FH AACHEN
UNIVERSITY OF APPLIED SCIENCES

Angriffe auf SCADA/ICS

Benedikt Paffen

Gregor Bonney

Lehrgebiet Datennetze, IT-Sicherheit
und IT-Forensik

IT Forensik
FH Aachen

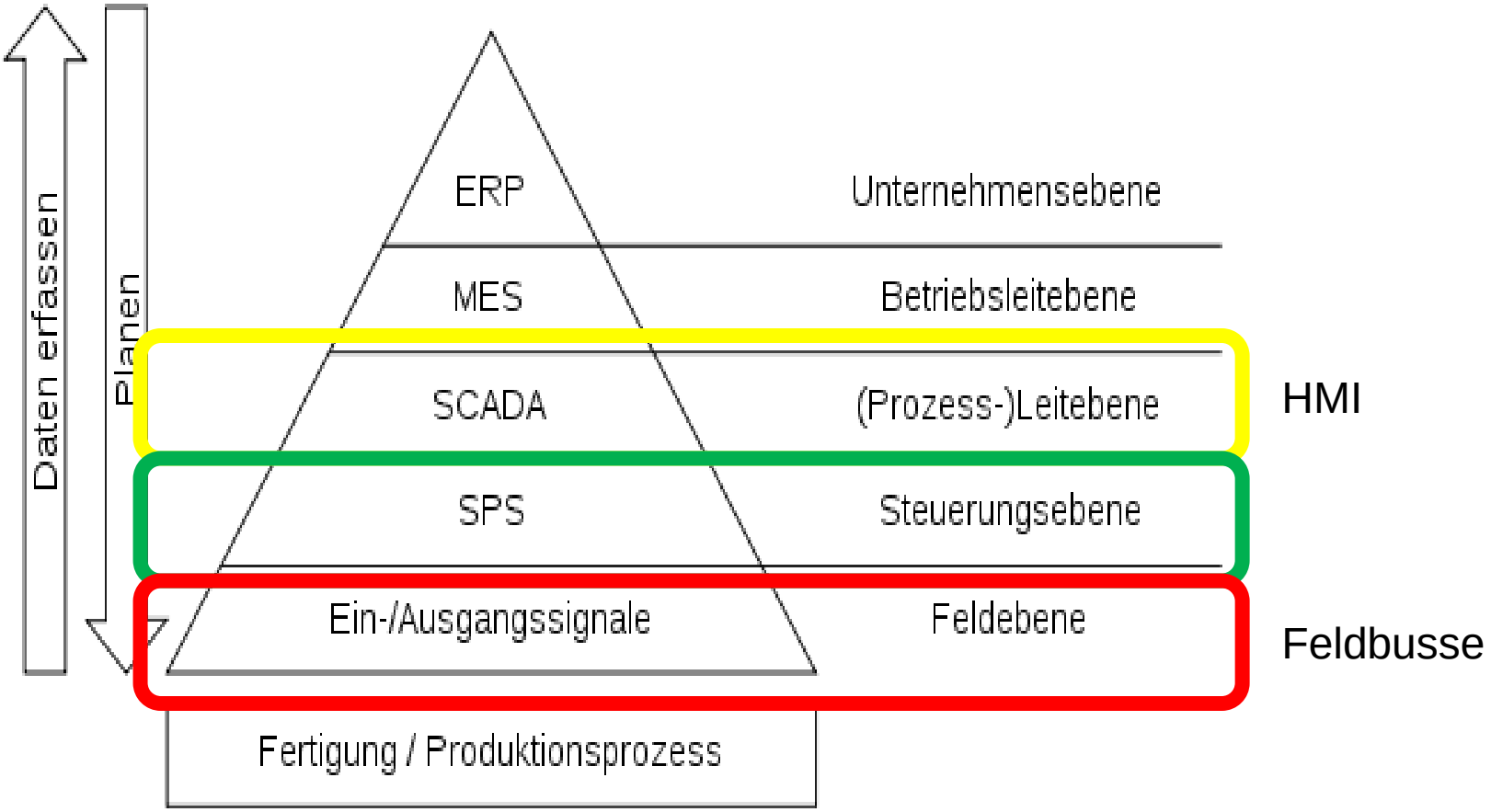
Agenda

1. Einführung
   - Was ist Scada?
   - Gefahren
2. Angriffsmöglichkeiten
   - Konventionelle Angriffe auf Scada/ICS
   - Auf ICS zugeschnittene Angriffe
     - Beispiel anhand einer S7
     - Beispiel anhand einer Beckhoff CX5020
3. Gegenmaßnahmen
   - Möglichkeiten
   - Hindernisse
4. Forensische Möglichkeiten

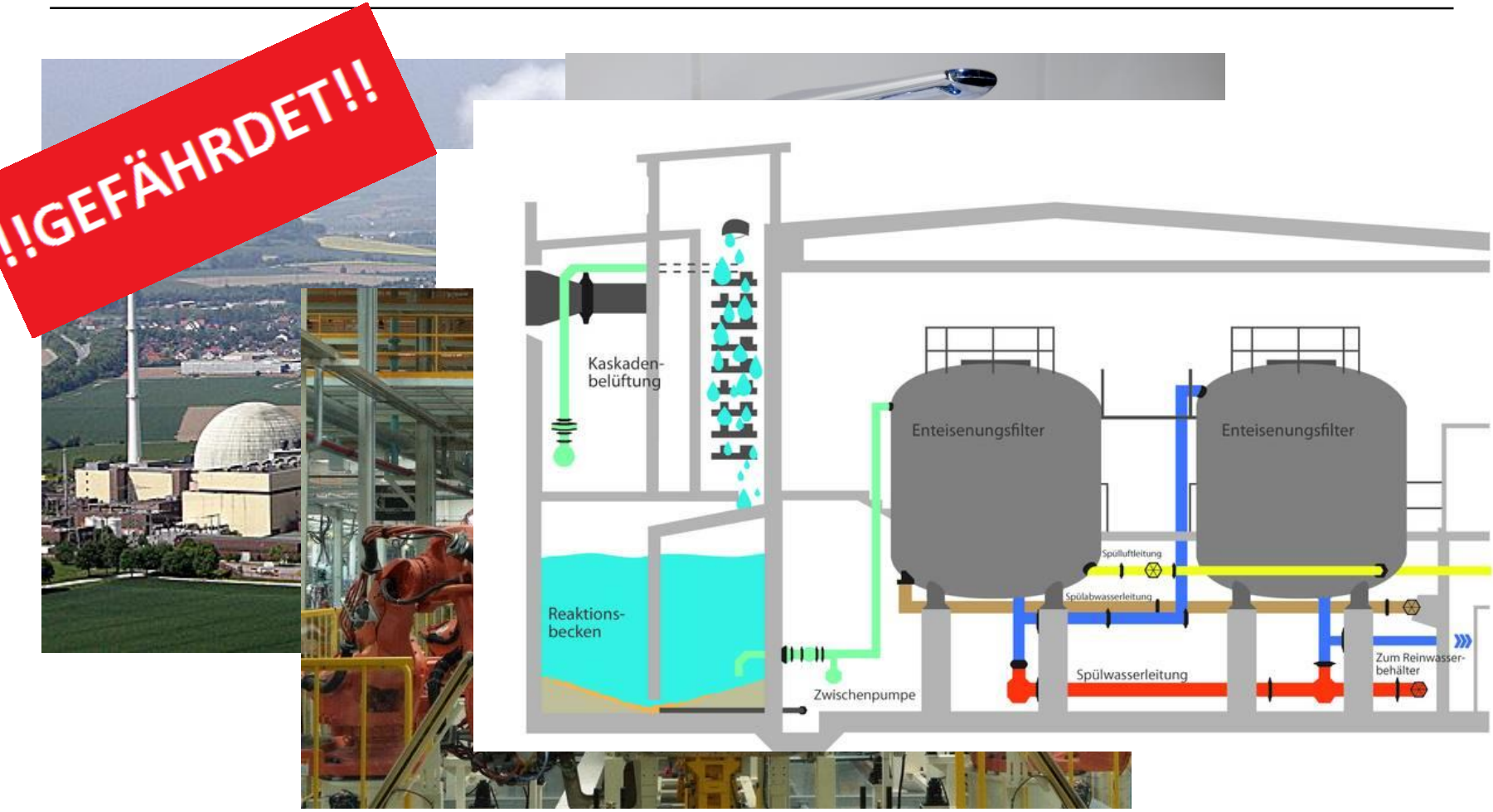
Einführung – Was ist Scada?

- Scada ist die Abkürzung für :
  - ✓ Supervisory
  - ✓ Control
  - ✓ And
  - ✓ Data
  - ✓ Acquisition
- Sammelt Daten
- Steuert Anlagen
- Besteht aus:
  - ➢ Sensoren / Aktuatoren
  - ➢ Speicherprogrammierbare Steuerung
  - ➢ Human-Machine Interfaces
  - ➢ Infrastruktur

Einführung – Was ist Scada?



Einführung - Gefahren



http://maylinee.files.wordpress.com/2009/11/atomkraftwerk_dpa.jpg
http://images.zeit.de/bilder/2009/29/auto/auto-clio/auto-clio-540x304.jpg
http://data.motor-talk.de/data/galleries/0/74/8653/8201117/d2-48788.jpg
https://kids.greenpeace.de/sites/kids.greenpeace.de/files/Wasserhahn_0.jpg
http://www.zvg-dieburg.de/typo3temp/pics/7d3435b383.jpg

Einführung - Gefahren

- Komponenten werden als normale Pc‘s behandelt
  - Kritische Infrastruktur „darf“ meistens nicht gepatcht werden
  - Laufzeiten von teilweise >= 10-20 Jahren
- Häufig direkte Anbindung an das Internet
- Bei der Entwicklung wurde selten auf Sicherheit geachtet
- „Layer-8 Problem“ (Benutzerebene)
  - Einfache Kennwörter z.B. 1234

Konventionelle Angriffe auf Scada/ICS

- Infizierung von wichtigen System, z.B. Arbeitsstation vom Operator
  - Direkter Zugriff auf Code, Passwörter und/oder Informationen
  - Schwer einzudämmen
- Infizierung von eigentlich nicht relevanten System, z.B. Arbeitsstationen von Mitarbeitern
  - System kann als „Hilfsmittel" zum Ziel verwendet werden
  - Social Engineering

Auf ICS zugeschnittene Angriffe

Siemens S7-300*:

- Bekanntes Beispiel „Stuxnet“
  - Urananreicherung wurde verhindert
  - Zentrifugen wurden zerstört
  - Manipulationen der angezeigten Werten
- Zugangsdaten wurden fest eingebrannt
  - Weitere Manipulation möglich
    - Ab- und Anschalten von CPU

*Firmwareversion 2.3.4.

Auf ICS zugeschnittene Angriffe

Beckhoff CX5020:

- Mini-Computer
  - Tastatur und Maus über USB
  - Monitoranschluss (DVI)
  - 2 Netzwerkanschlüsse
- Auslieferungszustand
  - Windows CE
  - ohne Kennwort (Administrator)
  - keine Firewall aktiv

Auf ICS zugeschnittene Angriffe

Beckhoff CX5020:

- Port Scan mit nmap

TCP

PORT	STATE	SERVICE
21/tcp	open	ftp
23/tcp	open	telnet
80/tcp	open	http
139/tcp	open	netbios-ssn?
443/tcp	open	tcpwrapped
445/tcp	open	netbios-ssn
987/tcp	open	unknown
5120/tcp	open	http
5357/tcp	open	http
8080/tcp	open	http-proxy
48898/tcp	open	tcpwrapped

UDP

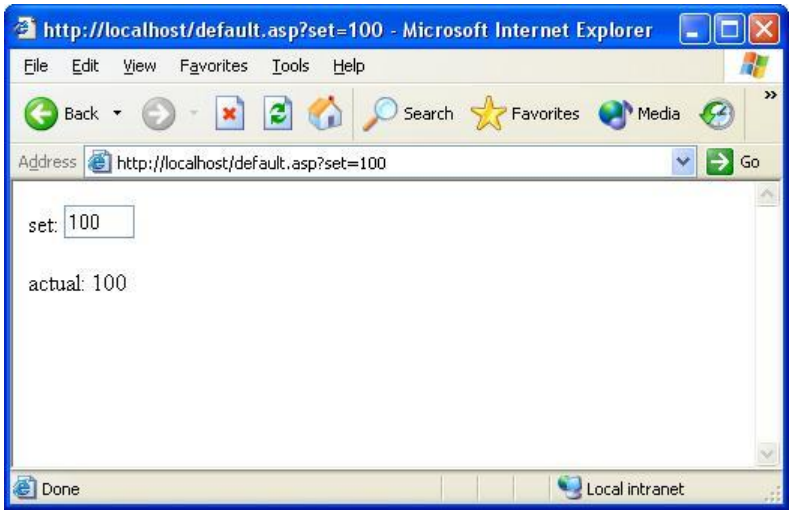
PORT	STATE	SERVICE
123/udp	open	ntp
137/udp	open	netbios-ns
138/udp	open|filtered	netbios-dgm
161/udp	open|filtered	snmp
1900/udp	open|filtered	upnp
48899/udp	open|filtered	unknown

Dienen zur Programmierung
via TwinCAT

Auf ICS zugeschnittene Angriffe

Beckhoff CX5020:

- Nutzungskonzept (beispielhaft)
  - Programmierung der SPS von einem Computer aus mit TwinCAT
  - Webserver zur Steuerung/Überwachung der Prozesse/Sensorwerte



Quelle: http://infosys.beckhoff.com/index.php?content=../content/1031/tcscriptdll/html/tcscriptdll_sample03.htm&id=

Auf ICS zugeschnittene Angriffe

Beckhoff CX5020:

- Absicherungsmaßnahmen
  - Kennwort setzen
  - Firewall einschalten

- Comfort vs. Sicherheit
  - Webserver weiterhin erreichbar
  - Ports zur Programmierung noch erreichbar

Auf ICS zugeschnittene Angriffe

Beckhoff CX5020:

- Gefahren
  - Single User System
    - Alle Prozesse laufen als Administrator (Windows CE)
  - Keine Verschlüsselung verwendet
  - Angreifbarkeit der Dienste hinter den offenen Ports
    - Webserver → Buffer overflow?
    - TwinCAT → unbekanntes Protokoll?

Gegenmaßnahmen

- Passwörter sinnvoll wählen
- Patchen
- Audits
- Verwenden von Subnetzen:
  - Bildung von Zonen
  - IPS (spezielle und allgemeine)
- VERWENDUNG VON VPNs!
- Absicherung/Authentifizierung von Feldbusen*

* Implementierungsmöglichkeit durch Hersteller muss gegeben sein

Hindernisse

- Patch Management
  - Ausfallzeiten oft teuer und/oder unmöglich
  - Unverträglichkeit von Software/Patchs
- Tests und Audits nur „im Labor“
  - Absturz kann schwere Folgen haben
- Schwache Hardware
  - Abarbeitung von Code oft auf dedizierter Hardware
- Betriebssysteme
  - Veraltet und nicht für Sicherheit ausgelegt

Forensische Möglichkeiten

- Betriebssystem von Flash Speicher gelesen
  - Wear Leveling
  - Unterschiedliche Controller / Hersteller
- Ramdisk zur Ausführungszeit
  - Wird beim Herunterfahren geschrieben
- Forensik-Tools zur Live-Response unter CE nicht lauffähig?

Ende

Vielen Dank für Ihre Aufmerksamkeit!

Gibt es Fragen?

Kontakt:

BenediktPaffen@alumni.fh-aachen.de
GregorBonney@alumni.fh-aachen.de