Digitalisierung und Sicherheit

VDI Bezirksverein Berlin-Brandenburg

Dipl.-Ing. (TU) Carsten J. Pinnow,
9. Netzwerktreffen des VDI Arbeitskreises Kunststofftechnik
am 31.03.2017

Industrie 4.0

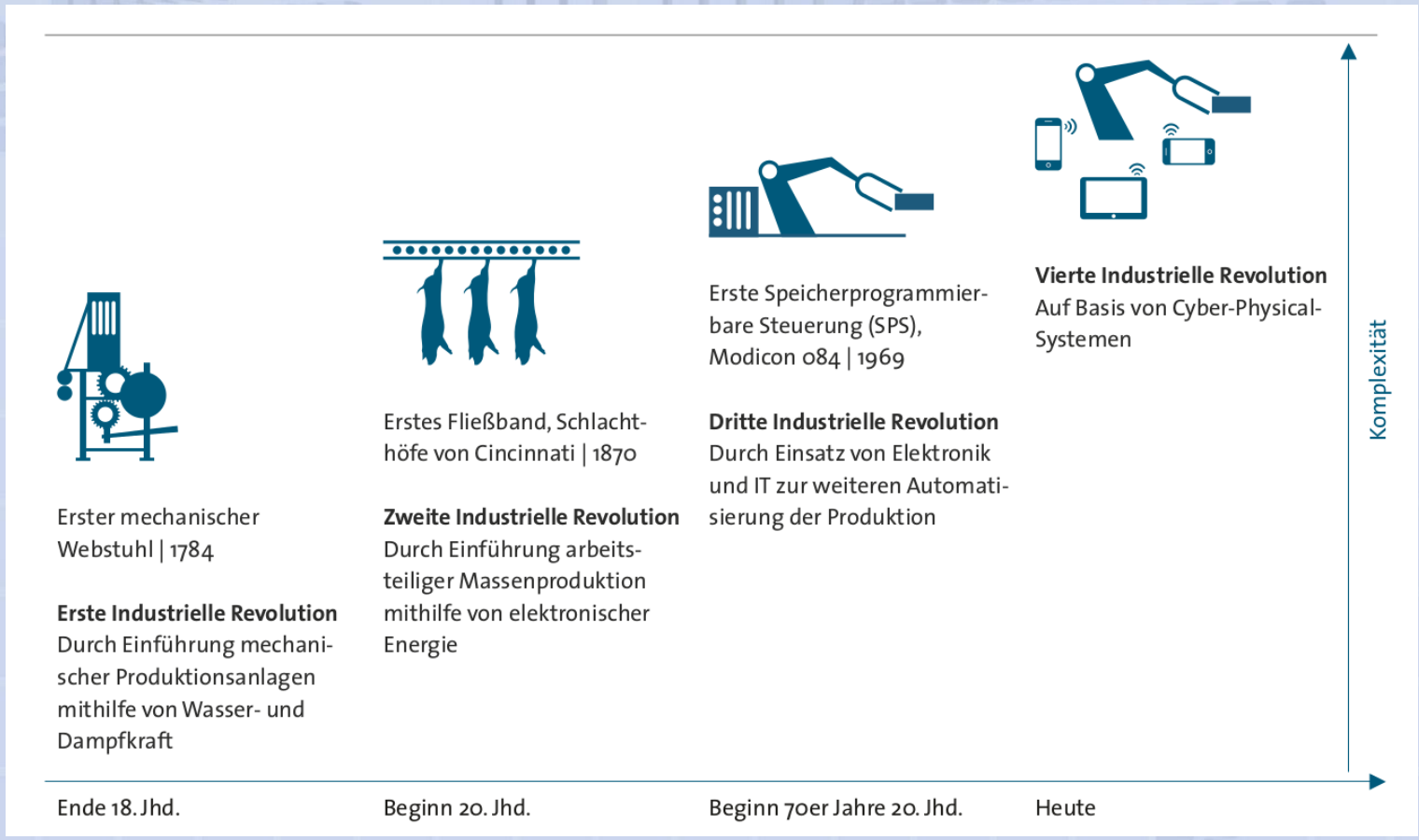


Bild: acatecht

Industrie 4.0 - Definition

- Industrie 4.0 bezeichnet die sogenannte vierte Industrielle Revolution, nach der Mechanisierung, Elektrifizierung und Informatisierung der Industrie.
- Intelligente Vernetzung von Produkten und Prozessen
- Cyber-Physical-Systems (CPS) werden weltweit vernetzt
- Durchgehende Digitalisierung der gesamten Wertschöpfungskette
- Entstehung von „Smart Factories“

Chancen

Versprochene Potenziale sind immens

- Rentable Produktion von Einzelstücken
- Ressourcen- und Energieeffizienz
- Resilienz von Betrieben
- Flexibilität (z.B. Ausfall von Zulieferern)
- Steigerung der Wertschöpfung
- Chancen gerade auch für KMU

Sicherheit als Gesamtsystem

In Sicherheitskonzepten müssen ganzheitlich

- Mensch
- Technik und
- Organisation

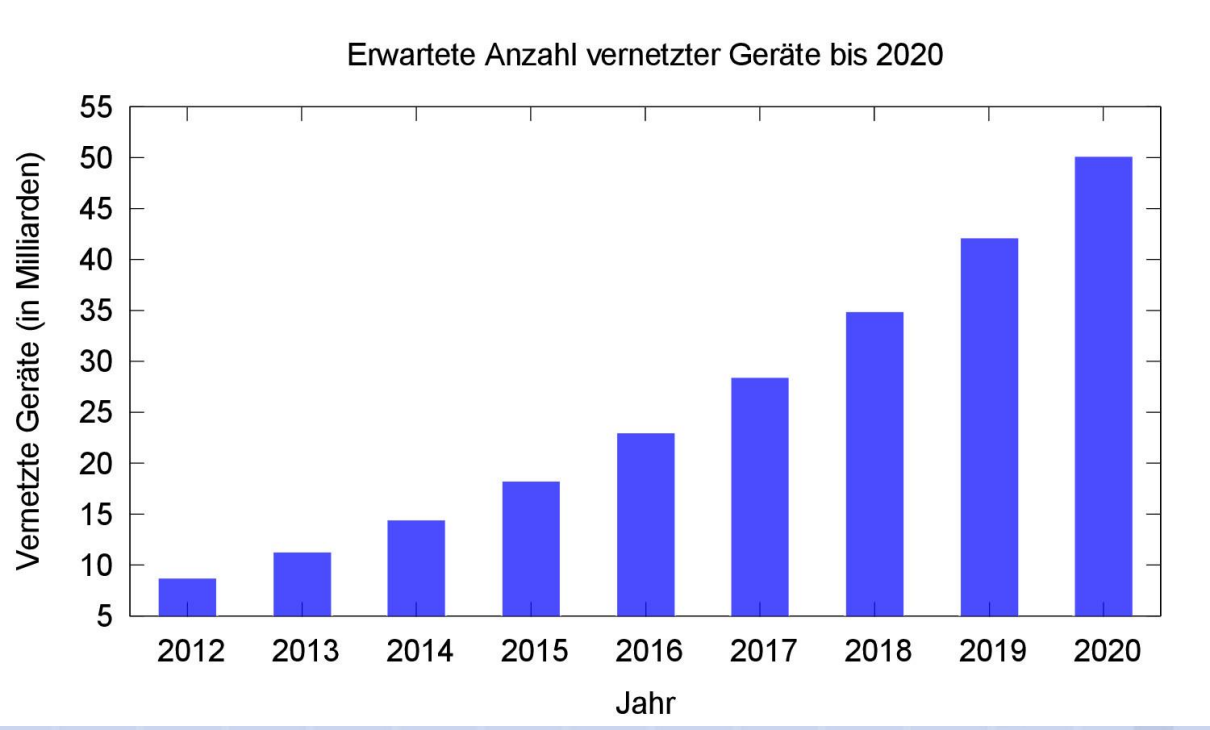
berücksichtigt werden

Begriff „Sicherheit“

Mit Sicherheit sind mehrere Aspekte gemeint:

- Safety
- Security

Risiken durch zunehmende Vernetzung



Zahlen: Cisco

Herausforderungen durch Industrie 4.0

Herausforderungen für Unternehmen sind:

- Lange Lebensdauer von Industrieanlagen
- Konvergenz von Automatisierungsinfrastruktur (Shop-Floor-IT) und der klassischen Unternehmensnetze (Office-IT)

Angriffe auf Industrieanlagen

- Reale Bedrohung
- Schadsoftware (Stuxnet, Flame. Duqu)
- Beispiele:
  - Schädigung eines Stahlwerkes in Deutschland (2014),
  - Attacke auf den saudischen Ölkonzern Saudi Aramco (2012)

Cyberangriffe auf Behörden etc.

- Tesla X3-Cryptovirus befiel im Februar 2016 u.a. Rechner des Rathauses in Rheine
- Kryptotrojaner Locky infiziert zehntausende PC und unter anderem ein Fraunhofer-Institut in Bayreuth
- IT-Schädlinge in Krankenhäusern in Nordrhein-Westfalen (2016)
- Rekord-DDoS-Attacke mit 1,1 Terabit pro Sekunde gesichtet (September 2016)

Anzahl der Cyberattacken steigt

- initiiert durch unterschiedliche Interessensgruppen (Konkurrenz, Staat, Militär, Organisierte Kriminalität)
- kein eigenes Know-how notwendig
- Werkzeuge sind weitgehend frei verfügbar
- CaaS (Cyberattacken as a Service)

Basisforderungen für Datensicherheit:

Gefordert sind im Betriebsalltag Funktionalität und hohe Qualität aller Komponenten, d.h. konkret

- Verfügbarkeit,
- Vertraulichkeit,
- Integrität

von

- Hardware,
- Software,
- Orgware

Basisforderungen für Datensicherheit:

und im Schadensfall Stabilität, also

- Schadenminimierung und
- schneller Wiederanlauf.

Mögliche Bedrohungsszenarien

- Verlust eines Tablet-PCs, Verlust von Speichermedien
- kein Backup
- Ausfall des Administrators
- Hackerangriff aus dem Internet
- „IT?“ → InnenTäter! (Motivations- / Bildungsmangel oder Kriminalität)
- Befall durch Schadprogramme (Viren, Trojaner, Würmer...)
- Arbeiten in der „Cloud“
- Mitarbeiter scheidet aus / wechselt die Abteilung

Häufige Versäumnisse (1)

- (Daten-)Sicherheit hat einen zu geringen Stellenwert.
- Dauerhafte Prozesse zur Beibehaltung des Sicherheitsniveaus fehlen.
- Sicherheitsvorgaben sind nicht dokumentiert.
- Kontrollmechanismen und Aufklärung im Fall von Verstößen fehlen.
- Die Rechtevergabe wird nicht restriktiv genug gehandhabt.
- IT-Systeme sind schlecht konfiguriert.
- Sensitive Systeme sind gegen offene Netze unzureichend abgeschottet (z.B. Fernwartung).

Häufige Versäumnisse (2)

- Sicherheitsmaßnahmen werden aus Bequemlichkeit vernachlässigt.
- Anwender und Administratoren sind mangelhaft geschult.
- Verfügbare Sicherheits-Updates werden nicht eingespielt.
- Mit Passwörtern wird zu sorglos umgegangen.
- **Erprobte** Not- und Wiederanlaufpläne fehlen

Sicherheitsanforderungen ändern sich

- „Cloud Computing“ → Datenverbleib
- „Bring Your Own Device“ (BYOD) → mehr mobile Geräte
- intensivere Nutzung von elektronischen Medien → Malware-Befall
- Kriminelle professionalisieren sich → Schwarzer Markt für Daten
- geänderte gesetzliche Rahmenbedingungen → Haftung für Entscheider
- Digitalisierung und Vernetzung nehmen zu
- Systeme werden „zweckenfremdet“

Herausforderungen

- Sicherheit wird für die Industrie 4.0 unterschätzt
- Industrie 4.0 vs. Sicherheit 0.1
- Neue Konzepte sind notwendig (Firewalls, Angriffserkennung, Identitätsmanagement und Antivirenscanner werden nicht helfen)
- ISO 27034: „Security by Design“ wird kaum beachtet
- Verteidiger können immer nur reagieren
- Namur NE153 ist eine besondere Herausforderung für Anlagenbauer und Hersteller von Industriesteuerungen

Verweigerung ist keine Option...

Gegen den Tonfilm! **Für lebende Künstler!**

An das Publikum!

Achtung! **Gefahren des Tonfilms!**

Viele Kinos müssen wegen Einführung des Tonfilms und Mangel an vielseitigen Programmen schließen!

Tonfilm ist Kitsch!

Wer Kunst und Künstler liebt, lehnt den Tonfilm ab!

Tonfilm ist Einseitigkeit!

100% Tonfilm = 100% Verflachung!

Tonfilm ist wirtschaftlicher und geistiger Mord!

Seine Konservenbüchsen-Apparatur klingt kellerhaft, quietscht, verdirbt das Gehör und ruiniert die Existenzen der Musiker und Artisten!

Tonfilm ist schlecht konserviertes Theater bei erhöhten Preisen!

Darum:

Fordert gute stumme Filme!
Fordert Orchesterbegleitung durch Musiker!
Fordert Bühnenschau mit Artisten!

Lehnt den Tonfilm ab!

Wo kein Kino mit Musikern oder Bühnenschau: Besucht die Varietés!

Internationale Artisten-Loge E. V.
Fossil

Deutscher Musiker-Verband.
Karl Schlementz

Druck: Gebr. Unger, Berlin SW 11.

Flugblatt um 1929

Bild: stummfilm.info

Sicherheit als erfolgskritischer Qualitätsfaktor

Gefragt sind:

- Politik
- Gesellschaft (Verbände, Vereine, Initiativen)
- Individuen

Voraussetzungen zur Nutzung von Chancen

- Standardisierungen und Referenzarchitekturen
- Grundlagenforschung und angewandte Forschung
- Rechtliche Rahmenbedingungen
- Ausbildung, Weiterbildung (frühzeitig)
- Beherrschung komplexer Systeme (Komplexität verringern)
- Infrastruktur (Breitbandnetze, Straßen etc.)
- Verbindliche und verständliche Regeln
- Prinzipien: Bezahlbare Sicherheit, „Security by Design“
- Entkopplung von Netzen / getrennte Netze

Allgemeine Empfehlungen

- Thema zur Chefsache machen
- „Digitalisierungsbeauftragen“ bestimmen
- Praktischen Umgang mit Sicherheitskomponenten einüben
- Awareness- / Bildungsprogramm

Vorgehensweise

- Informieren / Sensibilisieren
- Entscheiden
- Handeln

Schutzmaßnahmen (Mensch)

- Sensibilisierungskampagnen
- Mitarbeiterschulung
- Informieren über freie Quellen (VDE, VDI, BSI, DsiN, bitkom, SIBB, …)
- Veranstaltungen zur Fortbildung nutzen

Schutzmaßnahmen (Technik)

- Grundschutz (Virenscanner, Firewall, …)
- Rechteverwaltung
- Starke Passwörter
- Physische Sicherheit
- Vorsicht bei E-Mail-Anhängen und externen Datenträgern
- Datensicherung inkl. Test
- Verschlüsseln externer Datenträger

Schutzmaßnahmen (Organisation) I

- Zugänge zu IT-Systemen überwachen (extern, intern)
- Intern über denkbare Sicherheitsvorfälle spechen
- Szenarien und Lösungen dokumentieren
- Unternehmensdaten klassifizieren („digitale Kronjuwelen“ identifizieren)
- Verschlüsselungsszenarien (extern, intern)
- Private Nutzung der betrieblichen IT klar regeln

Schutzmaßnahmen (Organisation) II

- Überblick über die Systeme behalten
- Anbindungen an IT-Systeme genehmigen und dokumentieren
- Nutzung mobiler Endgeräte regeln
- Not- und Wiederanlaufplan erstellen und regelmäßig testen (Krisenstab)

Kontakt:

Dipl.-Ing. Carsten J. Pinnow

PINNOW & Partner GmbH
Helmholtzstraße 2-9. Aufgang D, 4. OG
D - 10587 Berlin

Tel.: 030 / 39 74 86 21-0
Mobil: 0179 / 29 08 551

E-Mail: carsten@pinnow.com
WWW: http://www.datensicherheit.de