Theory: ATPL / CPL / IR

- Es sind Ansätze vorhanden, die Informationssicherheit in der Fahrzeugelektronik und in Anwendungen ermöglichen
  - Lightweight Kryptographie auf Basis symmetrischer Verfahren mit Unterstützung in Hardware für
    - Verschlüsselung (gegen Fälschung und Datenanalyse → Vertraulichkeit u. ggf. Authentizität)
    - Elektronische Signaturen (gegen Fälschung u. Vortäuschung → Authentifizierung, Integrität …)
    - Für Updates der Software oder Konfiguration von Steuergeräten soll der Ursprung durch den OEM sichergestellt werden (ggf. auch mit Public Key Infrastrukturen) (gegen Fälschung u. Manipulation → Authentifizierung, Integrität, Rechtsverbindlichkeit)
    - Zeitliche Zuordnung der Daten und Nachrichten (Ausschluss veralteter Daten) (gegen Wiedereinspielung/Wiederholung → Integrität, Verbindlichkeit)
    - …

Ausblick und Zusammenfassung

EDOH
Consulting: Safety & IT-Security
Aviation Theory: ATPL / CPL / IR

- Das automatisierte Fahren kann aus heutiger Sicht nur gelingen, wenn das Fahrzeug bezüglich der Situationserfassung und Entscheidung vollkommen autonom ist.
  - Ein Mischverkehr von Fahrzeugen mit oder ohne automatisiertes Fahren spielt keine Rolle.
  - Keine Kommunikation mit anderen Fahrzeugen oder Infrastruktur (Probleme bezüglich Zeitfaktor für die Übertragung und Datenfusion sowie Vertrauensstellung der Kommunikationspartner und Zuverlässigkeit und Verbindlichkeit der Daten tritt erst gar nicht auf, die „Angriffsfläche“ reduziert sich auf das Fahrzeug selbst)

Ausblick und Zusammenfassung

EDOH
Consulting: Safety & IT-Security
Aviation Theory: ATPL / CPL / IR

- Aus technischer Sicht scheint das automatisierte Fahren in wenigen Jahren realistisch aber nicht in allen Ländern oder Regionen anwendbar
  - Sensoren entwickeln sich weiter und liefern immer bessere Daten für die Objekterkennung und Objektunterscheidung
  - Datenfusion hoher Datenmengen und Auswertung gelingt immer besser durch Parallelverarbeitung und hohe Performanz der Elektronik und Software
  - Trotzdem wird der Einsatz nur auf beherrschbare Szenarien beschränkt bleiben müssen (siehe Indien, China …, nur auf Autobahnen und nur unter bestimmten Wetterbedingungen bzw. Umweltbedingungen)

Ausblick und Zusammenfassung

EDOH
Consulting: Safety & IT-Security
Aviation Theory: ATPL / CPL / IR

- Automatisiertes Fahren wirft verschiedene Rechtsfragen auf und Rechtsnormen müssen geschaffen werden
  - Gefährdungshaftung wie bisher???
    - Wer ist der Gefährder/Verursacher im Schadensfall und haftbar zu machen? → Fahrer, Hersteller, Werkstatt …
  - In welchen Situationen dürfen die automatisierten Funktionen überhaupt nur benutzt werden und wie wird der Missbrauch bzw. falscher Gebrauch verhindert
    - Z.B. nur auf Autobahnen oder mehrstreifig ausgebauten Bundesstraßen mit getrennten Fahrbahnen bezüglich Fahrtrichtungen nutzbar
      - Automodus kann nur auf Autobahnen oder ähnlichen Straßen aktiviert werden (z.B. nicht in Städten oder auf Landstraße)
  - Ist eine neue/zusätzliche Infrastruktur zu schaffen (z.B. Parkhaus für Parkhauspilot)???

Ausblick und Zusammenfassung

EDOH
Consulting: Safety & IT-Security
Aviation Theory: ATPL / CPL / IR

- **Es besteht jedoch kein Zweifel daran, für automatisiertes oder autonomes Fahren ist Informationssicherheit zur Erfüllung der funktionalen Sicherheit und auch zur Erfüllung von Rechtsnormen unerlässlich**

> Vielen Dank für Ihre Aufmerksamkeit!

> Fragen? Diskussionen?

Kontakt

EDOH
Consulting: Safety & IT-Security
Aviation Theory: ATPL / CPL / IR

Ingenieurbüro EDOH
Dipl.-Ing. Harald Hauff
Hopfenstraße 4b
D-85254 Einsbach
Deutschland

Tel.: +49 (0) 8135 939173
Fax.: +49 (0) 8135 939198
E-Mail: harald.hauff@ib-edoh.de