IT-SICHERHEIT IN ZEITEN VON INDUSTRIE 4.0

PROF. DR. TOBIAS HEER – HOCHSCHULE ALBSTADT SIGMARINGEN

ZU MEINER PERSON

- Tobias Heer
  - Hochschule: Professor an der Hochschule Albstadt-Sigmaringen
    - Netzwerke
    - Kommunikationssicherheit
    - Offensive Sicherheit
  - Industrie: CTO Office bei Hirschmann Automation & Control
    - Sicherheit von Industrienetzwerken
    - Industrie 4.0
    - Drahtlose Kommunikation, WLAN
  - Arbeit im Bereich Industrie 4.0
    - Plattform Industrie 4.0 – AG 3 – Sicherheit vernetzter Systeme
    - ZVEI – Sicherheit Industrie 4.0

Hochschule Albstadt-Sigmaringen
Albstadt-Sigmaringen University

HIRSCHMANN
A BELDEN BRAND

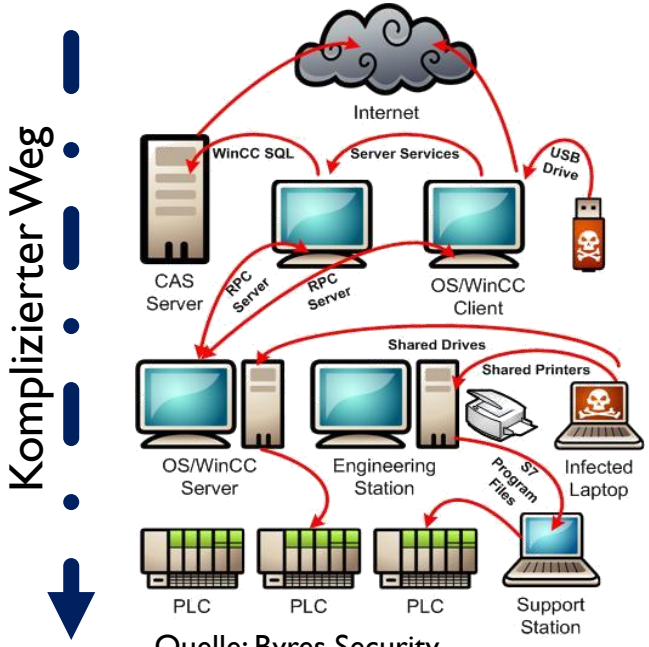
PLATTFORM INDUSTRIE 4.0

ZVEI: Die Elektroindustrie

SICHERHEIT UND INDUSTRIE – EIN NEUES THEMA?

- Cyberangriffe auf Industrieanlagen gibt es bereits seit Jahrzehnten
- Besonders bekannt: Stuxnet
  - Angriff auf Urananreicherung im Werk Natanz (Iran)
  - Erste Stuxnet Version: November 2005
  - Entdeckung von Stuxnet: ca. 2009
  - Ende des Angriffs: Juni 2012
- Angreifer bei Stuxnet: Advanced Persistent Threat - Geheimdienste
  - Große Herausforderung: Schadcode auf Industriegeräte bekommen → Air Gap.
- Muss ich als Firma im schönen Schwabenländle Angst vor einem solchen Angreifer haben?
  - Vermutlich eher nicht → Ist nun alles gut?

Quelle: http://blog.nuclearsecrecy.com/tag/centrifuges/



Quelle: Byres Security

CYBERSICHERHEIT UND KEKSPRODUKTION – WAS DA KANN SCHON SCHIEF GEHEN?

Bildquelle: Jerome C. Baysmore, U.S. Air Force - Beispielbild

ANGRIFF AUF EINE KANADISCHE KEKSFABRIK – AUGUST 2015 (INDUSTRIE 3.0)

- Annahme der Ingenieure: “Was soll schon passieren? Im schlimmsten Fall sind die Kekse ungenießbar. Da fällt uns eine Tagesproduktion aus.”

- Angreifer dringen ins Netzwerk ein und beginnen damit das Netzwerk zu Analysieren
  - Steuerungen wurden gestört
  - Keine Kontrolle über die Anlage
  - Keksteig trocknete in den Rohren ein – die Rohre mussten herausgeschnitten werden

Bildquelle: Jerome C. Baysmore, U.S. Air Force - Beispielbild

ANGRIFFE AUF DIE INDUSTRIE

Angriffe auf Industrieanlagen

OT

Stuxnet (Iran, Siemens PLCs) (2010)

Black Energy 2 (Spionage) (Dez 2010)

Deutsches Stahlwerk (Sabotage) (2014)

HAVEX RAT (Spionage, OPC) (Dez 2014)

Black Energy 3 Power Ukraine (Dez 2015)

Wannacry (DB, Renault, Nissan)

Zeit

Angriffe auf Industriebetriebe

IT

Night Dragon (Spionage, Oil& Gas) (2009)

Operation Aurora (Spionage & Manip., Tech) (2009)

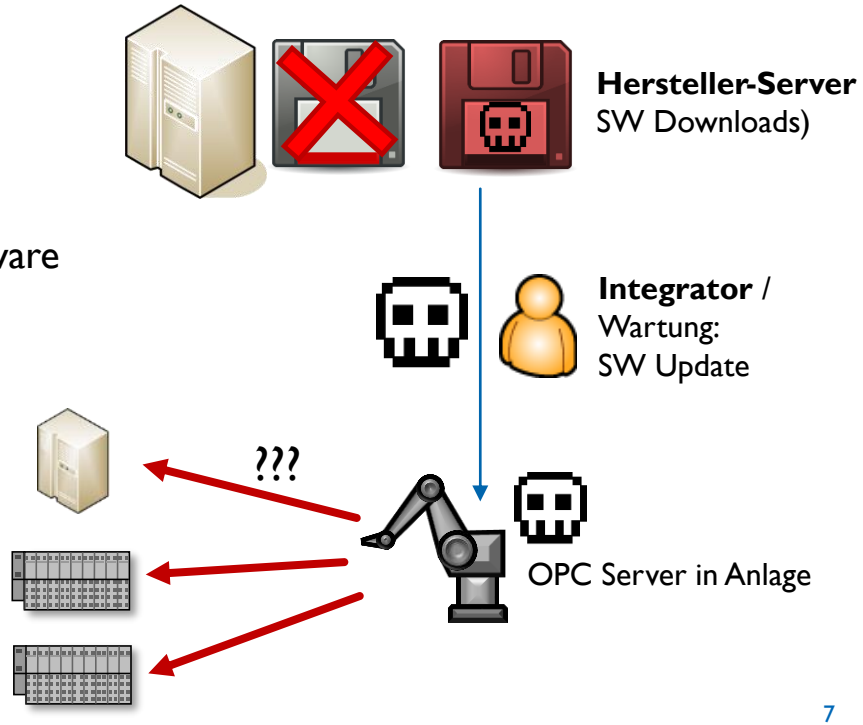
Shamoon (Saudi Arabian Oli) (Wiper) (2012)

Wannacry (Ransomware) (Mai, 2017)

Hochschule Albstadt-Sigmaringen
Albstadt-Sigmaringen University

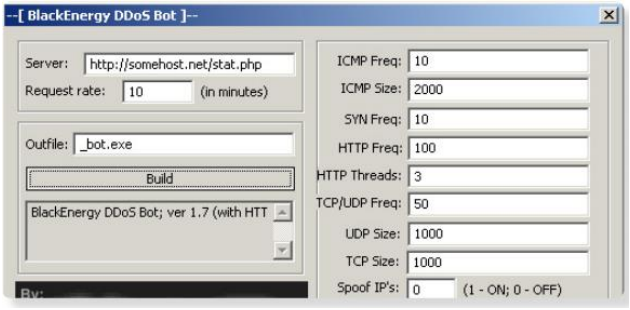
DRAGONFLY / HAVEX RAT

- Die Dragonfly Kampagne verwendete das HAVEX Remote Access Tool (HAVEX RAT)
- Ca. 2000 Anlagen infiziert
  - Hauptsächlich Anlagen aus dem Bereich PT&D und Petrochemie
- Angriff hatte „nur“ Spionage als Ziel → Keine Unterbrechung der Produktion
  - Verwendung von OPC um Industrieanlagen auszuhorchen und zu kartografieren
- Möglichkeit weitere Module und Funktionen nachzuladen
- Verbreitung über verschiedene Wege:
  - Spam Mails (Spear Phishing)
  - Watering Hole Attack: Austausch der Gerätesoftware auf Webseiten der Hersteller
- Hersteller in De, Fr und Ru betroffen
  - Remote Management Software
  - Kamera-Software
  - ICS Applikationen

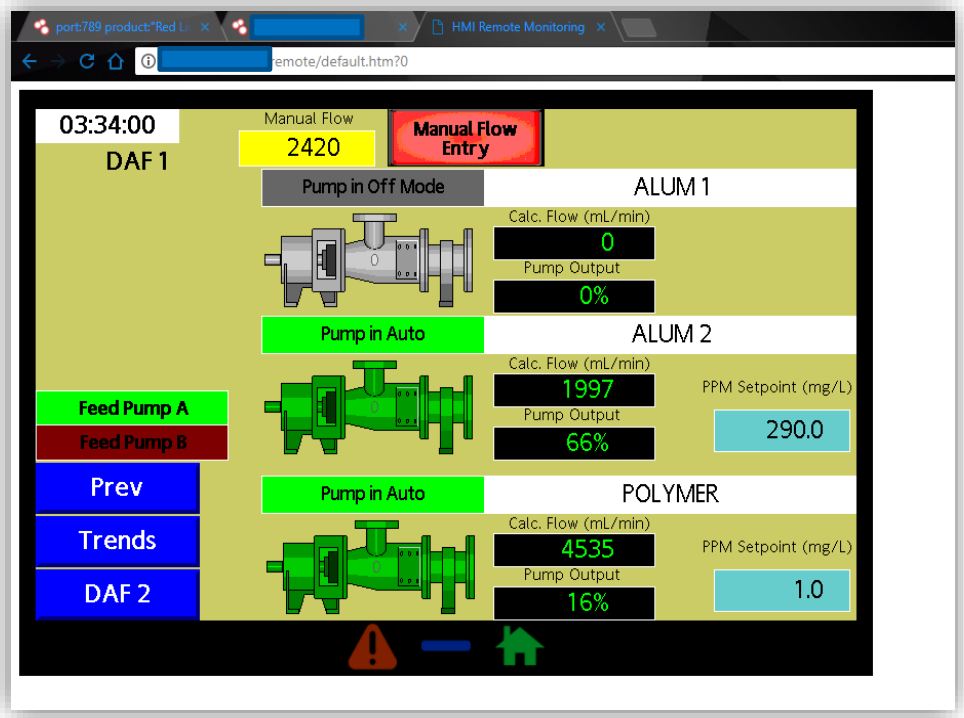


BLACKENERGY 2

- Blackenergy 2: Angriffe auf Industrieanlagen
- Primärer Fokus: HMI
  - Siemens SIMATIC
  - GE SIMPLICITY
  - Advantech WebAccess
- Angriff gegen HMI Systeme die mit dem Internet verbunden waren
- Vorteil von Angriff auf HMI:
  - Parameter können verändert werden
  - Tatsächlicher Zustand der Anlage kann verschleiert werden
  - Angreifer hat direkte Kontrolle über Internet-Verbindung



Originaler BlackEnergy Builder von 2007, Quelle: F-Secure.com



SCADA Interface einer Pumpensteuerung (bei shodan.io gefunden)

BLACKENERGY 3 UND KIEW BLACKOUT 2015

- Blackenergy 3 enthält keinen Schadcode der direkt Industrieanlagen angreift
  - Angriff über Büro Netzwerke der Energieversorger
  - Eindringen über Verbindungen zwischen Büro- und Produktionsnetzwerk
  - Zerstörung von PC Systemen in den Anlagen durch KillDisk Malware
  - Zerstörung von Seriell-zu-Ethernet Konvertern durch fehlerhafte Firmware
- Im Dezember 2015 wurden 225.000 Haushalte durch Blackenergy 3 vom Strom abgeschnitten
  - Der Energieversorger benötigte 6 Stunden um die Anlagen wieder von Hand anzufahren
  - In manchen Anlagen musste bis zu einem Jahr ein Handbetrieb gefahren werden
  - Volle Automatisierung wurde erst nach einem Jahr wiederhergestellt

Umspannwerk, Quelle: Wikimedia[1]

STROMAUSFALL IN DER UKRAINE (23.12.2015):

Hallo, hier Parlament!

Zu alt! Bitte aktualisieren!

E-Mails an Mitarbeiter des Energieversorgers, mit der Werchowna Rada als vermeintlichem Absender, dem ukrainischen Parlament.

Anhang: eine Word-Datei; Beim Öffnen erschien die Meldung, die Word-Version sei veraltet, zum Aktualisieren müsse ein Makro ausgeführt werden.

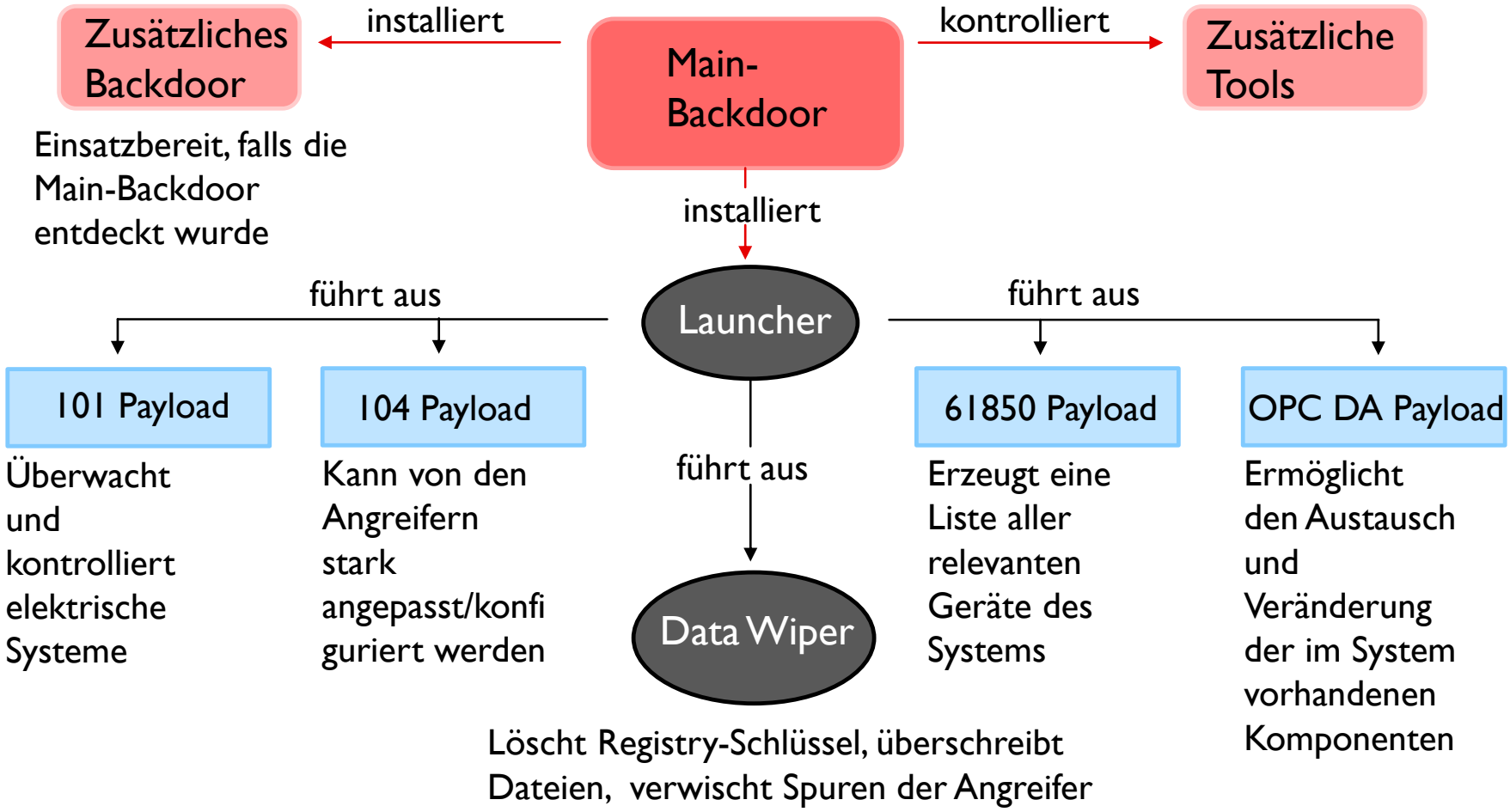
Makro installiert Black Energy 3 Malware. Anlage wird über Büro Netz infiziert und gestört.

CRASHOVERRIDE / INDUSTROYER

- Malware die spezifisch auf Industrieanlagen zugeschnitten ist
  - Ist in der Lage Schaltkreisunterbrecher in Umspannwerken und Kraftwerken zu manipulieren
  - Ziele in den Bereichen Energie-, Wasserversorgung und Verkehrssteuerung
- Erfolgreicher Angriff (Test?) verursachten einen großflächigen Stromausfall für 75 Minuten in Kiew/Ukraine am 17. Dezember 2016
  - Siemens SIPROTEC Unterbrecher
  - Anonyme Kommunikation über TOR Netzwerk
- Angriff auf Los Angeles Verkehrssteuerungssystem verursachte Staus
- Adaptive Malware mit vielen Erweiterungen für Protokolle in Industrieanlagen
  - IEC 104, IEC 101, IEC 61850, OPC DA

Kraftwerk, Quelle: Wikimedia

INDUSTROYER / CRASHOVERRIDE MALWARE MAIN-BACKDOOR



DEUTSCHES STAHLWERK 2014

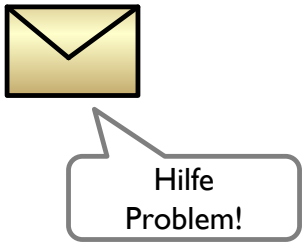
- Erwähnung in BSI Lagebericht 2014
- Um welches Stahlwerk es sich handelt, wird nicht genannt.
- Der Vorfall blieb zunächst komplett geheim.
  - Er wurde erst mit dem Lagebericht 2014 des Bundesamts für Sicherheit in der Informationstechnik bekannt.
  - Der Angriff führte dazu, dass ein Hochofen nicht mehr kontrolliert heruntergefahren werden konnte
  - Die gesamte Anlage wurde schwer beschädigt
  - Die genauen Schäden und Einzelheiten des Vorfalls wurden nicht veröffentlicht

Bundesamt für Sicherheit in der Informationstechnik

Hochofen, Quelle: Wikipedia

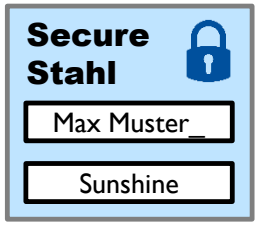
VORGEHENSWEISE DER ANGREIFER (LAUT BSI)

Erstellung einer gefälschten Webseite mit Login Feldern



Mail an Service-Firma, mit dem Link zur gefälschten Webseite

Hierbei wird angegeben, man sei Kunde der Servicefirma und die Anlage habe ein Problem



Erhalt der Zugangsdaten des Service-Technikers

Der Techniker wird auf die original Seite umgeleitet, um keinen Verdacht zu schöpfen

Zugriff auf das Stahlwerk mit den Anmeldedaten des Servicetechnikers

WANNACRY / WANNACRYPTOR

- Ransomware Wannacry
  - Infektion von ungeschützten Windows Systemen (bis Windows 7) weltweit
  - Große Schäden in Industrie-Anlagen, Transportwesen, etc.
- Malware dringt in Intranet der Firma ein und verbreitet sich von dort aus auf Systeme die nicht aus dem Internet erreichbar sind
- Spezialsysteme (Kassensysteme, Geldautomaten, Anzeigen, …) aufgrund schlechtem Patch-Stand besonders betroffen
- Nettes Detail: Der Angriff stammt aus dem Arsenal der amerikanischen Geheimdienste und wurde 5 Jahre lang unbemerkt genutzt
- Ca. 3000 Infektionen von Industrie-Anlagen mit gewöhnlicher Malware jährlich (https://dragos.com/blog/mimics/)

Geldautomaten in China:

Anzeigetafeln bei der Deutschen Bahn:

WANNA CRY - ÜBERSICHT

- Hintergrund:
  - Veröffentlichungen auf Wiki Leaks über Schwachstellen im Windows Betriebssystem namens Eternalromance, -blue, -synergy.
  - Höchst wahrscheinlich wurde Microsoft von der CIA über entwendete Zero Day Exploits gewarnt.

Quelle: Heise-Security[1]

12. März

- Microsoft stellt vorsorglich einen Sicherheitspatch für unterstützte Systeme zur Verfügung

14. April

- Veröffentlichung detaillierter Exploit Anleitungen
- Experten warnen vor einem baldigem großangelegtem Angriff

12. Mai

- Erste Maleware unter Verwendung der veröffentlichten Schwachstelle Eternalblue infiziert ein Krankenhaus in Großbritanien, ihr Name WannaCry

13. Mai

- Ein entdeckter „Kill-switch“ stoppte weitere Verbreitung in Netzwerken
- Microsoft verteilt nachträglich kostenlose Updates für XP

AUSWIRKUNGEN VON WANNACRY

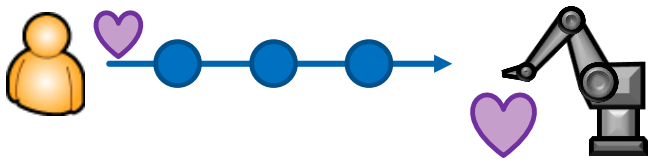
- 147 Varianten von WannaCry wurden gefunden (Quelle: AV Test)
- Schaden geht in die Milliarden
  - Krankenhäuser in GB mussten Betrieb einschränken
  - Ausfall der Fahrkartenautomaten und Anzeigetafeln der DB
  - Innenministerium in Russland meldete 1.000 infizierte Rechner
  - Renault stoppt Produktion in einigen Werken
  - Nissan Werk Sunderland wurde infiziert
  - Tankstellen und Geldautomaten in China konnten keine Transaktionen durchführen
  - Telefónica, FedEx, Stahlkonzern Sandvik und viele weitere Betriebe betroffen
- Nur ca. 30.000 EUR Lösegeld erzielt
- War das Ziel wirklich das Lösegeld?

RENAULT

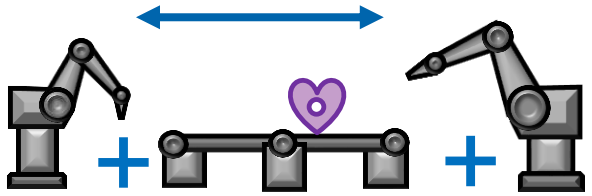
SICHERHEIT UND INDUSTRIE 4.0?

… UND MIT INDUSTRIE 4.0?

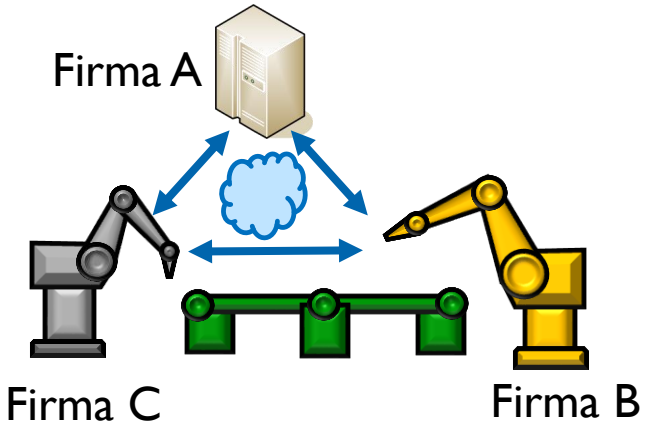
- Kundenspezifische Produktion:
  - Kunden können ihre eigenen Kekse bestellen?



- Wandelbare Produktion:
  - Neue Zusammenstellung von Maschinen und Abläufen
  - Stichwort Plug & Produce

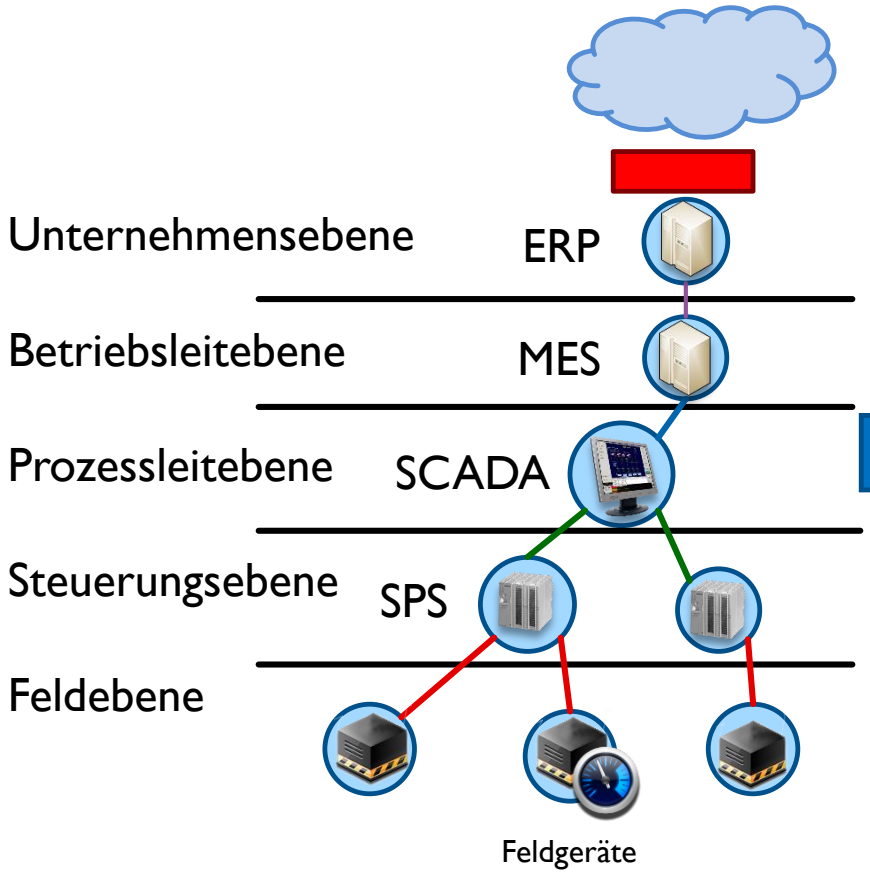


- Wertschöpfungsnetzwerke
  - Engere operative Zulieferer – Produzenten-Beziehungen
  - Kommunikation über Unternehmensgrenzen
  - Kommunikation über Standortgrenzen
  - Dienstleister in der Fertigung

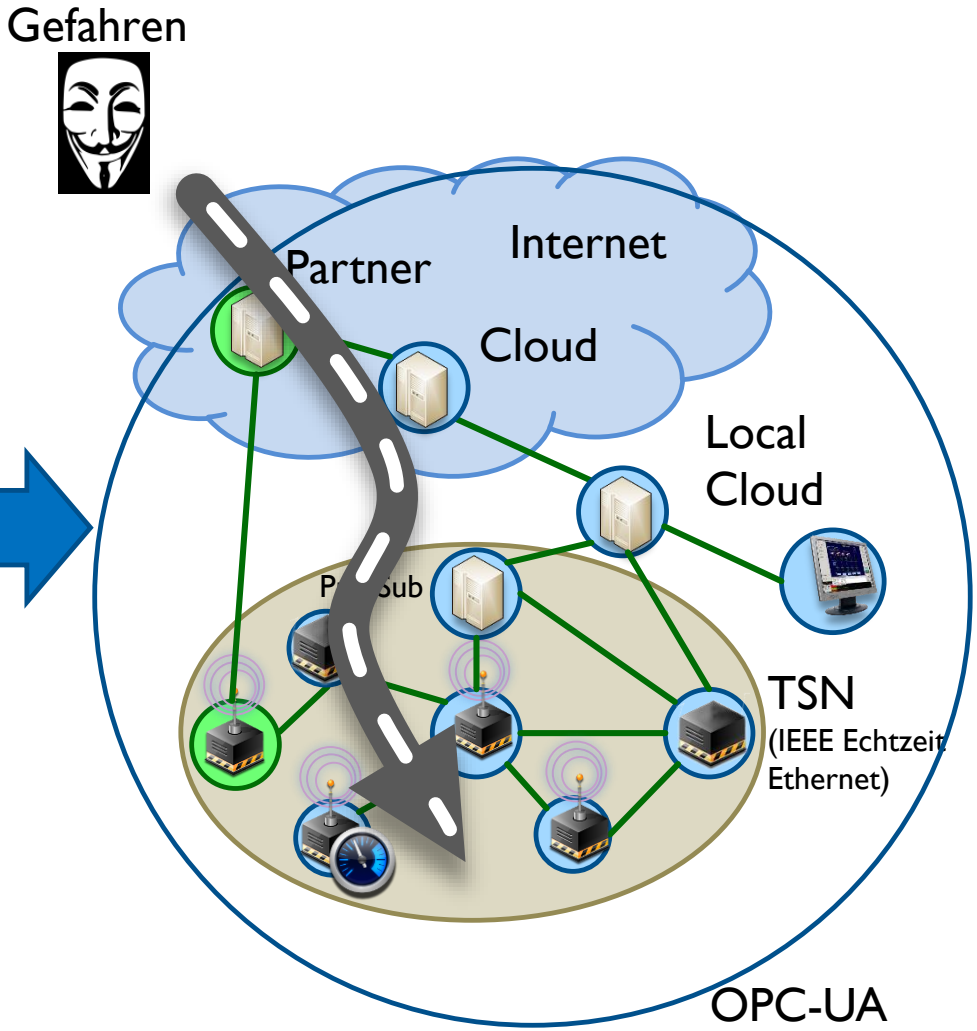


I-4.0 - NEUE KOMMUNIKATIONSSTRUKTUREN

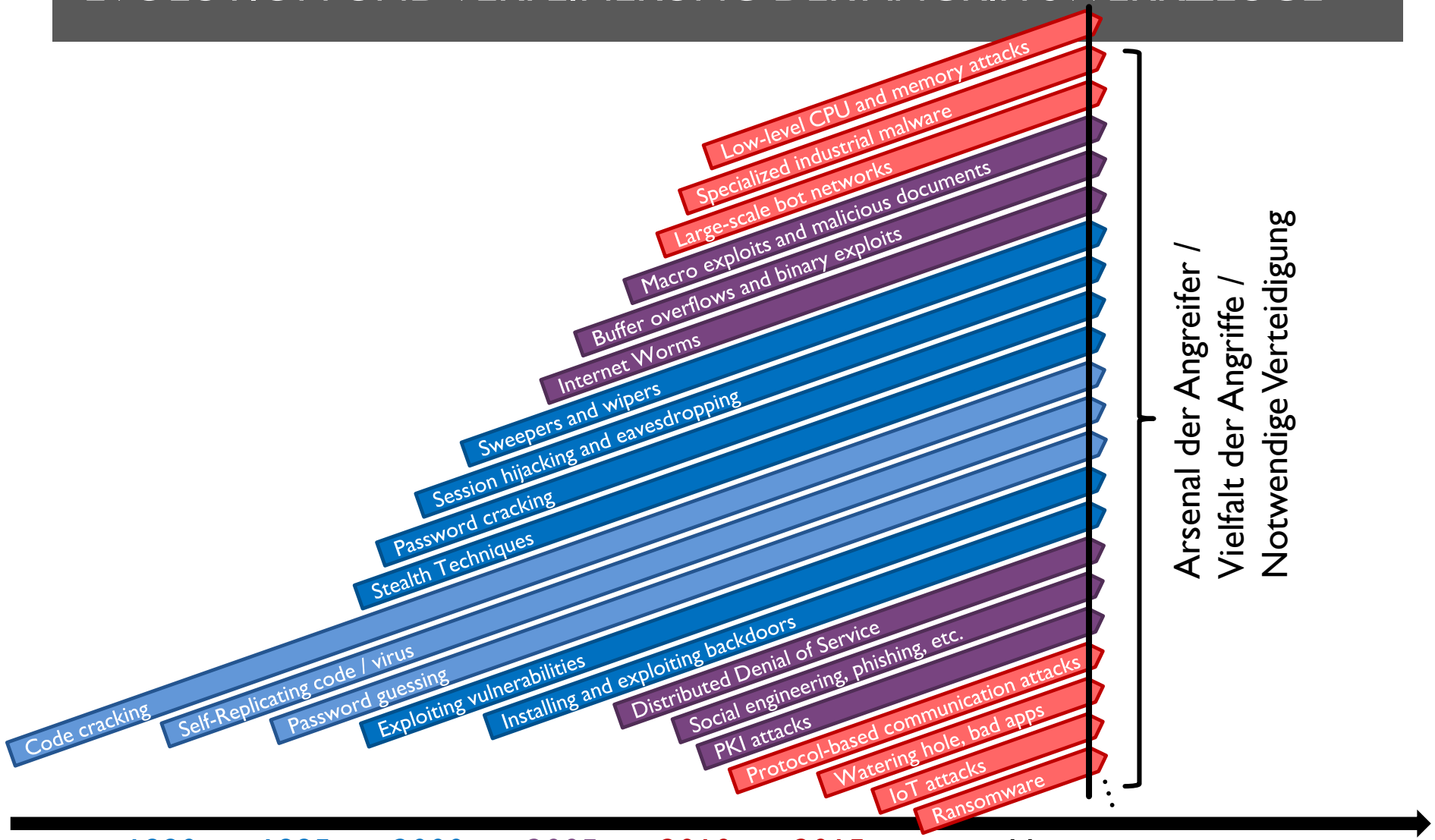
Automatisierungspyramide



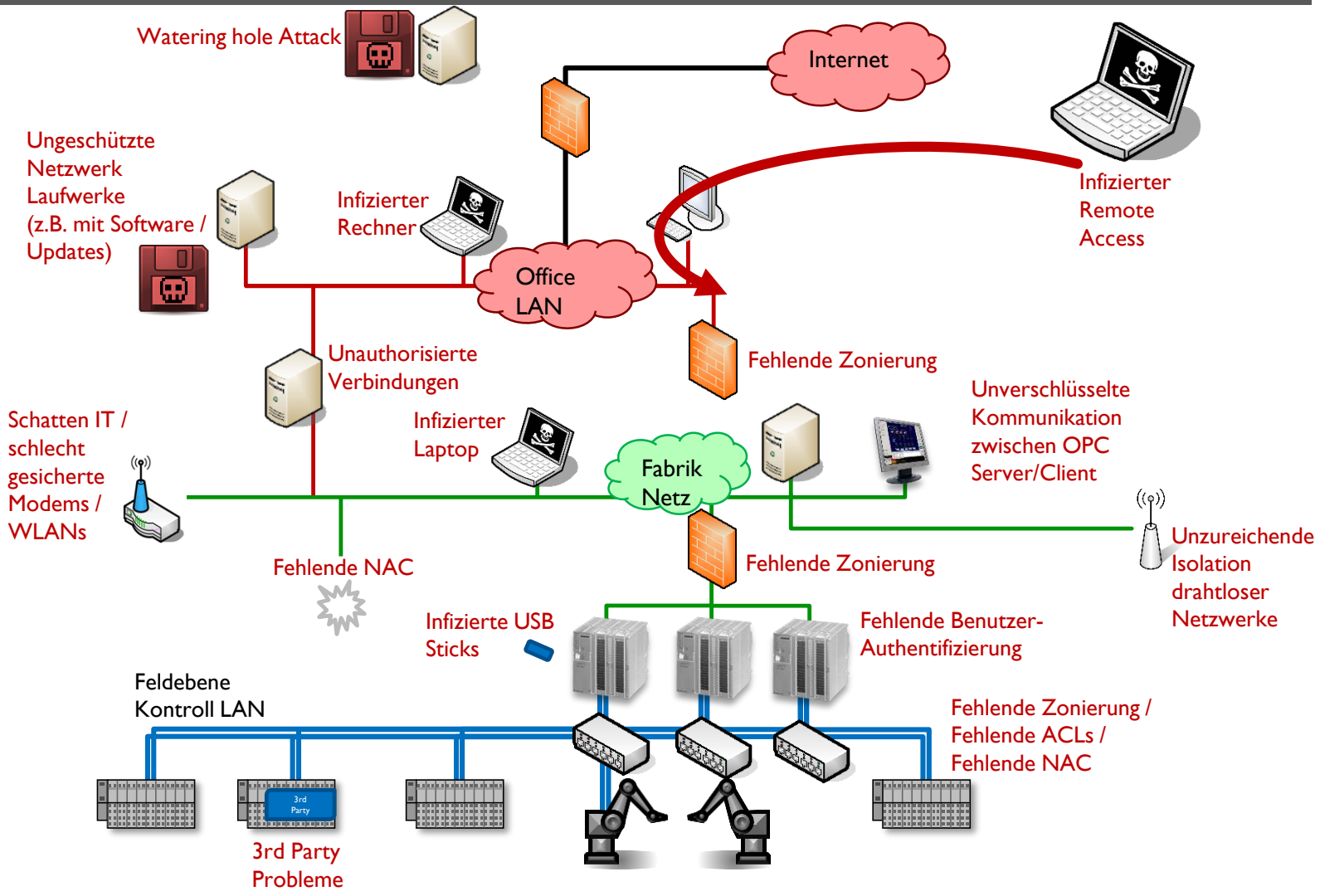
Industrie 4.0 Kommunikation



EVOLUTION UND VERFEINERUNG DER ANGRIFFSWERKZEUGE

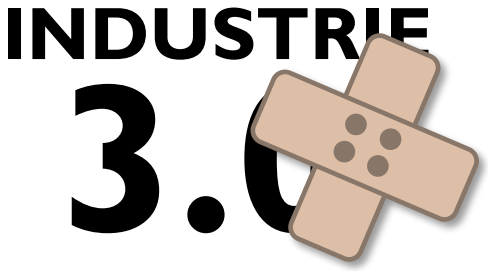


TYPISCHE ANGRIFFSWEGE IN EINER INDUSTRIE-ANLAGE



INDUSTRIE 4.0 SICHERHEIT - WO ANFANGEN?

- Einfache Antwort: Bei Industrie 3.0
  - Verantwortlichkeiten klären
  - Prozesse einführen
  - Aktuelle Systeme absichern
  - „Awareness“ schaffen
  - Gute Basis: ISO/IEC 62443

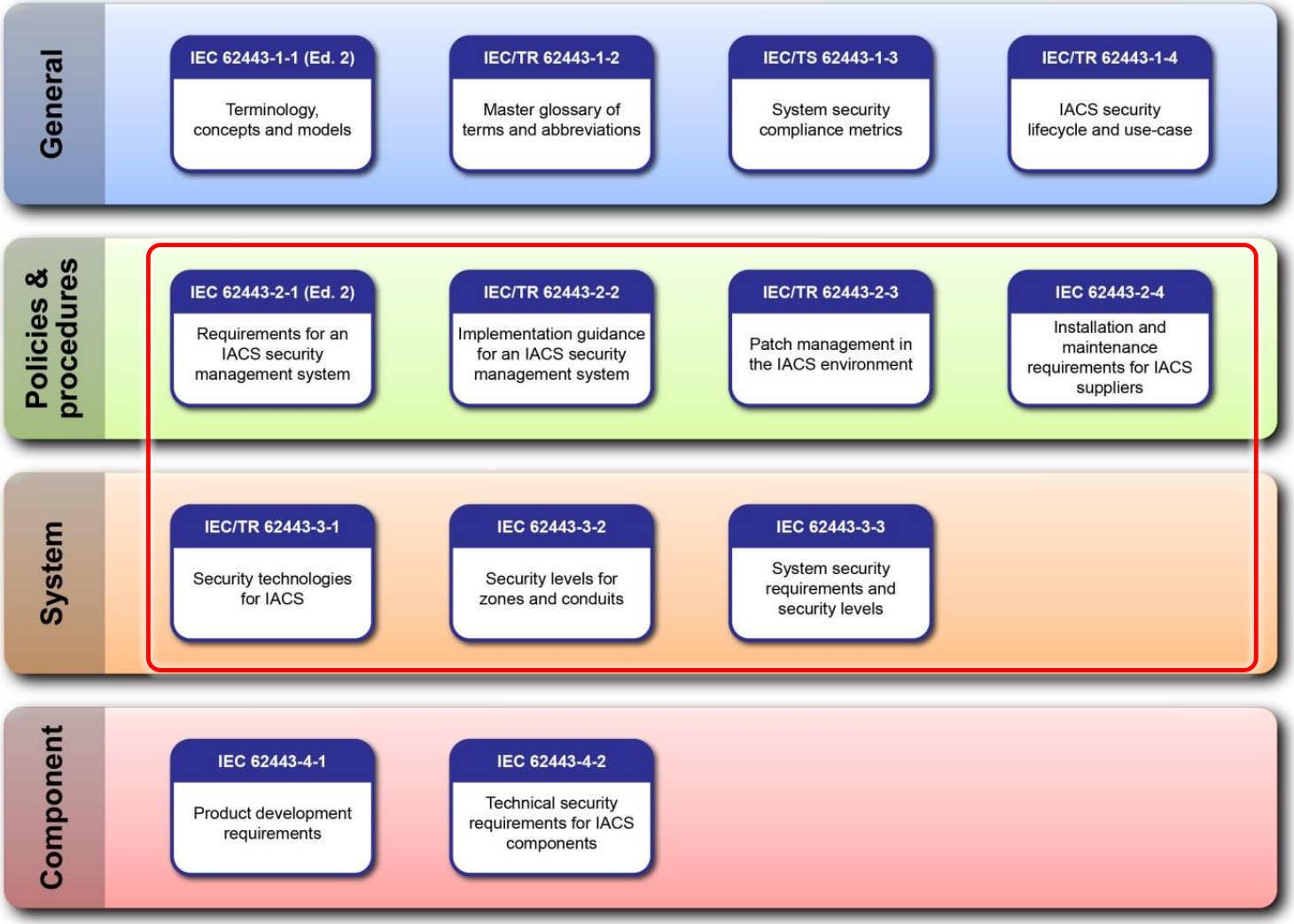


- Vorbereitung auf Industrie 4.0?
  - Aufbau des Security Konzepts prüfen
  - Harte Schale, weicher Kern
    funktioniert
    mit Industrie 4.0 nicht mehr!
  - Sicherheit an allen Punkten

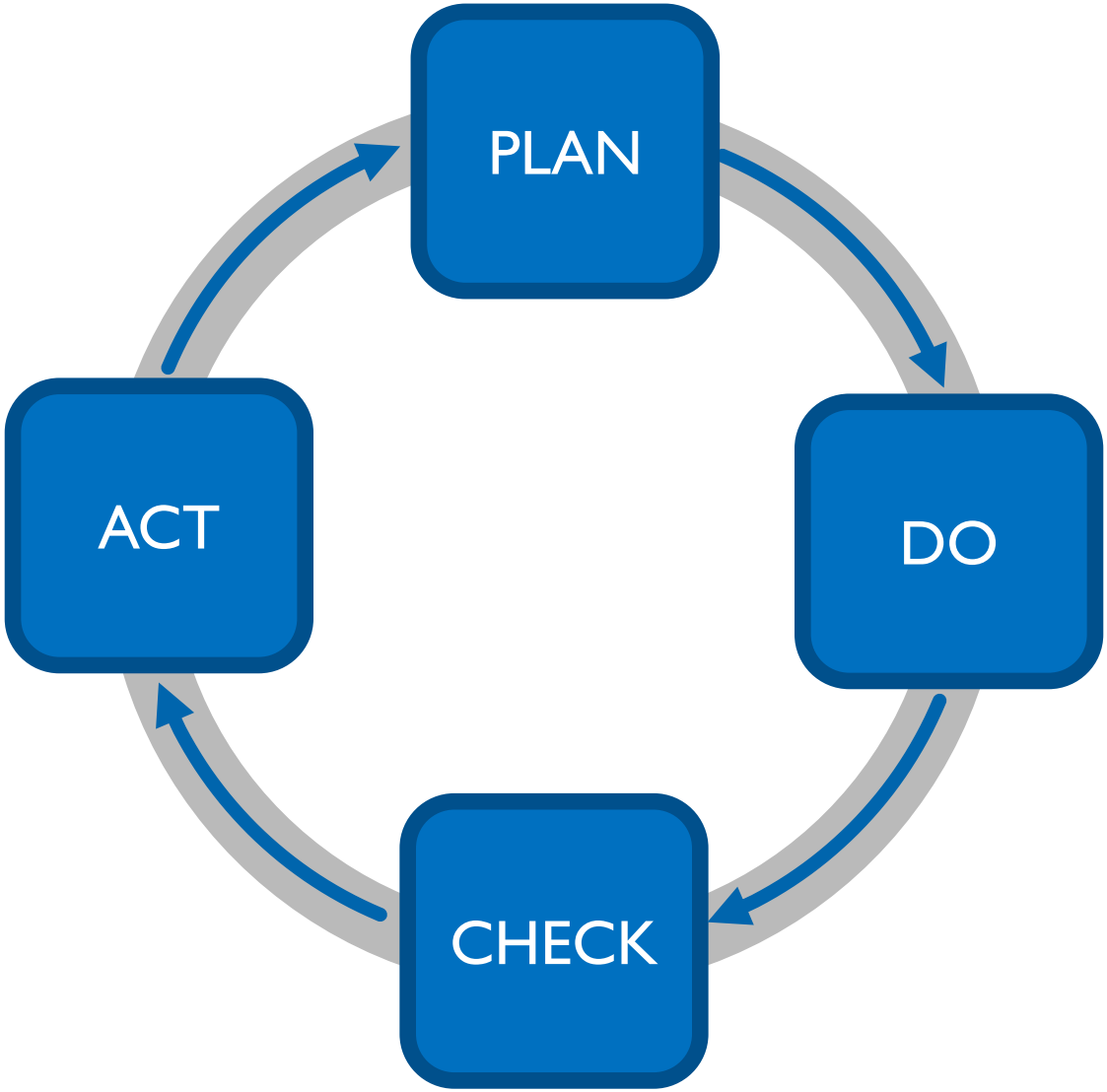
Quelle: Asterix der Gallier

Quelle: Wikimedia

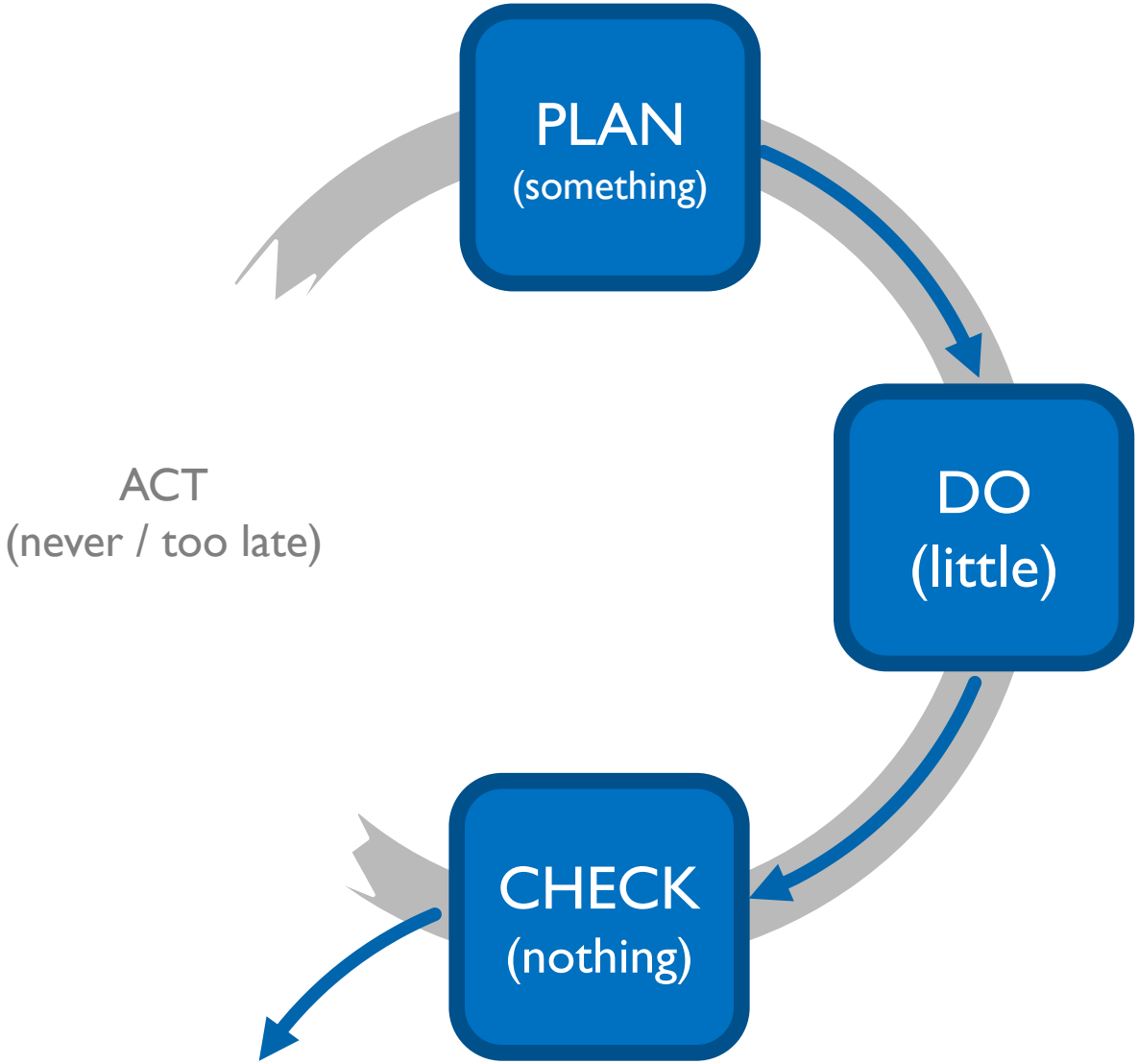
ISO/IEC 62443 SICHERHEITS-NORM FÜR DIE INDUSTRIE



NACHHALTIGE SICHERHEIT PDCA (THEORIE)



NACHHALTIGE SICHERHEIT PDCA (REALITÄT)



WIE MACHT MAN COMPUTER, NETZWERKE UND FIRMEN SICHER?

- Verschiedene Sicherheitsmaßnahmen wirken auf unterschiedliche Art und Weise:
  - Präventiv:
    - Gute Passwörter, aktuelle Software, Anti-Virus, Schulungen, …
  - Detektierend
    - Intrusion Detection System, Systemüberwachung, Kontrolle
  - Reaktiv
    - Incident Response Team, Anti-Virus, Intrusion Prevention System

STUDIENGANG IT SECURITY HS-ALBSIG

- Studieninhalte:
  - IT Sicherheit und Prozesse
  - Netzwerke, Netzwerksicherheit
  - Betriebssysteme, Systemsicherheit
  - Offensive Sicherheit
  - Forensik
  - Kryptografie
- Berufsbilder:
  - Security Analyst
  - IT Security Officer (ISO)
  - Security Engineer (Entwickler)
  - Security - Auditor
  - Penetrationstester
- Projekte
  - HSAS-Honeynet
    - Beobachten realer Angreifer auf Köder-Infrastruktur
  - Produkt Honeynet / Farm
    - Beobachten des Umgangs von Angreifern mit (Kommunikations-) Produkten
  - Sichere Industrienetze mit OPC UA
    - Handhabbare Sicherheit mit OPC UA
    - Testbed mit NAC, Zertifikatsbasiertem Zugriff, nachhaltiger Sicherheitspflege

Hochschule
Albstadt-Sigmaringen
Albstadt-Sigmaringen University

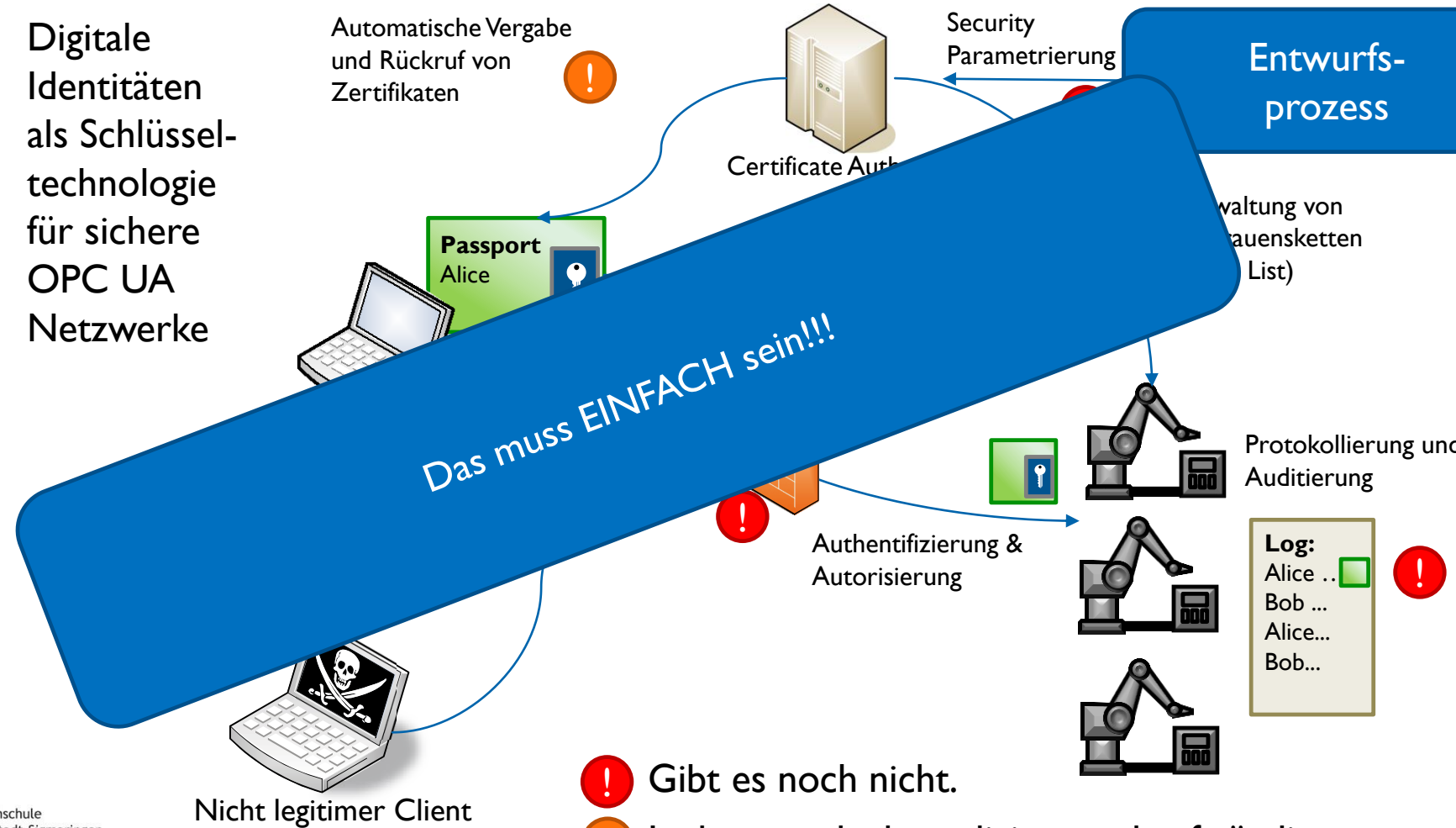
ZUSAMMENFASSEND: DIE SACHE MIT DER IT SICHERHEIT

- IT Security ist ein Katz- und Maus- Spiel zwischen Angreifern und Verteidigern
  - Neue Angriffe → Neue Verteidigung → Neue Angriffe
- Die Ausgangslage ist nicht besonders günstig
  - Industrienetze werden jahrzehntelang gereiften Bedrohungen ausgesetzt
  - Solide Sicherheit ist dringend nötig.
- Es gibt keine Wunderwaffen in der IT Sicherheit
  - Mitdenken ist gefragt!

Was ist das Allerwichtigste wenn man sein Rad vor Diebstahl schützen will?

EFFEKTIVER UND EFFIZIENTER EINSATZ VON DIGITALEN IDENTITÄTEN

- Digitale Identitäten als Schlüssel-technologie für sichere OPC UA Netzwerke



Gibt es noch nicht.

Ist heute sehr kompliziert und aufwändig.