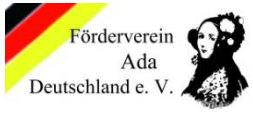
9. - 10. Juli 2018 | 1. Workshop | Karlsruhe

Konstruktion von SafeWare

Herausforderung für das Internet der Dinge

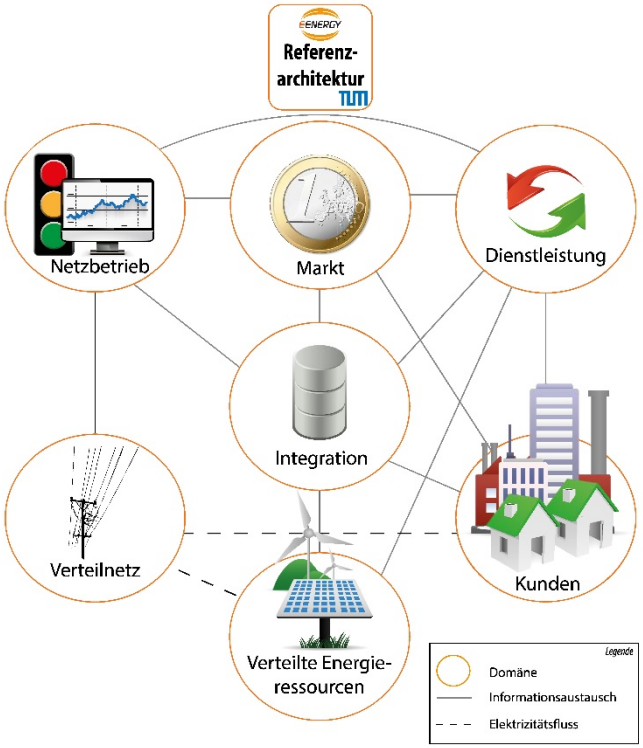


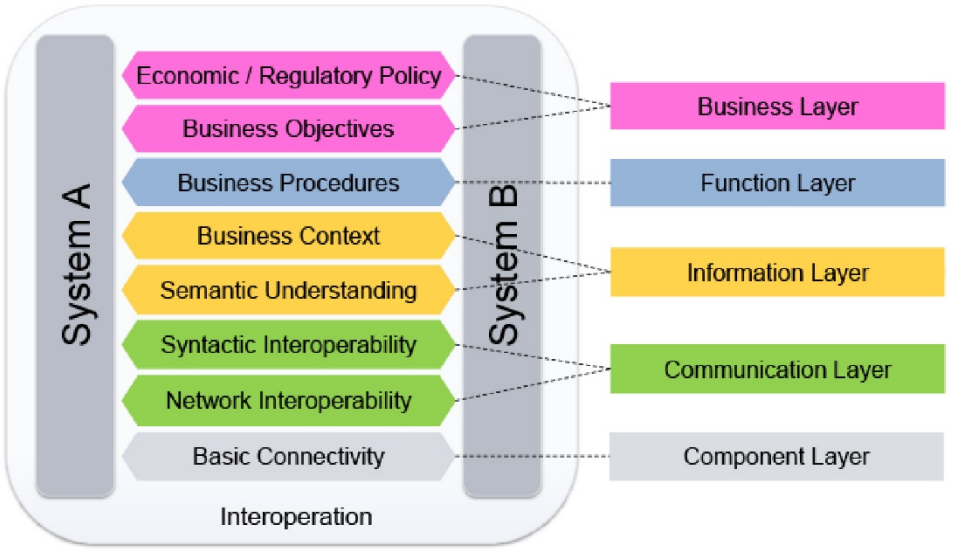
… Software Umfänge

Software-Anwendung	Codeumfang	Fehler Standard 0,5% (V-Modell)	Fehler Höchstqualität: 0,01% (Militär, Aerospace)
Durchschnittliche iPhone~App	40.000	200	4
Herzschrittmacher	80.000	400	8
Photoshop 1.0	128.000	640	13
Space Shuttle Flugsoftware	400.000	2.000	40
Grafikschnittstelle CryEngine 2	1.000.000	5.000	100
Hubble Weltraumteleskop	2.000.000	10.000	200
Windows 3.1	2.500.000	12.500	250
Kontrollsoftware einer US-Militärdrohne	3.500.000	17.500	350
Mars Curiosity Rover	5.000.000	25.000	500
Google Chrome	7.000.000	35.000	700
Photoshop CS 6	10.000.000	50.000	1.000
OpelAmpera	10.000.000	50.000	1.000
Android OS	12.000.000	60.000	1.200
Boeing 787 Dreamliner	14.000.000	70.000	1.400
Linux3.10	16.000.000	80.000	1.600
Firefox Browser	18.000.000	90.000	1.800
F-35 Kampfflugzeug	24.000.000	120.000	2.400
Windows7	40.000.000	200.000	4.000
Microsoft Office 2013	45.000.000	225.000	4.500
Teilchenbeschleuniger Large Hadron Collider	50.000.000	250.000	5.000
Windows Vista	50.000.000	250.000	5.000
Facebook	62.000.000	310.000	6.200
MacOSXI0.4	86.000.000	430.000	8.600
Steuersoftware für moderne Autos	100.000.000	500.000	10.000
Webseite healthcare.gov	500.000.000	2.500.000	50.000
Menschliches Genom	3.300.000.000	16.500.000	330.000

Anmerkung: Komplexität der Software-Strukturen ist nicht berücksichtigt.
Hohe cC verstärkt Fehlerquote massiv!

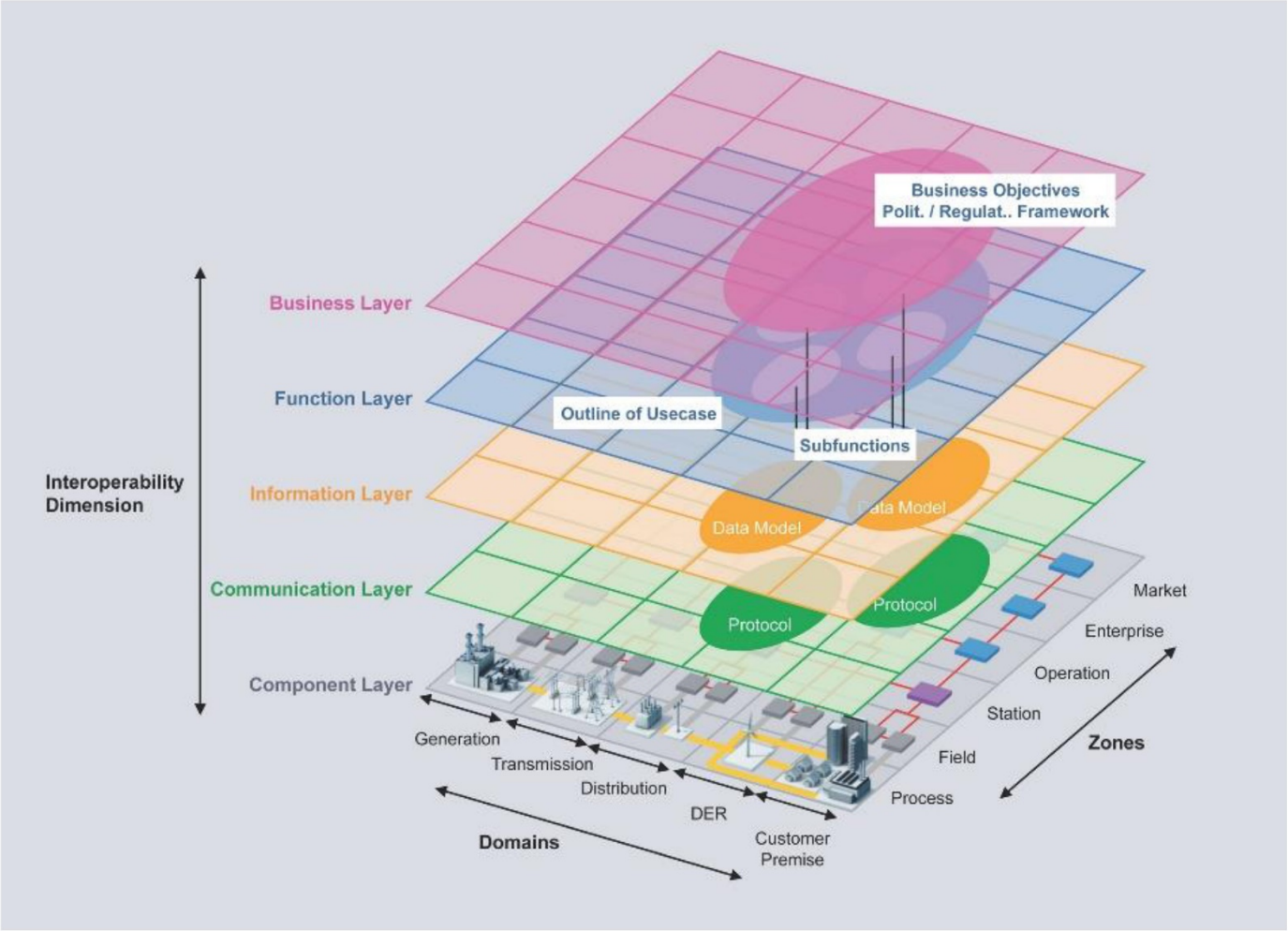
Smart Grid der Zukunft



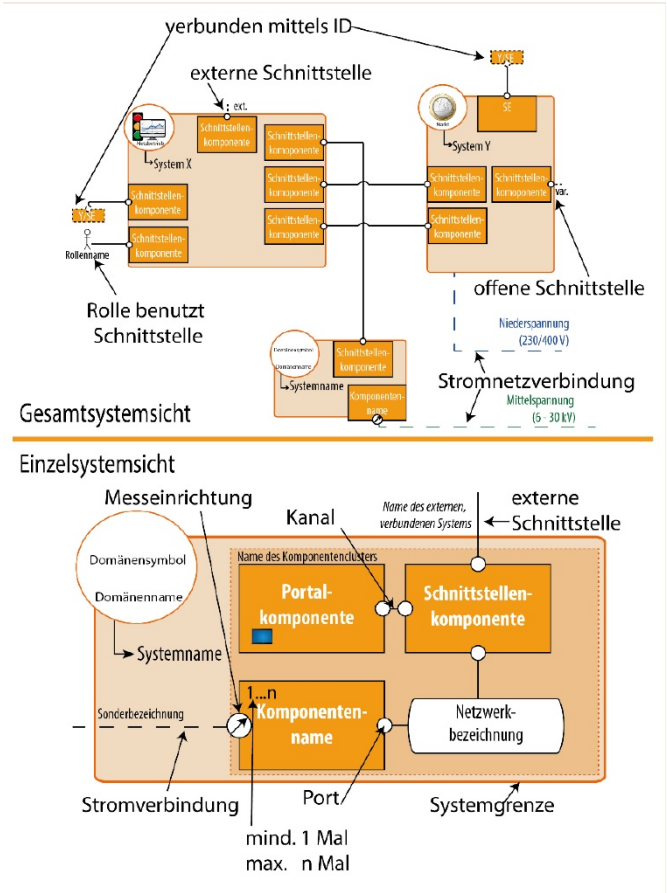


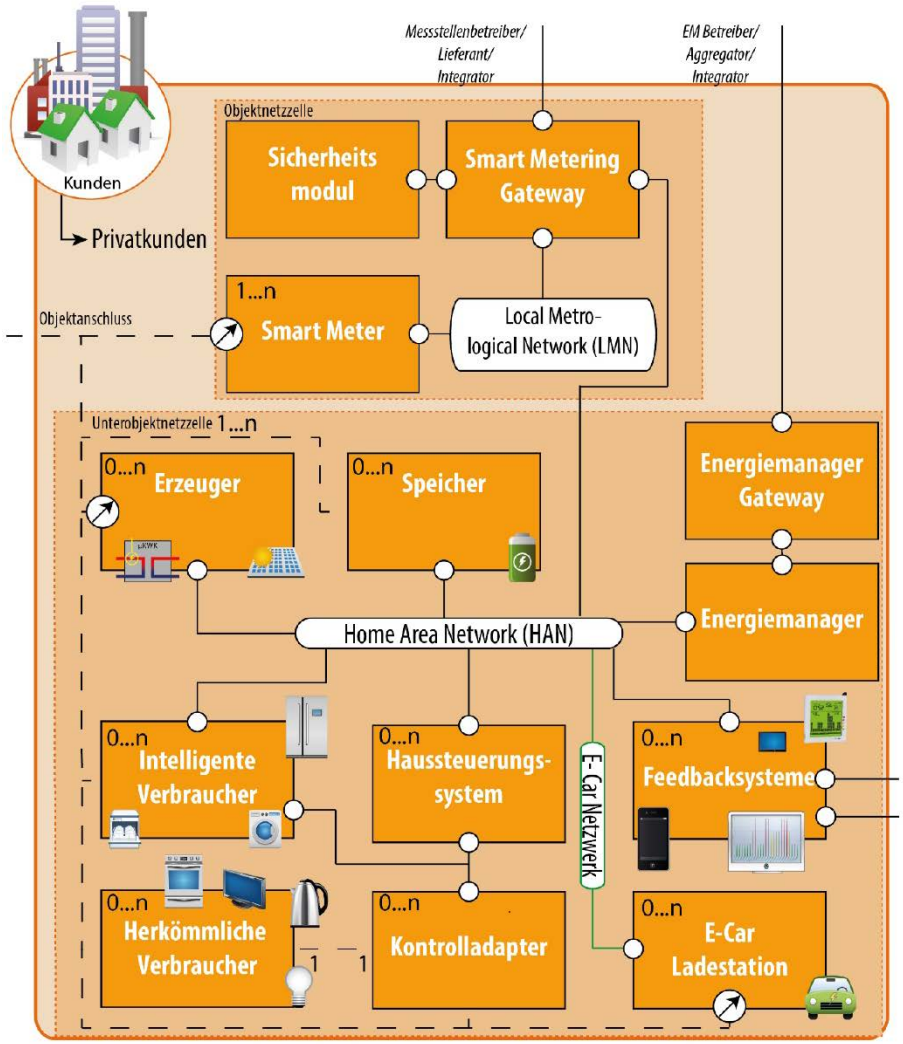
DIE E-ENERGY REFERENZARCHITEKTUR. EINE VISION FÜR EIN SMART ENERGY SYSTEM MADE IN GERMANY.
MAXIMILIAN IRLBECK, VASILEIOS KOUTSOUMPAS. TECHNISCHE UNIVERSITÄT MÜNCHEN.
E-ENERGY BEGLEITFORSCHUNG, BEREICH INFORMATIONS- UND KOMMUNIKATIONSTECHNOLOGIE. Stand: 15. Juni 2015

Smart Grid - Struktur



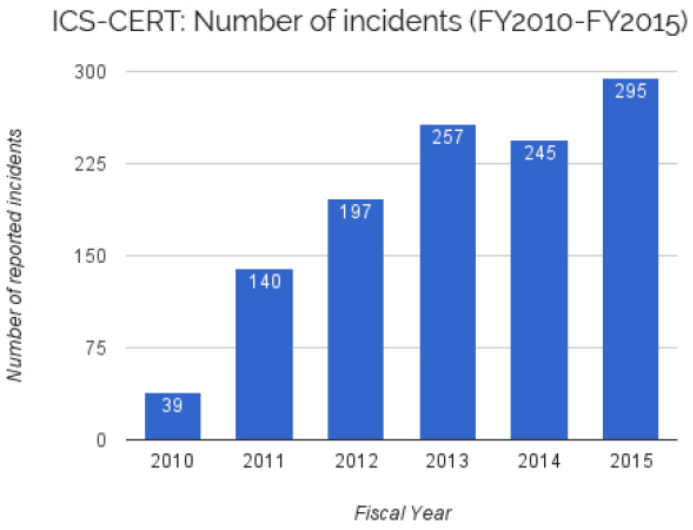
Smart Grid - Struktur

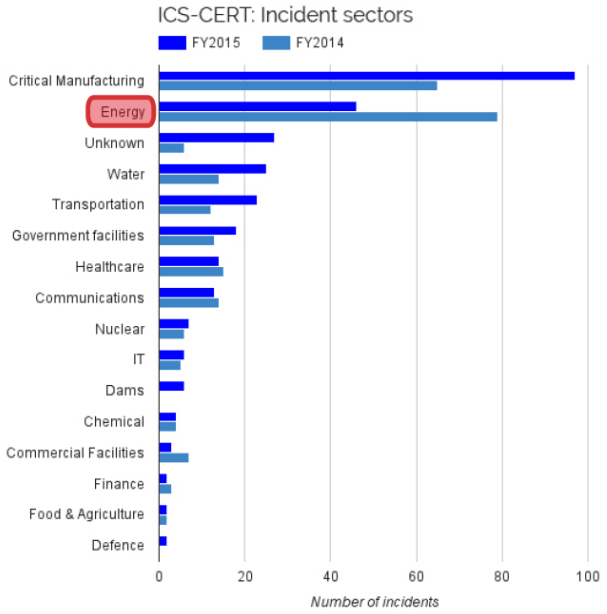




Attack Scenarios – Security Status

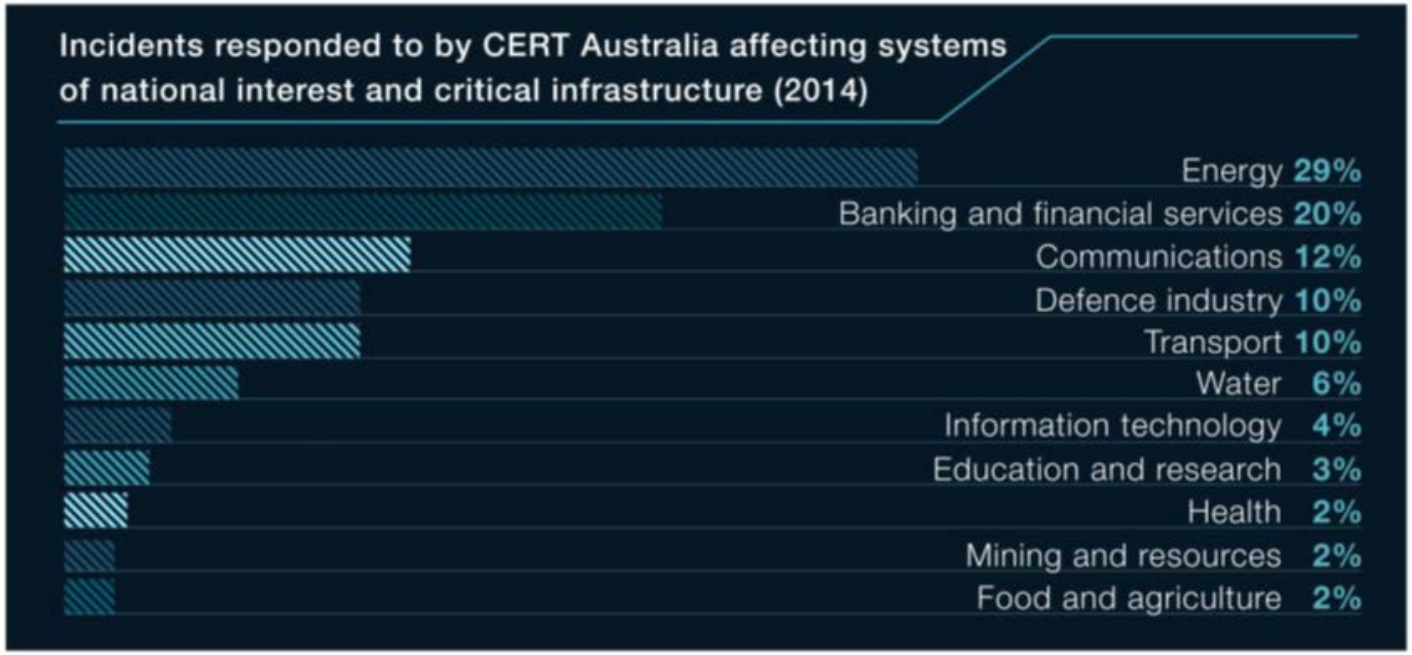
- Increasing number of reported incidents in ICS overall between 2010 and 2015
- Energy sector → no. 1 target of incidents in ICSs in 2014





https://ics-cert.us-cert.gov/

Attack Scenarios - Security

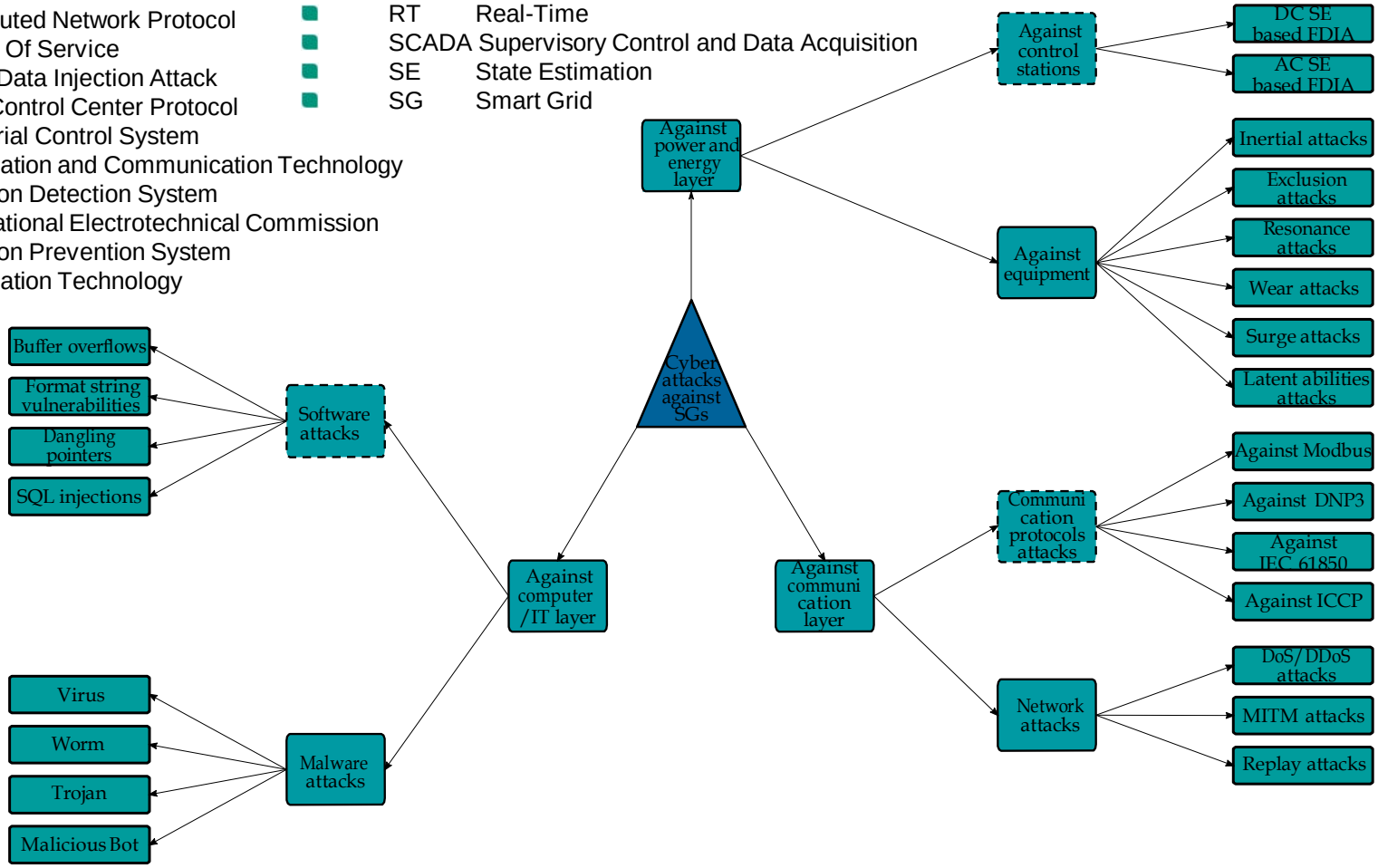


The Australian Cyber Security Centre Threat Report 2015

Angriffsklassen - Grafik

Abbreviations

- AMI Advanced Metering Infrastructure
- BDD Bad Data Detection
- DDOS Distributed Denial of Service
- DNP Distributed Network Protocol
- DOS Denial Of Service
- FDIA False Data Injection Attack
- ICCP Inter-Control Center Protocol
- ICS Industrial Control System
- ICT Information and Communication Technology
- IDS Intrusion Detection System
- IEC International Electrotechnical Commission
- IPS Intrusion Prevention System
- IT Information Technology
- MITM Man-In-The-Middle
- PCS Process Control System
- PLC Programmable Logic Controller
- RT Real-Time
- SCADA Supervisory Control and Data Acquisition
- SE State Estimation
- SG Smart Grid



Angriffspunkte im Smart Grid

Common vulnerability	Reason for concern
Unpatched published vulnerabilities	Most likely attack vector
Web Human-Machine Interface (HMI) vulnerabilities	Supervisory control access
Use of vulnerable remote display protocols	Supervisory control access
Improper access control (authorization)	SCADA functionality access
Improper authentication	SCADA applications access
Buffer overflows in SCADA services	SCADA host access
SCADA data and command message manipulation and injection	Supervisory control access
SQL injection	Data historian access
Use of standard IT protocols with clear-text authentication	SCADA host access
Unprotected transport of application credentials	SCADA credentials gathering

Ten common vulnerabilities identified in NSTB assessments (Table 1)
National Supervisory Control and Data Acquisition (SCADA) Test Bed (NSTB)

Vulnerability Analysis of Energy Delivery Control Systems, September 2011, Idaho National Laboratory, Idaho Falls, Idaho 83415, http://www.inl.gov

… Automobil

- >50% Innovationen Software-bedingt
- Sicherheitskritische Software >10 Millionen Lines of Code
- **Gaspedal- und Motorsteuerung > 1 Million Lines of Code**
- Software Oberklassenfahrzeug entspricht der eines Kampfflugzeuges
- Fehlererkennungsrate (Betriebsbewährung / Reifegrad) nicht messbar, residuale Fehler unbekannt
- **SW ohne Autonomie!**

Analyse aus 2016 von K. R. Bährle

- Fehlauslösung Seitenairbag: SW Fehler in Steuergerät
- Feststellbremse ohne Wirkung: SW Fehler im Steuergerät
- Hochlauf ohne Benutzer: SW Fehler in Motorsteuerung
- Fehlauslösung Kopfairbag: SW Fehler in Steuergerät
- ABS regelt falsch: SW Fehler
- Kraftstoff- und Motorabschaltung: SW Fehler
- Ungewollte Beschleunigung: SW Fehler
- Notlauf wegen Werte außerhalb Grenzen: SW Fehler
- Bremskraft vermindert: SW Fehler
- Deaktivierung von Gurtstraffer statt Airbag: SW Fehler
- Fehlfunktion Automatikgetriebe, Kontrollverlust: SW Fehler
- Ersatzrad nicht erkannt, ABS fällt aus: SW Fehler

Beispiel Sicherheitsgerät Siprotec 5 (Siemens)

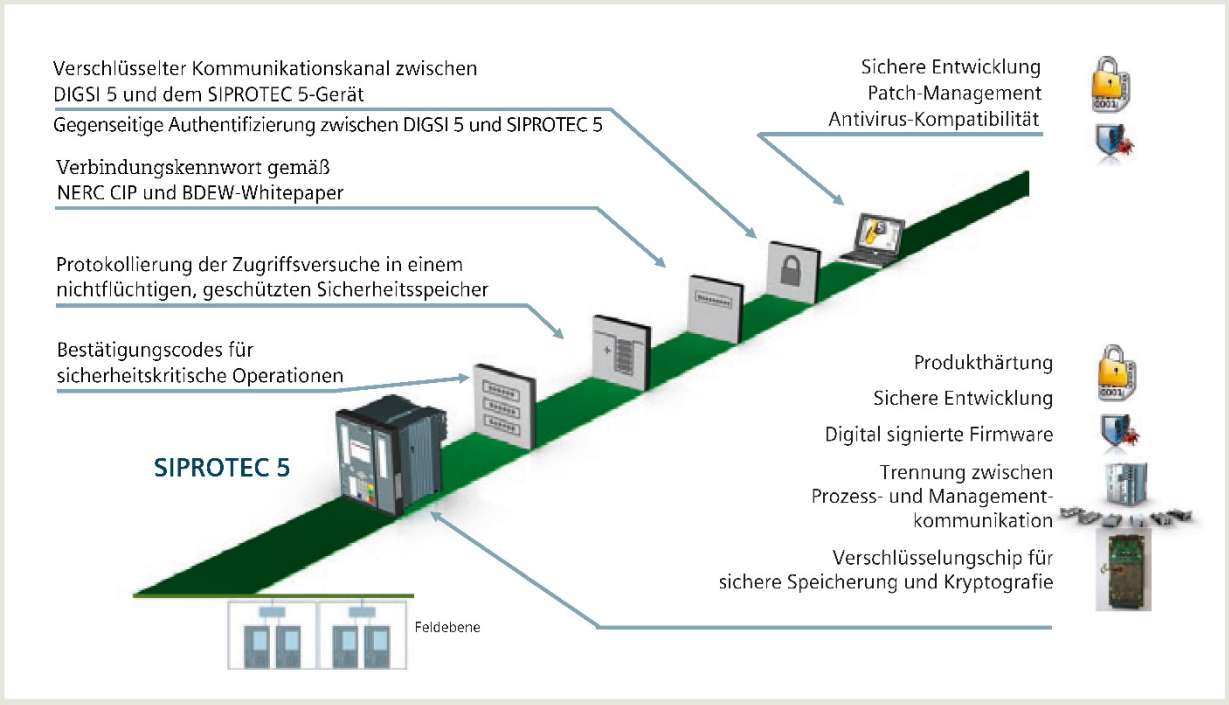


Abb. 8: Sicherheitseigenschaften eines modernen Schutzgeräts

Cyber Security im Energiemanagement
Auszug aus dem Power Engineering Guide, Ausgabe 8.0, Siemens AG

CERT
Advisory (ICSA-18-067-01) Siemens SIPROTEC 4, SIPROTEC Compact, DIGSI 4, and EN100 Ethernet Module (Update B) Original release date: March 08, 2018 | Last revised: May 17, 2018
CVSS v3 7.5 - ATTENTION: Exploitable remotely/low skill level to exploit - Vendor: Siemens - Equipment: SIPROTEC 4, SIPROTEC Compact, DIGSI 4, and EN100 Ethernet module - Vulnerabilities: Missing Authentication for Critical Function, Inadequate Encryption Strength
Successful exploitation of these vulnerabilities could allow an attacker to upload a modified device configuration that could overwrite access authorization passwords, or allow an attacker to capture certain network traffic that could contain authorization passwords.

Beispiel Cisco

- Cisco Releases Security Updates, Original release date: May 16, 2018

- Cisco has released updates to address vulnerabilities affecting multiple products.
- A remote attacker could exploit some of these vulnerabilities **to take control of an affected system**.

- NCCIC encourages users and administrators to review the following Cisco Security Advisories and apply the necessary updates:
  - Digital Network Architecture Center Static Credentials Vulnerability cisco-sa-20180516-dnac
  - Digital Network Architecture Center Authentication Bypass Vulnerability cisco-sa-20180516-dna2
  - Digital Network Architecture Center Unauthorized Access Vulnerability cisco-sa-20180516-dna
  - Enterprise NFV Infrastructure Software Linux Shell Access Vulnerability cisco-sa-20180516-nfvis
  - Meeting Server Media Services Denial-of-Service Vulnerability cisco-sa-20180516-msms
  - Identity Services Engine EAP TLS Certificate Denial-of-Service Vulnerability cisco-sa-20180516-iseeap
  - IoT Field Network Director Cross-Site Request Forgery Vulnerability cisco-sa-20180516-fnd

Cyber Security

- 21.11.2017 **Intel Firmware** Vulnerability
  Intel has released recommendations to address vulnerabilities in the firmware of the following Intel products: Management Engine, Server Platform Services, and Trusted Execution Engine. An attacker could exploit some of these vulnerabilities to **take control of an affected system**.
- 21.11.2017 **Symantec** Releases Security Update
  Symantec has released an update to address a vulnerability in the Symantec Management Console. A remote attacker could exploit this vulnerability to **take control of an affected** system.
- 20.11.2017 **Windows** ASLR Vulnerability
  The CERT Coordination Center (CERT/CC) has released information on a vulnerability in Windows Address Space Layout Randomization (ASLR) that affects Windows 8, Windows 8.1, and Windows 10. A remote attacker could exploit this vulnerability to **take control of an affected system**.
- 16.11.2017 **Siemens** SICAM (Substation Control Systems and Remote Terminal Units)
  CVSS v3 9.8, Remotely exploitable/low skill level to exploit. Public exploits are available. Missing Authentication for Critical Function, Cross-site Scripting, Code Injection. Successful exploitation of these vulnerabilities could allow an unauthenticated remote attacker to execute arbitrary code. (Siemens: Features: Remote maintenance via encrypted end-to-end security!)
- 15.11.2017 **Cisco** Releases Security Update
  Cisco has released a security update to address a vulnerability in its Voice Operating System software platform. Exploitation of this vulnerability could allow a remote attacker attacker **to take control of an affected system**

US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

Cyber Security

- Common Vulnerability Scoring System (CVSS): High Vulnerabilities will be labeled High severity if they have a CVSS base score of 7.0 - 10.0
- **Beispiele:**
  BMC Medical and **3B Medical Luna CPAP Machine**, 08/15/2017
  Medical device advisory contains details for an improper input validation vulnerability in BMC Medical's and 3B Medical's Luna continuous positive airway pressure therapy machine.
  Siemens SIPROTEC 4 and **SIPROTEC Compact** (Update B), 07/27/2017
  Advisory contains mitigation details for improper input validation, missing authorization, and improper authentication vulnerabilities in the Siemens SIPROTEC 4 and SIPROTEC Compact devices.

- 21.11.2017 **In**
  Intel has release
  products: Manag
  attacker could e
- 21.11.2017 **Sy**
  Symantec has r
  Console. A rem
- 20.11.2017 **W**
  The CERT Coor
  Windows Addre
  and Windows 1(
  system.
- 16.11.2017 **Si**
  CVSS v3 9.8, R
  Missing Authent
  exploitation of th
  arbitrary code. (
- 15.11.2017 **C**
  Cisco has releas
  software platform. Exploitation of this vulnerability could [illegible] a remote attacker attacker **to take control of an affected system**

…are of the following Intel …ecution Engine. An …**ffected system**.

…tec Management …**of an affected** system.

… vulnerability in …ows 8, Windows 8.1, …**control of an affected**

…te Terminal Units) …s are available. …ection. Successful … attacker to execute …nd-to-end security!)

… Operating System

Autonomes Fahren

- “EXPLAINING AND HARNESSING ADVERSARIAL EXAMPLES”
- → Panda bleibt Panda – für den Mensch

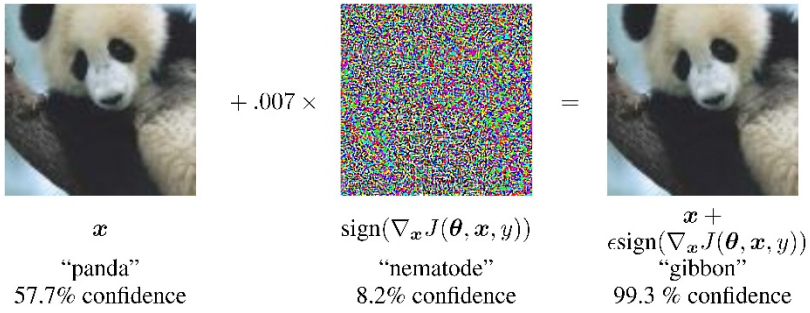


Figure 1: A demonstration of fast adversarial example generation applied to GoogLeNet (Szegedy et al., 2014a) on ImageNet. By adding an imperceptibly small vector whose elements are equal to the sign of the elements of the gradient of the cost function with respect to the input, we can change GoogLeNet’s classification of the image. Here our ϵ of .007 corresponds to the magnitude of the smallest bit of an 8 bit image encoding after GoogLeNet’s conversion to real numbers.

Maschinelle Klassifikation??

- “Accessorize to a Crime: Real and Stealthy Attacks on State-of-the-Art Face Recognition“
- → eine bunter Brille macht einen anderen Menschen!

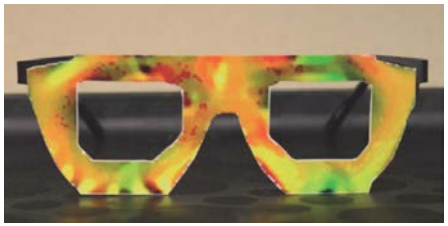


Figure 3: An impersonation using frames. Left: Actress Reese Witherspoon (by Eva Rinaldi / CC BY-SA / cropped from https://goo.gl/a2sCdc). Image classified correctly with probability 1. Middle: Perturbing frames to impersonate (actor) Russel Crowe. Right: The target (by Eva Rinaldi / CC BY-SA / cropped from https://goo.gl/AO7QYu).

… Update Sicherheit Autonomes Fahren

- Deep Learning zur automatischen Erkennung von Situationen und einzelnen Verkehrsteilnehmern
- „Universal adversarial perturbations“ sind für den Menschen irrelevant

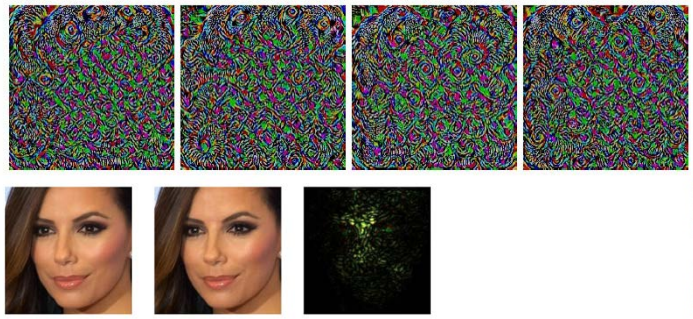


Figure 2: A dodging attack by perturbing an entire face. Left: an original image of actress Eva Longoria (by Richard Sandoval / CC BY-SA / cropped from https://goo.gl/7QUvRq). Middle: A perturbed image for dodging. Right: The applied perturbation, after multiplying the absolute value of pixels' channels ×20.

- … für die Maschine nicht!
  → aus der Wollsocke wird ein indischer Elefant, … ein Grau-Papagei, … ein Papagei, … und so weiter.

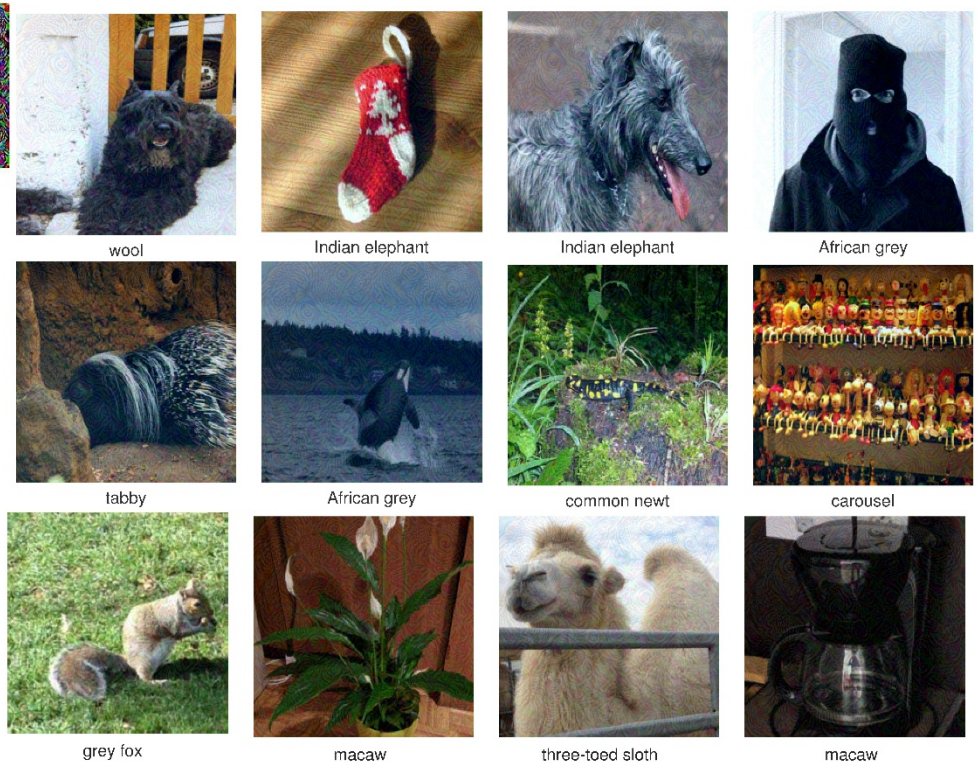


Figure 3: Examples of perturbed images and their corresponding labels. The first two rows of images belong to the ILSVRC 2012 validations set, and the last row are random images taken by a mobile phone camera. We refer to the appendix for the original images.

… Update Sicherheit Autonomes Fahren

Universal Adversarial Perturbations Against Semantic Image Segmentation

Jan Hendrik Metzen
Bosch Center for Artificial Intelligence, Robert Bosch GmbH
janhendrik.metzen@de.bosch.com

Mummadi Chaithanya Kumar
University of Freiburg
chaithu0536@gmail.com

Thomas Brox
University of Freiburg
brox@cs.uni-freiburg.de

Volker Fischer
Bosch Center for Artificial Intelligence, Robert Bosch GmbH
volker.fischer@de.bosch.com

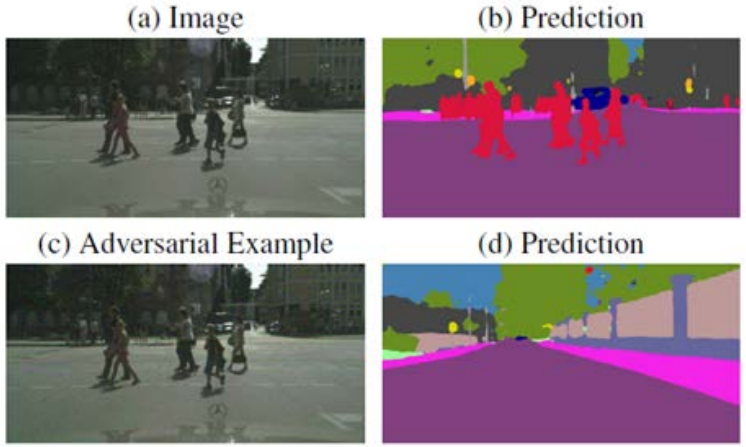
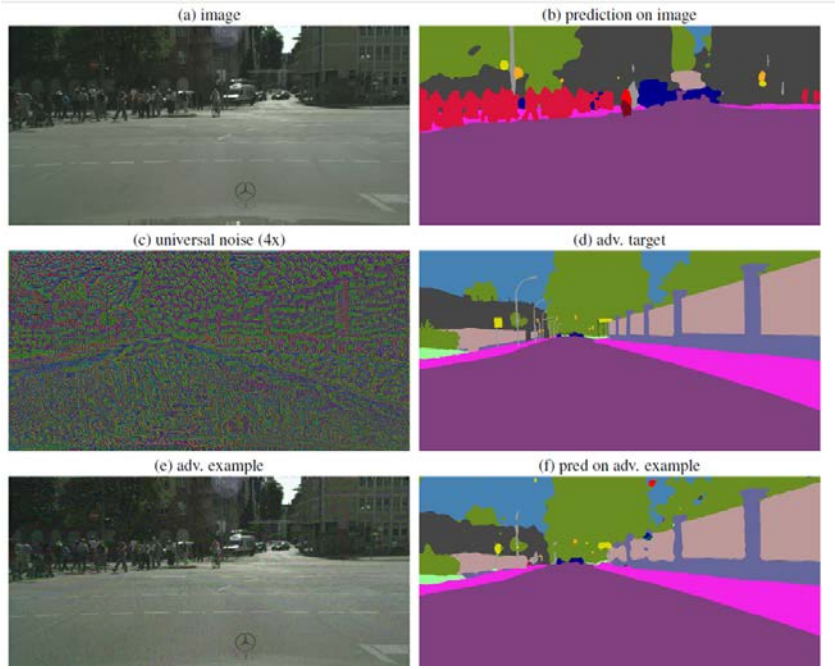
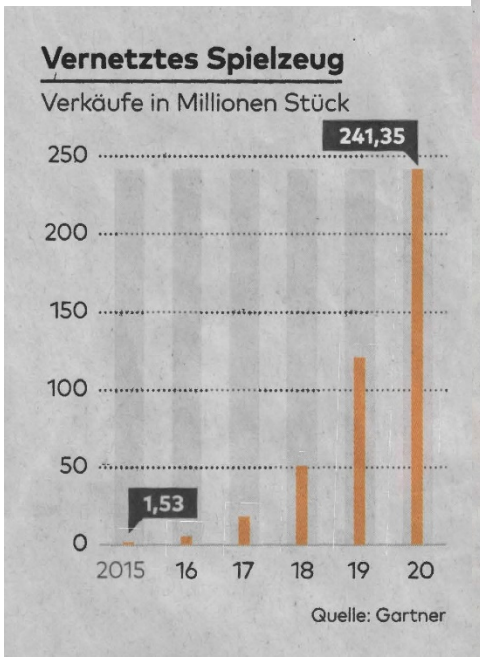


Figure 1. The upper row shows an image from the validation set of Cityscapes and its prediction. The lower row shows the image perturbed with universal adversarial noise and the resulting prediction. Note that the prediction would look very similar for other images when perturbed with the same noise (see Figure 3).



…Update Sicherheit IoT (Toys)

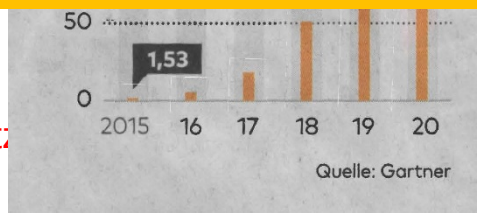
- Puppe Cayla (vom selben Hersteller wie der Roboter i-Que) hat ein Mikrofon im Nacken und schneidet Unterhaltungen mit, die über das Internet übertragen werden.
- Teddys sprechen Sprachnachrichten von den Eltern über das Internet aus. Sollte sich hier jemand von außen zwischenschalten, könnte der Teddy das Kind auffordern, die Wohnungstür zu öffnen. Die möglichen Folgen sind in der Tat beängstigend.
- Puppe ,“Hello Barbie“ von Mattel wurde gehackt. Die Puppe beantwortet die Fragen der Kinder aus der Cloud.
- Ähnlich arbeiten die smarten Lautsprecher Echo von Amazon und Google Home von Google. JackuboWski war es nach eigenen Angaben gelungen, die Anbieterserver durch eigene Server zu ersetzen und so die Sprachnachrichten von Kindern abzufangen, die mit ihrer ,“Hello Barbie“ spielten.
- Schwachpunkt ist Drahtlosverbindung zur Smartphone-App über Bluetooth. Einige Hersteller verzichten hier komplett auf Passwort- oder Pin-Schutz.



Einfallstor für Cyber-Kriminelle: Puppe „Cayla“

…Update Sicherheit IoT (Toys)

- Weitere Gefahren:
  Wiederholt gelang es Hackern, Informationen von Spielzeugen aus Datenbanken der Hersteller zu stehlen.
- Der Lernspielzeug-Anbieter VTech musste dies vor zwei Jahren erfahren, als ihm **64 Millionen Kinder-Profile** mit Namen, Geschlechtsangaben und Geburtsdatum sowie fast **fünf Millionen Eltern-Konten** abhanden kamen. In Deutschland waren knapp 900.000 Profile und Konten betroffen. Dort waren Postanschriften, EMail-Adressen, Passwörter, IP-Adressen und die Liste der bisherigen. Downloads verzeichnet.
  Nachlässig war auch die Firma Spiral Toys. Sie hatte die Daten in einer Datenbank aufbewahrt, die vermutlich wegen eines Einrichtungsfehlers im Internet schlichtweg offen geblieben war. Erpresser griffen die Daten ab ·und waren nach Aussage von Experten damit in der Lage, sogar auf die Sprachaufnahmen der Nutzer zuzugreifen.
- Schwachpunkt ist Drahtlosverbindung zur Smartphone-App über Bluetooth.
  Einige Hersteller verzichten hier komplett auf Passwort- oder Pin-Schutz



safeware
engineering
safe and secure software