

# IT-Sicherheit und Digitalisierung – Wie passt das zusammen?

Prof. Dr. Hannes P. Lubich  
Institut für Mobile und Verteilte Systeme  
Fachhochschule Nordwestschweiz

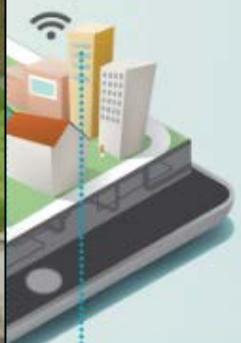
SUSTAINABILITY



**PREDICTIVE MAINTENANCE**  
Enables the analysis of data received from sensors installed in lifts to predict breakdowns.



**TRAFFIC MONITORING**  
Cameras with video analytics installed at highways to detect traffic jams, accidents and other traffic misconduct.



SECURITY



**SMART CCTV**  
Usage of cameras and video analytics to facilitate people-counting, illegal intrusion, objects left unattended and vehicle plate recognition.



**BEHAVIOUR ANALYTICS**  
Cameras that detect persons who may be drowning in a pool.

**CLIMATE CHANGE AND FLOOD MODELLING**  
Tools that allow users to model flooding and climate change, particularly in cities that are in a conceptual stage.

**WATER MANAGEMENT**  
Detect water quality by using camera analytics to examine marine life in water.

**SMART LIGHTING**  
Sensors and controllers in light fittings that allow light to dim if no presence is detected, saving energy and expenditure.



Auton  
Jahrh



**DERLY MONITORING**  
Installation of sensors comes to detect the ill-being of elderly persons and their movements.

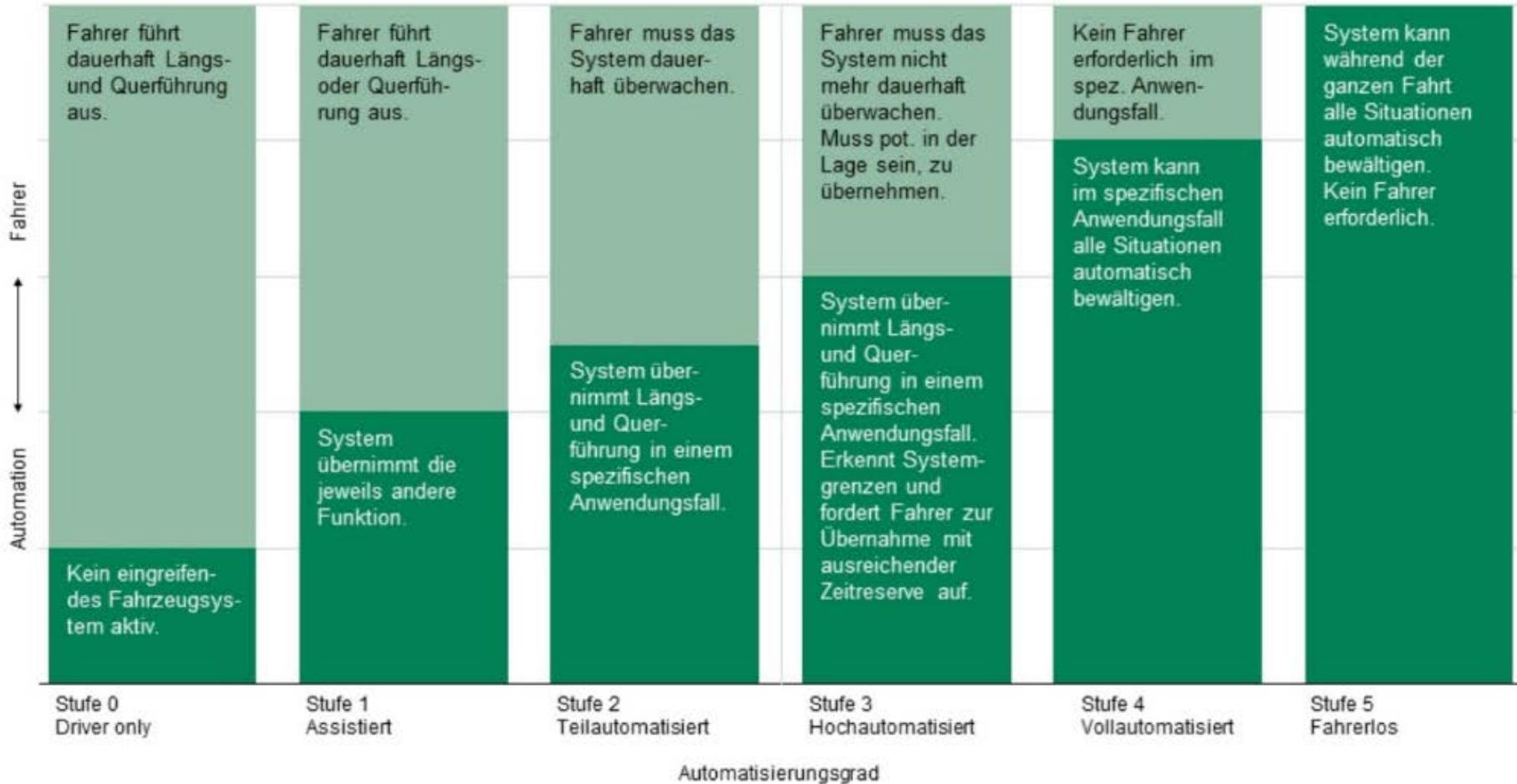
**SMART TOILET**  
Sensors that detect if the toilet is wet or has run out of toilet paper, enabling the deployment of cleaners based on need rather than scheduled cleaning.

**FIRE & SMOKE DETECTION**  
Cameras and video analytics that detect fire and smoke.

**FACIAL RECOGNITION**  
Cameras and laptops with stored data used to identify blacklisted individuals.



## Stufen des automatisierten Fahrens



# Ausgangslage

- Rechenleistung, Speicherleistung, schnelle, drahtlose Kommunikation, Miniaturisierung, «Internet of Things» Infrastrukturen
  - Selbstlernende / selbstadaptierende Echtzeit-Systeme
  - Wirtschaftliche, rechtliche, regulatorische und gesellschaftliches Interesse, Pilot-Umsetzungen usw.
- 
- Starke Abhängigkeit von bedingt zuverlässiger / sicherer ICT (Sensorik, Hardware, Software, Kommunikation, Interaktion mit externen Systemen und Instanzen)
  - Erste Presse-Meldungen über Angriffe und Schäden
  - Grosse Hoffnungen, aber auch grosse Unsicherheiten

# Informationssicherheit / Bedrohungen



# Virtuelle IT-Schäden werden physisch

## Schwachstelle Infotainmentsystem

### Gelungener Hackerangriff auf fahrendes Auto

Die Horrorvorstellung jedes Autofahrers: Ein Hacker kapert aus der Ferne das fahrende Auto, greift in die Lenkung ein, steht auf die Bremse oder gibt Vollgas! Kürzlich geschehen in Amerika.



n  
ändert

iffsbranche ein  
e Schiffe  
lehr...

pacemakers

f t b e Share

GETTY IMAGES

e a firmware update

as having cyber-security

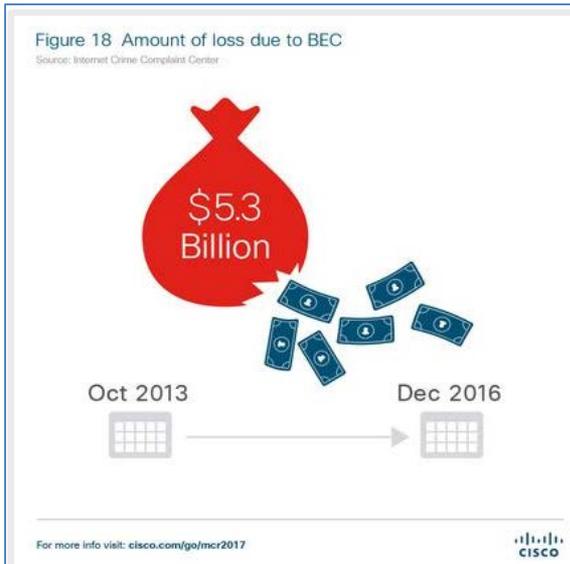
issues that could let them be hacked.

# Angreifer und Motivationen

- Extern:
  - Hacker / Cracker
  - Informationssammler
  - Kriminelle Personen/Organisationen
  - Aufklärungsdienste
  - Partner / Kunden
  - Konkurrenten
  - Fanatiker / Terroristen
  - Militär
- Intern:
  - Unzufriedene Mitarbeiter
  - Lieferanten / Wartung
  - System Spezialisten
  - Kriminelle
  - Unvorsichtige Mitarbeiter
- Reputation (“Community”, Freunde, Öffentlichkeit, ...)
- Langeweile (oft mit dem Angreiferalter verknüpft)
- Schaden / Rache (privater Streit, aktuelle / ehemalige Angestellte, ...)
- Wettbewerber (Offerten, Kunden, Konditionen, Intentionen patentiertes Material, ...)
- Direkter Vorteil (Software, Musik, ...)
- Indirekter Vorteil (Lizenzen, Information, Zugang, ...)
- Privater Auftrag (Kommerziell / Industriespionage)
- Staatsauftrag (Terrorismusbekämpfung, militärische Aufklärung, Standortstärkung, ...)

# Kosten / Nutzen

Goods and services	Percentage	Range of prices
Bank accounts	22%	\$10-\$1000
Credit cards	13%	\$0.40-\$20
Full identities	9%	\$1-\$15
eBay accounts	7%	\$1-\$8
Scams	7%	\$2.5/week - \$50/week for hosting. \$25 for design
Mailers	6%	\$1-\$10
Email addresses	5%	\$0.83/MB-\$10/MB
Email passwords	5%	\$4-\$30
Drop (request or offer)	5%	10%-50% of total drop amount
Proxies	5%	\$1.50-\$30



## Cyber-Kriminalität: Das unterschätzte Risiko

Nur **6%** der kleinen und mittelständischen Unternehmen betrachten Cyber-Kriminalität als mögliches Risiko.

**6%**

**31%** **31%** der befragten Unternehmer halten Datenverlust für bedeutendes Risiko, sind aber nicht dagegen versichert.

**94%** **94%** der Unternehmen haben KEINE Versicherung für Schäden durch Cyber-Kriminalität.

**64.000** **64.000** gemeldete Fälle von Cyber-Kriminalität 2012 in Deutschland.

**500 Mrd.** Euro ist der geschätzte jährliche Schaden durch Cyber-Kriminalität weltweit.

**500.000.000.000 €**

© Quelle: GfK-Befragung, HISCOX DNA Studie, FIS 2012, Center for Strategic and International Studies (CSIS)  
Grafik: www.gov.de | Gesamtverband der Deutschen Versicherungswirtschaft (GDV)

# Angriffsziele und Angriffswege

- Ziele:
  - Hersteller (inkl. Zulieferer-Kette)
  - Fahrzeug im Betrieb beim Kunden / Nutzer
  - Verbundene Infrastrukturen (von Smart Phone bis Smart Road)
  - Kontroll- und Steuersysteme der Betreiber, des Staats usw.
- Wege:
  - Hardware (Chips. Sub-Systeme)
  - Sensorik (wie erkenne ich ein Objekt der physischen Welt?)
  - Lernsystem («fake news» für Fahrzeuge?)
  - Kommunikation und Schnittstellen («man in the middle» etc.)
  - Software / Anwendungen (Routenplaner, Stauwarnung, etc.)
  - Datenaustausch (Auto-Auto, Auto-Strasse, Auto-Kontrollsystem)
  - Mensch («social engineering» usw.)

# Rechtliche Aspekte, Haftung etc.



*"Speeding, officer? You'll have to ask the self-driving car."*

# Moralische und ethische Aspekte

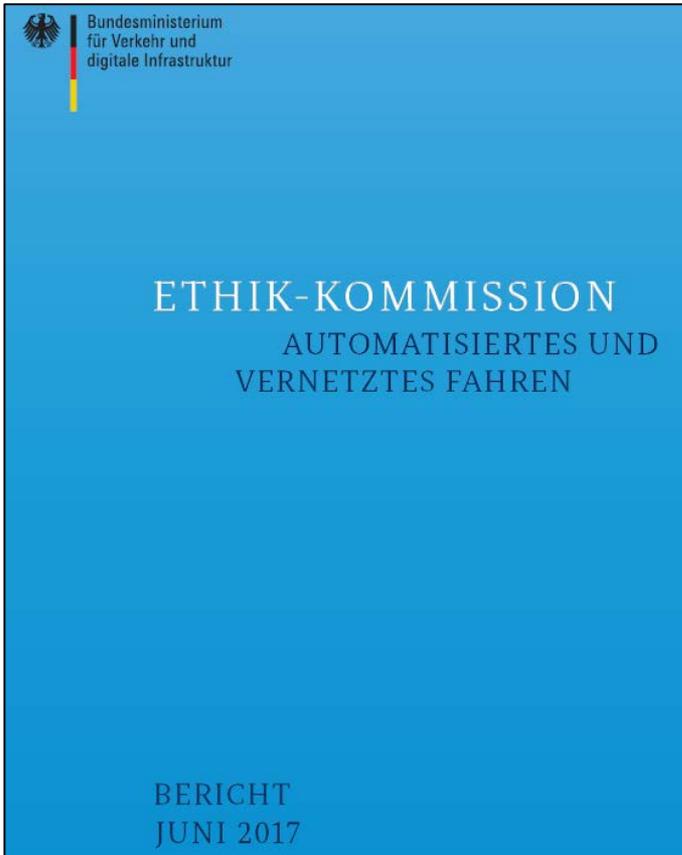


# Künstliche Intelligenzen als gesellschaftlich handelnde Entitäten?

- Alexa sagt in Mordprozess aus: <http://www.inside-it.ch/articles/46880>
- IoT: Selbstlernende / -handelnde Systeme - von autonomen Lebensmittelbestellungen durch Kühlschränke bis hin zu autonomen Fahrzeugen mit inhärenten ethischen Handlungskonflikten (wen überfahre ich?)

Offene Fragen: Gesellschaftliche Akzeptanz, Versicherbarkeit / Haftung, Zubilligung einer rechtlichen Person analog zu juristischen Personen? → kein IT-Problem

# Künstliche Entitäten und Ethik



9. Bei unausweichlichen Unfallsituationen ist jede Qualifizierung nach persönlichen Merkmalen (Alter, Geschlecht, körperliche oder geistige Konstitution) strikt untersagt. Eine Aufrechnung von Opfern ist untersagt. Eine allgemeine Programmierung auf eine Minderung der Zahl von Personenschäden kann vertretbar sein. Die an der Erzeugung von Mobilitätsrisiken Beteiligten dürfen Unbeteiligte nicht opfern.
10. Die dem Menschen vorbehaltene Verantwortung verschiebt sich bei automatisierten und vernetzten Fahrsystemen vom Autofahrer auf die Hersteller und Betreiber der technischen Systeme und die infrastrukturellen, politischen und rechtlichen Entscheidungsinstanzen. Gesetzliche Haftungsregelungen und ihre Konkretisierung in der gerichtlichen Entscheidungspraxis müssen diesem Übergang hinreichend Rechnung tragen.

Auszug aus den  
20 Grundsätzen

# Konsequenzen für die weitere Entwicklung des autonomen Verkehrs

- Gesamtsystem betrachten: smart car + smart road + ...)
- Virtuelle ICT-Schäden → Schäden in der realen Welt
- Technik, Wirtschaft, Politik, Recht & Gesellschaft involviert
- Die Entwicklung wird (und sollte) sich nicht aufhalten lassen, aber Reflektion und Aufmerksamkeit sind nötig
- Schäden erwarten und akzeptieren, vor allem im hybriden Mensch-Maschine-Betrieb (ÖV und Individualverkehr)



Fachhochschule Nordwestschweiz  
Hochschule für Technik  
Institut für Mobile und Verteilte Systeme

Prof. Dr. Hannes P. Lubich  
Dozent für ICT System Management  
Bahnhofstrasse 6, CH-5210 Windisch

T: +41 56 202 78 21 (direkt)  
hannes.lubich@fhnw.ch  
<http://www.fhnw.ch/personen/hannes.lubich>