Cyber-physische Risiken in der chemischen Industrie

Matthias A. Eckhart

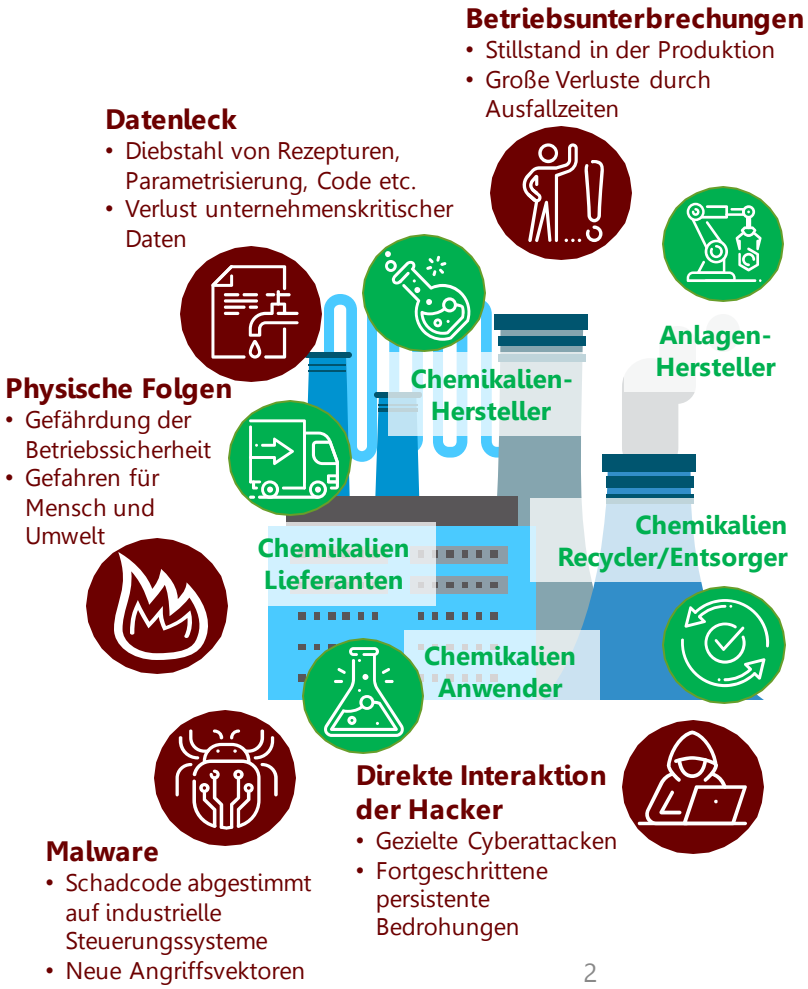
Vernetzungsveranstaltung: Advanced Digital Technologies für nachhaltige Geschäftsmodelle in der Chemiewirtschaft

8. September 2022

OT Security

OT: Operational Technology

- Cyberattacken gegen industrielle Steuerungssysteme können **physische Schäden** hervorrufen und damit die **Betriebssicherheit** gefährden
- **Angriffsfläche** wird durch den Einsatz von Advanced Digital Technologies **massiv erhöht**
- **Bedrohungslandschaft** verändert sich ständig
- **Beispiel:** Sicherheitsvorfall in der chemischen Industrie
  - Angriff auf Wasseraufbereitungsanlage („Kemuri Water Company", berichtet von Verizon im Jahr 2016)
  - Eingesetzte Altsysteme sind ein attraktives Angriffsziel
  - Manipulation der Wasserbehandlungsprozesse: potenzielle **chemische Verunreinigung** durch synthetische Substanzen
  - Angriff konnte durch Warnsystem noch rechtzeitig gestoppt werden
  - Angriff wurde vermutlich von einer Hacktivist-Gruppe mit syrischen Verbindungen ausgeführt



IT & OT im Vergleich

IT		OT
Unternehmensnetzwerk		Industrielles Netzwerk
Daten	**Asset**	Prozess
Vertraulichkeit Integrität Verfügbarkeit		**Verfügbarkeit** Integrität Vertraulichkeit
Keine Safety Auswirkungen	**Risikofolge**	Physischer Schaden
3-7 Jahre	**Lifecycle**	15-30 Jahre
Wöchentlich	**Patchzyklus**	> Jährlich
> 5 ms	**Reaktionszeit**	~ 1 µs-10 ms
Basis vorhanden	**Sec. Awareness**	Security? Safety!

Mit Sicherheit in die vierte industrielle Revolution

Neue Technologien eröffnen neue Angriffswege

Robotik
- Vergrößerte Angriffsfläche durch mehr Funktionalität
- Hohe Komplexität erschwert Absicherung
- Abhängigkeit zu einigen wenigen Herstellern

Big Data & Cloud
- Risiken durch Angriffe auf Cloud-Dienste
- Kontrollverlust über Daten
- Abhängigkeit zu Cloud-Anbieter

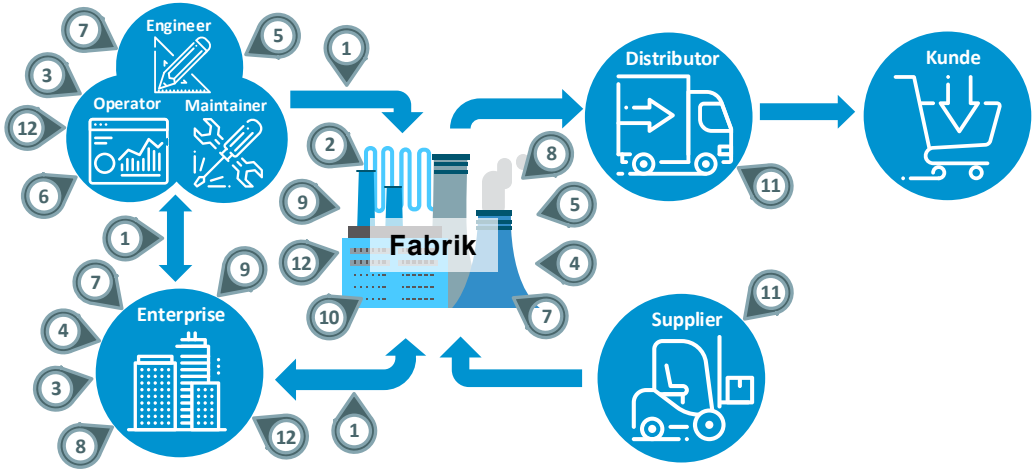
Konnektivität & IoT
- Vergrößerte Angriffsfläche
- IoT-Geräte: Beliebte Angriffsziele
- Altsysteme werden internetfähig

Künstliche Intelligenz
- Backdoors in Trainingsdaten
- Diebstahl der ML Modelle
- Rückgewinnung der Trainingsdaten

Simulation
- Diebstahl wertvoller Modelle
- Missbrauch zur Malware-Entwicklung
- Gezielte Verfälschung der Ergebnisse

Additive Fertigung
- Sabotage der Design-Artefakte
- Diebstahl der Spezifikationen
- Angriffe auf die Supply Chain

12 Aspekte der sicheren Produktion



Zugriffsschutz	1	5	Sicherheitstests	9	Patching & Backup
Physischer Schutz	2	6	Sicherheitstraining	10	Malware Schutz
Sichere Entwicklung	3	7	Datensicherheit	11	Sichere Supply Chain
Segmentierung	4	8	Risikomanagement	12	Schutz mobiler Geräte

Der digitale Zwilling

Die Anfänge

"A digital twin is an integrated […] simulation of a […] system that uses the best available ***physical models, sensor updates,*** *[…] etc., to* ***mirror*** *the life of its […] flying twin."* (Shafto et al., 2010)

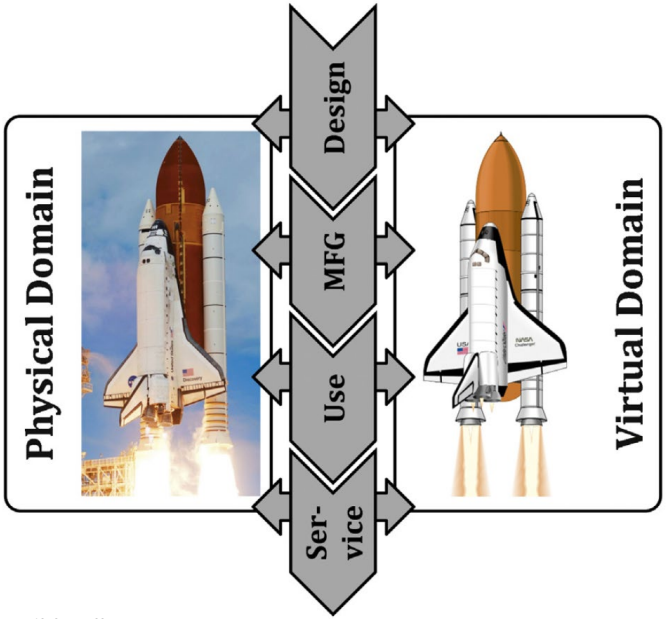
M. Shafto et al., "Draft modeling, simulation, information technology & processing roadmap," Technology Area, vol. 11, 2010.

Ursprung

Das Konzept hat ihren Ursprung in der Raumfahrtindustrie (NASA).

Zweck

Digitale Zwillinge wurden zur Unterstützung bei Zertifizierungen und Missionen entwickelt.



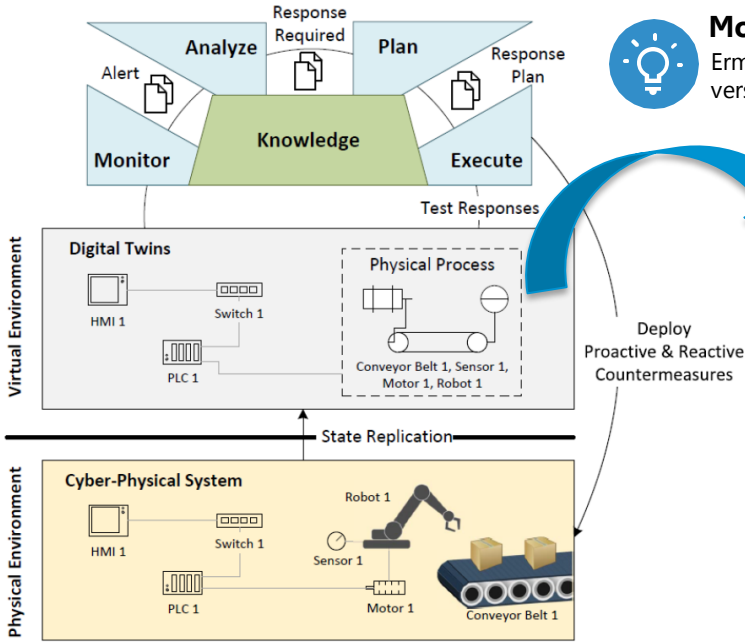
Bildquelle:

B. Schleich, N. Anwer, L. Mathieu, and S. Wartzack, "Shaping the digital twin for design and production engineering," CIRP Annals, vol. 66, no. 1, pp. 141–144, 2017, issn: 0007-8506.

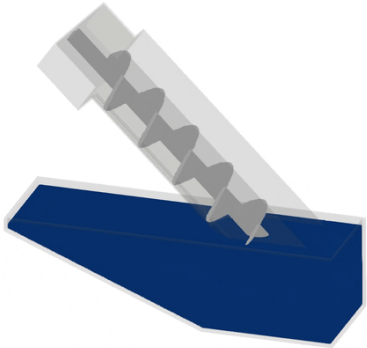
Der digitale Zwilling

Im Kontext von IT/OT Security

1. **System-Emulator inkl. I/O Simulation**
2. **Netzwerk-Emulator**
3. **Simulation des physikalischen Prozesses**
4. **Synchronisation mit realem System**



Modulare Architektur
Ermöglicht Integration verschiedener Simulationsmodelle



Simulation entwickelt von enrag

Bildquelle:

M. Eckhart, A. Ekelhart, and R. Eisl, "Digital twins for cyber-physical threat detection and response," ERCIM News, vol. 2021, no. 127, 2021.

Matthias A. Eckhart

SBA Research

Floragasse 7, 1040 Wien

+43 664 448 34 35

meckhart@sba-research.org

Bundesministerium Klimaschutz, Umwelt, Energie, Mobilität, Innovation und Technologie

Bundesministerium Digitalisierung und Wirtschaftsstandort

FFG Forschung wirkt.

wirtschafts agentur wien Ein Fonds der Stadt Wien

European Commission

FWF Der Wissenschaftsfonds.

netidee OPEN INNOVATIONS