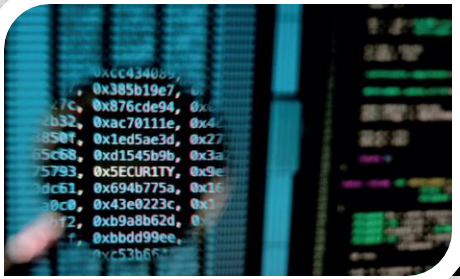


Security Day 2014

Six Ways to Kill by Hacking

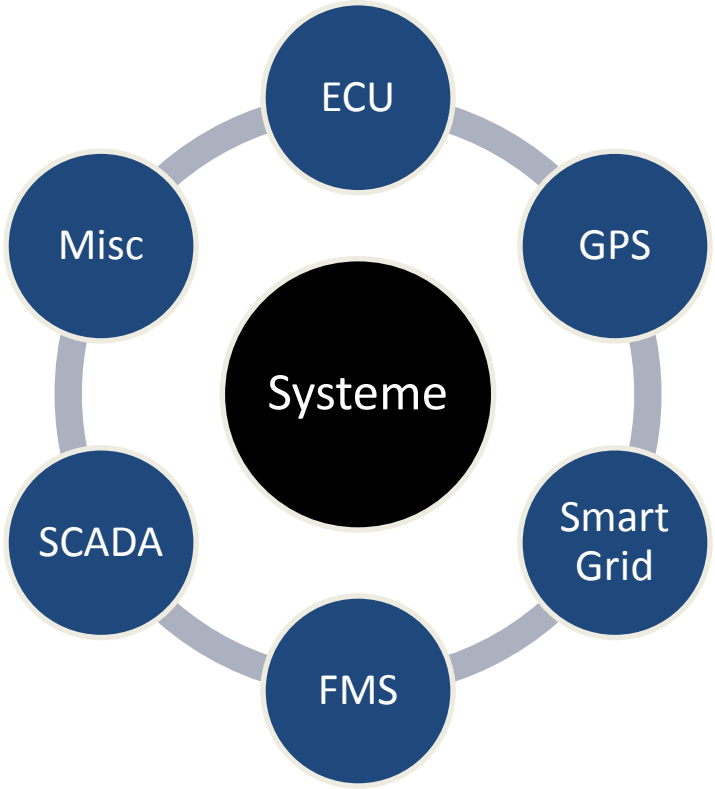
Kritische Systeme · Infrastruktur

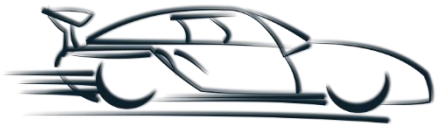
Ein mörderischer Querschnitt

Robert Luh
Institut für IT Sicherheitsforschung, FH St. Pölten

Einleitung

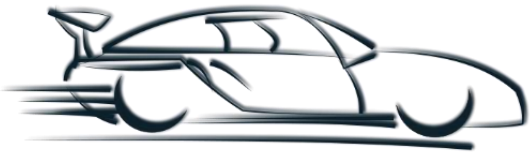
- Thema: Systeme und kritische Infrastruktur
  - Funktionsweise, Sicherheit, Bedrohungen
- Potential für Personenschaden
  - Einzelpersonen, Systemzusammenbruch, Chaos

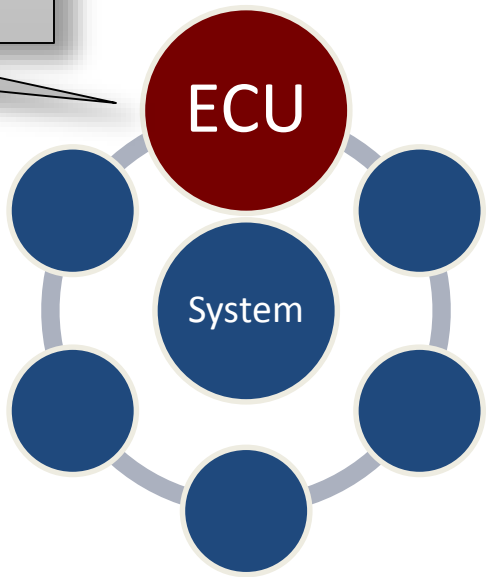




Case #1

- Fahrzeug-Computer
  - Electronic Control Unit (ECU)
  - 50-70 ECUs in einem modernen Auto
  - Verantwortlich für nahezu alle Funktionen
  - Kommunikation über internes Netzwerk (CAN Bus)





ECU: Controller Area Network (CAN)

High-Speed Network

- Motorsteuerung (ECM)
- Bremssteuerung (EBCM)
- Schaltung (TCM)

Low-Speed Network

- Heizung/Klima (HVAC)
- Türsteuerung (RCDLR)
- Airbag und Gurte (SDM)
- Dashboard (IPC)
- Radio
- Diebstahlsicherung

Netze sind verbunden via:
Diagnosesystem (BCM), Telematik

ECU: Sicherheit

Mängel:

- Zugriff auf Bus
  - Etwa über manipuliertes (USB) Gerät
  - On-Board Diagnostics Port (OBD-II) + Laptop
  - Wireless (via Sensoren, Telematik, GSM/UMTS,…)
- CAN Packets
  - Broadcast an alle CAN-Teilnehmer
  - Anfälligkeit für DoS (blockiert ECU-Funktion)
  - Keine Authentifizierung
  - Unzureichende Access Control
    - Diagnosemodus der Werkstätten
    - Schwaches Schlüsselmaterial (16 bit)

Tatmittel ECU

Attack Status: CONFIRMED

Erhöhen der Motor RPM

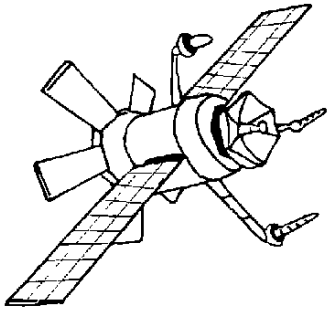
Verriegeln der Türen

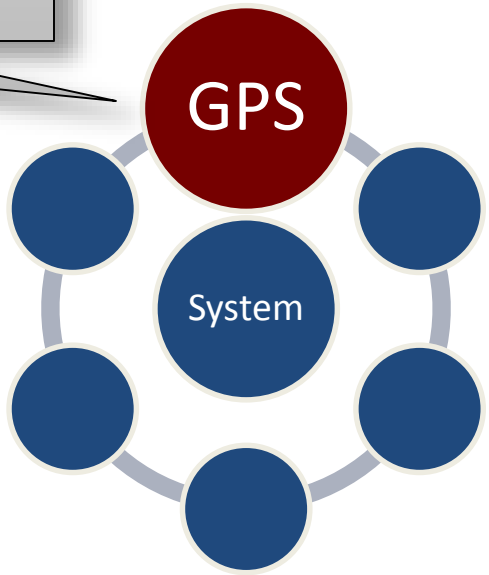
Falsifizierung des Tachos

Deaktivieren der Bremsen

Case #2

- GPS
  - Global Positioning System (GPS)
  - Navigation und Zeitgebung
  - Triangulation (Distanz von 4+ Satelliten durch Transitzeit des Signals)
  - Zeitgebung durch Sat-Atomuhr





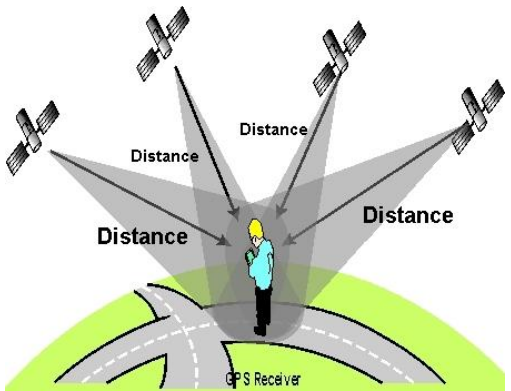
GPS: Nutzung und Technik

Nutzung

- Zivile und militärische Navigation
- Regulierung der Frequenz von Strom-/Telekom-Netzen
- Zeitgebung (auch Internet/NTP)
- Tracking-Systeme
- Frachtverladesysteme

Datenübertragung

- C/A Code (Uhrzeit, Woche, Nav-Daten, Satellit-ID)
- Signalstärke ca. -160dBW (schwach!)



GPS: Sicherheit

Mängel/Bedrohungen:

- Signal-Verschlüsselung
  - Nicht vorhanden (ziviles GPS)
- Jamming
  - Stören des Signals durch ein stärkeres
- Spoofing
  - Fälschung und Überschreiben des Signals
  - Gaukelt echtes Signal vor (manipulierte C/A Daten)
  - Denial of Service auf Endgeräte möglich
- Endgeräte
  - Normale Computer mit oft mangelnder Absicherung
  - Fehlende Integritäts-/Plausibilitätsprüfung

Tatmittel GPS

Attack Status: CONFIRMED/EXPERIMENTAL

Manipulation einer Route

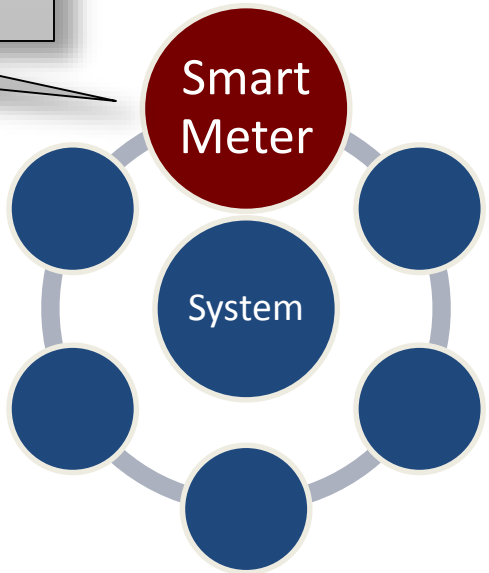
Stören von Ampeln

Middle-of-Earth Angriff

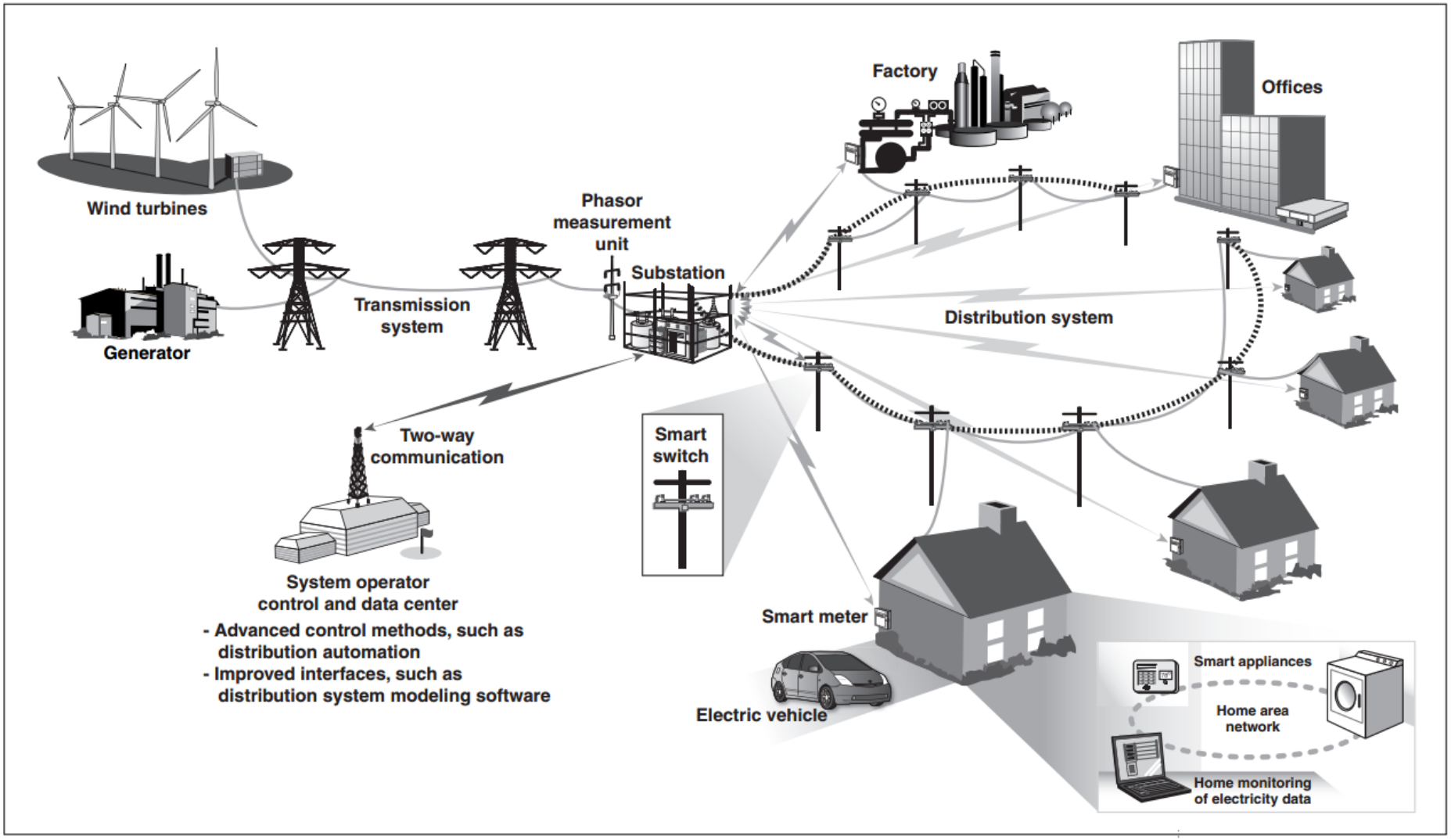
De-Sync des Stromnetzes

Case #3

- Smart Meter
  - Mess- und Steuergerät (Zähler)
  - Meist für Auslieferung von Strom und Gas
  - Vernetzt zum Smart Grid
  - Kommunikation mit HAN/LAN, WAN
  - Wired (PLC) oder Wireless (RF Mesh)
  - Einführung in EU bis 2020



Smart Grid: Aufbau



Quelle: United States Government Accountability Office

Smart Grid: Sicherheit

Mängel/Bedrohungen:

- Mängel
  - Geräte-IDs nicht geheim
  - Passwörter-Wiederverwendung
- Angriffsvektoren
  - Speicher: z.B.: Auslesen von Admin-Passwörtern
  - RF-Signal: Abfangen, Störung, Malware-Verbreitung
  - WAN: MITM Angriffe
- Szenarien
  - Auslesen von Verbrauchsinfos, Rückschlüsse auf verwendete Geräte
  - Service-Unterbrechung
  - Energiediebstahl

Tatmittel Smart Meter

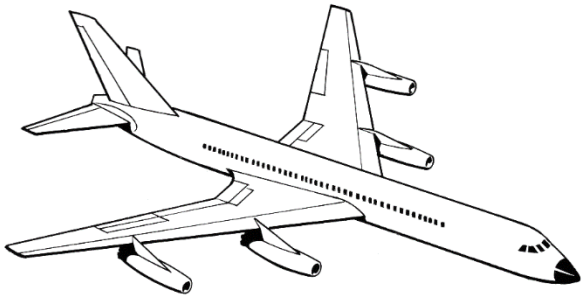
Attack Status: EXPERIMENTAL

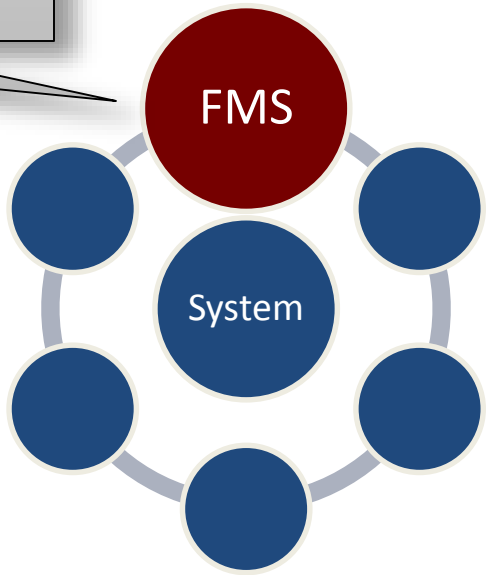
Ausfall

USA 2003: 55 Mio. Betroffene
Indien 2012: 670 Mio. Betroffene

Case #4

- ADS-B/ACARS
  - Automatic Dependent Surveillance Broadcast (ADS-B)
  - Aircraft Communications Addressing and Reporting (ACARS)
  - Flight Management System (FMS)





Flugzeug-Kommunikation: Funktionsweise

ADS-B (Flugzeug Tracking)

- Radio-Datenübertragung von und zum Flugzeug
- Einbau in alle Flugzeuge (USA) bis 2020

ACARS (Bodenstation <> Flugzeug: Datenaustausch)

- Radio oder Satellitenverbindung
- Ankunfts-/Abflug-Informationen
- Wetterdaten
- Triebwerksinformationen

FMS (Bordcomputer)

- Navigationsdatenbank, Flugplan
- Autopilot

FMS: Sicherheit

Mängel/Bedrohungen:

- ADS-B
  - Keine Verschlüsselung
  - Keine Authentifizierung
- ACARS
  - Leichtes Mithören erleichtert Reverse Engineering
- FMS
  - Computersysteme mit Schwachstellen (wie jedes andere auch)

Tatmittel FMS

Attack Status: EXPERIMENTAL/THEORETICAL

Einspielen v. Wegpunkt

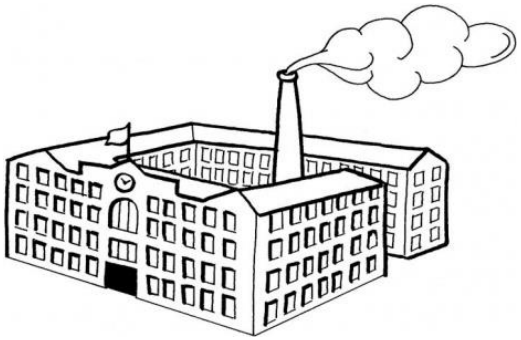
Ändern von Pos.-Daten

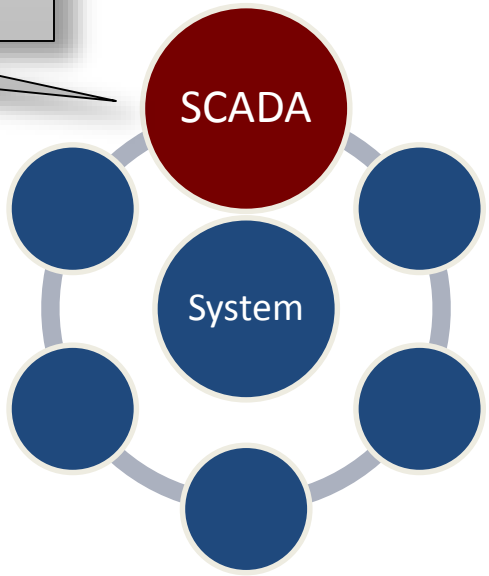
Störung interner Sys.

Autopilot-Änderung

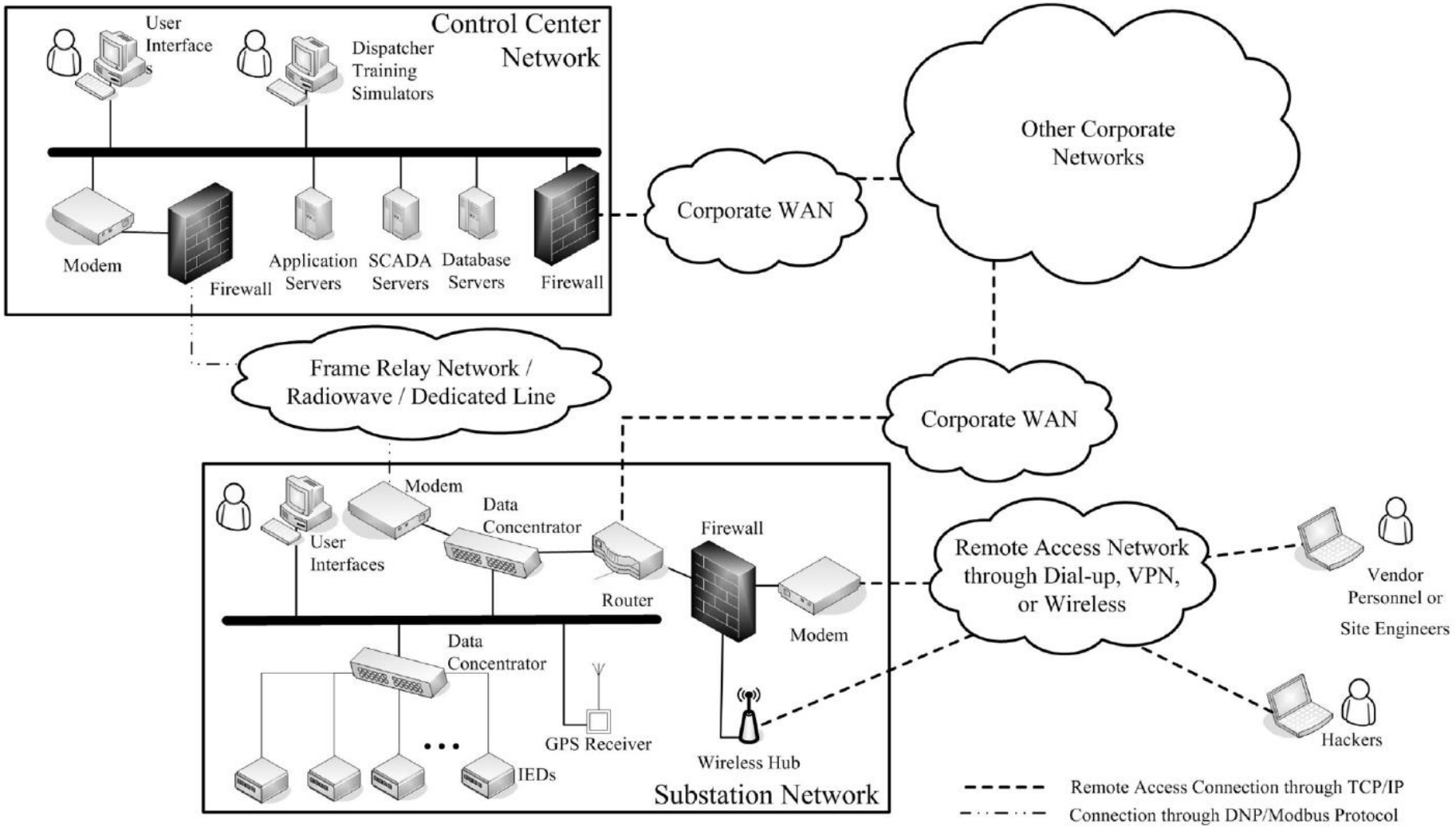
Case #5

- Industrielle Steuerungen
  - Supervisory control and data acquisition (SCADA) Systeme
  - Fertigung, Prozesssteuerung, Automation, Versorgung, Transport,…
  - Abgeschirmtes Netzwerk
  - Remote-Zugriff für Wartungstechniker
  - Programmierung idR durch Windows-SW





SCADA-System: Aufbau



SCADA: Sicherheit

Mängel/Bedrohungen:

- Sicherheit bei Industrie-Computern (CPUs) bisher keine Priorität
- Alte Technologien; wenig Leistung und Speicher (allerdings Echtzeit-fähig)
- Angriffsvektor Programmier-PC (normaler Rechner)
- Web Server direkt auf CPU (z.B. aktuelle SIMATIC Generation)
- Zunehmende (Internet-)Vernetzung; IP-basiert
  - Dial-up, VPN, Wireless, Satellit,…

Tatmittel SCADA

Attack Status: CONFIRMED/EXPERIMENTAL

Gebäude:
Heizung aus

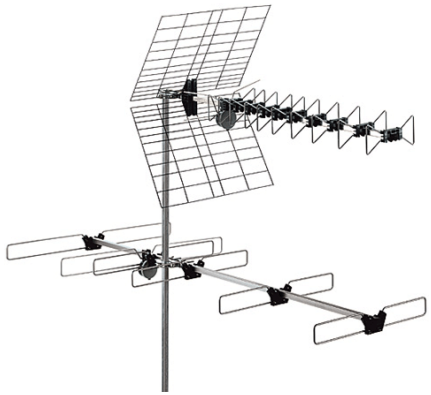
Kanalisation
überfluten

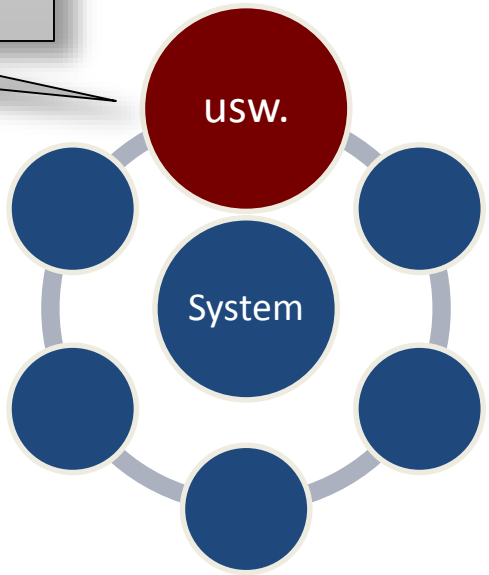
Pipeline-
Bruch

Hollywood
Szenario X

Case #6+

- Stromschlag vom Herzschrittmacher (Remote Hack, 10m Reichweite)
- Manipulation medizinischer Geräte in Spitälern (kommunizieren via LAN)
- Viele weitere Radio-Signal-Komm.: Spoofing/Jamming mithilfe eines Software-Radios (SDR)
- …





Fazit

„Warum einfach, wenn es auch mit einem Computer geht“

- Hi-Tech Morde brauchen viel Know-How
- Aber: Schwachstellen sind oft sehr alt…
- …oder noch kaum erforscht

- Cybercrime nimmt stark zu
- Internet-Verbreitung nimmt zu (IoT und co.)
- Infrastrukturangriffe gefährden nationale Stabilität; nehmen zu

Computer sind mehr als nur PCs und Laptops!
Exoten bleiben nicht immer Exoten!
Sicherheit muss mithalten!
Neue Experten sind gesucht!

Es hat begonnen…

Attack Status: PENDING

Quellen

ECU

K. Koscher et al., “Experimental Security Analysis of a Modern Automobile”, IEEE Symposium on Security and Privacy, 2010.
D.K. Nilsson and U.E. Larson, “A Defense-in-Depth Approach to Securing the Wireless Vehicle Infrastructure”, Journal of Networks, Vol. 4, No.7, 2009.
C. Miller and C. Valasek, “Adventures in Automotive Networks and Control Units”, 2013.
I. Rouf et al., “Security and Privacy Vulnerabilities of In-Car Wireless Networks: A Tire Pressure Monitoring System Case Study”, University of South Carolina, 2010.
University of Innsbruck, “Vehicular Networks (C2X)”, Computer and Communications Systems, Lehrstuhl für Technische Informatik, University of Innsbruck, 2012.
R. Havelt and B. Oliviera, “Hacking the Fast Lane: Security Issues with 802.11p, DSRC, and WAVE”, Trustwave Spider Labs, 2011.
A. Bellissimo et al., “Secure Software Updates: Disappointments and New Challenges”, 1st USENIX Workshop on Hot Topics in Security, HotSec, 2006.
Security Week/AFP, “Car-hacking Researchers Hope to Wake up Auto Industry”, Security Week, https://www.securityweek.com/car-hacking-researchers-hope-wake-auto-industry (accessed 2013/07/30), 2013.

GPS

J.A. Volpe, “Vulnerability Assessment of the Transportation Infrastructure Relying on the Global Positioning System”, National Transportation Systems Center, 2001.
J.S. Warner and R.G. Johnston, “GPS Spoofing Countermeasures”, Los Alamos National Laboratory, 2003.
T. Nighswander et al, “GPS Software Attacks”, CCS’12, Raleigh, North Carolina, USA, 2012.

Smart Grid

G. Rasche, “Intrusion Detection System for Advanced Metering Infrastructure”, Electric Power Research Institute, University of Illinois at Urbana-Champaign, 2012.
P. McDaniel and S. McLaughlin, “Identifying (and Addressing) Security and Privacy Issues in Smart Electric Meters”, http://cnls.lanl.gov/~chertkov/SmarterGrids/Talks/McDaniel.pdf, Network and Security Research Center, Pennsylvania State University, 2011.
C. S. King, “The Economics of Real-Time and Time-of-Use Pricing for Residential Consumers”, Technical report, American Energy Institute, 2001.
S. McLaughlin et al., “Multi-vendor Penetration Testing in the Advanced Metering Infrastructure”, Network and Security Research Center, Pennsylvania State University, 2010.
E. Naone, “Meters for the Smart Grid”, MIT Technology Review Magazine, September/October, 2009.
United States Government Accountability Office, “ELECTRICITY GRID MODERNIZATION - Progress Being Made on Cybersecurity Guidelines, but Key Challenges Remain to be Addressed”, http://www.gao.gov/new.items/d11117.pdf (accessed 2013/11/04), 2011.
U.S.-Canada Power System Outage Task Force, “Interim Report: Causes of the August 14th blackout in the United States and Canada“, 2003.
Organization for Security and Co-operation in Europe (OSCE), “Good Practices on Non-Nuclear Critical Energy Infrastructure Protection from Terrorist Attacks Focusing on Threats Emanating from Cyberspace”, OSCE Study, 2013.
Ausschuss für Bildung, Forschung und Technikfolgenabschätzung, “Gefährdung und Verletzbarkeit moderner Gesellschaften – am Beispiel eines großräumigen und langandauernden Ausfalls der Stromversorgung“, Drucksache 17/5672 des Deutschen Bundestages, 2011.

ADS-B/ACARS/FMS

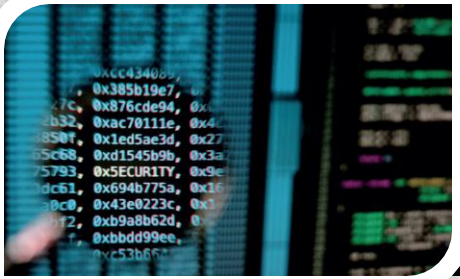
L. Constantin, “Researcher: Vulnerabilities in aircraft systems allow remote airplane hijacking”, http://www.pcworld.com/article/2033807/vulnerabilities-in-aircraft-systems-allow-remote-airplane-hijacking-researcher-says.html (accessed 2013/04/23), IDG News Service, 2013.
A. Greenberg, “Researcher Says He's Found Hackable Flaws In Airplanes' Navigation Systems (Update: The FAA Disagrees)”, http://www.forbes.com/sites/andygreenberg/2013/04/10/researcher-says-hes-found-hackable-flaws-in-airplanes-navigation-systems/ (accessed 2013/07/06), Forbes, 2013.

SCADA

B. Galloway and G.P. Hancke, “Introduction to Industrial Control Networks”, University of Pretoria, revised version, 2012.
C. Ten et al., Vulnerability Assessment of Cybersecurity for SCADA Systems”, IEEE Transactions on Power Systems, Vol.23, No.4, 2008.
N. Subramanian, “Improving Security of Oil Pipeline SCADA Systems Using Service-Oriented Architectures”, OTM 2008 Workshops, LNCS 5333, pp. 344–353, 2008.
G.G. Brown et al., “Analyzing the Vulnerability of Critical Infrastructure to Attack and Planning Defenses”, Operations Research Department, Naval Postgraduate School, 2005.
N. Falliere et al., “W32.Stuxnet Dossier“, Symantec Security Response, Version 1.4, 2011.
D.E. Sanger, “Obama Order Sped Up Wave of Cyberattacks Against Iran”, http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html (accessed 2013/07/06), The New Your Times, 2012.
Industrial Control Systems Computer Emergency Response Team, “Incident Response Activity: Brute Force Attacks on Internet-Facing Control Systems”, ICS-CERT Monitor, April/May/June, 2013.

Misc

United Nations Office on Drugs and Crime, “Comprehensive Study on Cybercrime”, Draft, 2013.
International Telecommunications Union, “Internet users per 100 inhabitants 2006-2013”, http://www.itu.int/en/ITU-D/Statistics/Documents/statistics/2012/ITU_Key_2006-2013_ICT_data.xls (accessed 2013/06/29), ITU Geneva, 2013.
D. Evans, “The Internet of Things - How the Next Evolution of the Internet Is Changing Everything”, Cisco Internet Business Solutions Group, 2011.
T. Heer et al., “Security Challenges in the IP-based Internet of Things”, RWTH Aachen University, 2011.
Department of Homeland Security, “National Strategy for Homeland Security”, www.hsdl.org/?view&did=479633 (accessed 2013/06/27), DHS, 2007.
J. Kirk, “Pacemaker hack can deliver deadly 830-volt jolt”, http://www.computerworld.com/s/article/9232477/Pacemaker_hack_can_deliver_deadly_830_volt_jolt (accessed 2013/11/04), Computer World, 2012.
Wikipedia, “Software-defined Radio”, http://en.wikipedia.org/wiki/Software-defined_radio (accessed 2013/11/04), 2013.



Security Day 2014

Vielen Dank für Ihre Aufmerksamkeit!
Viel Spaß am Security Day!

Fragen?