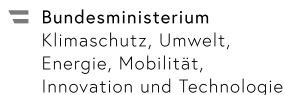




Mit dem digitalen Zwilling zur sicheren Produktion

Matthias Eckhart (SBA Research & Universität Wien)

30.05.2022, Summit Industrie 4.0 Österreich



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

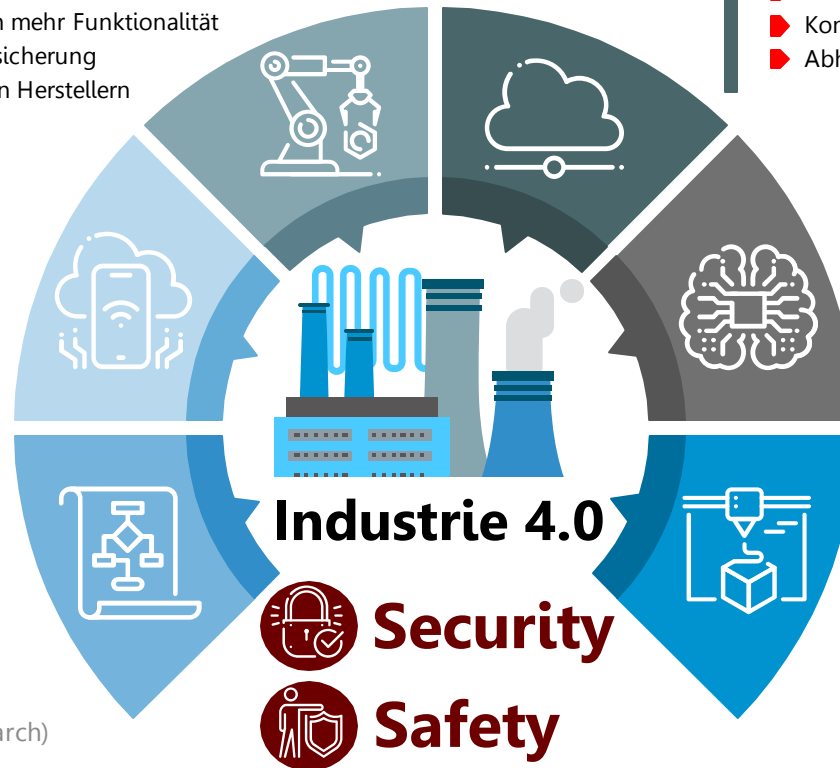
- ▶ Backdoors in Trainingsdaten
- ▶ Diebstahl der ML Modelle
- ▶ Rückgewinnung der Trainingsdaten

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



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.



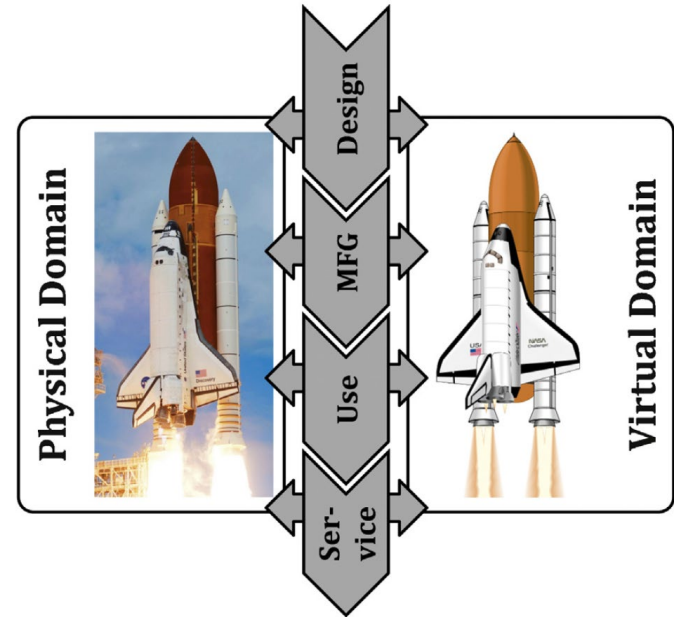
Ursprung

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



Zweck

Digitale Zwillinge wurden zur Unterstützung bei Zertifizierungen und Missionen entwickelt.







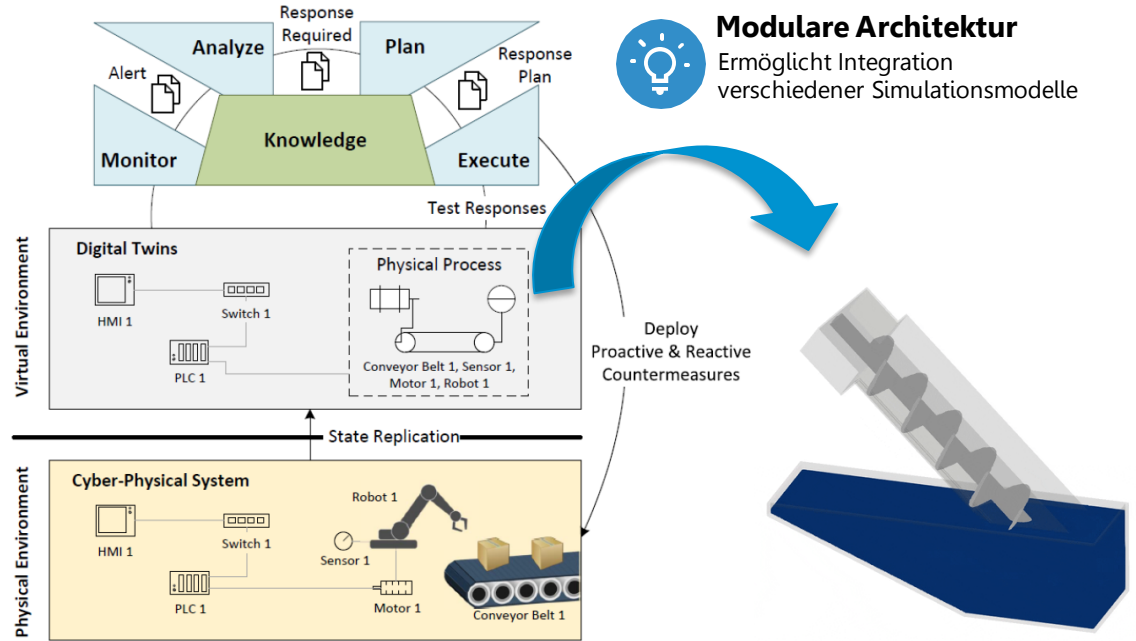
Bildquelle:

B. Scheich, 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

Bildquelle:

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

Simulation
entwickelt von 

Aufbau und Anwendungen des Frameworks

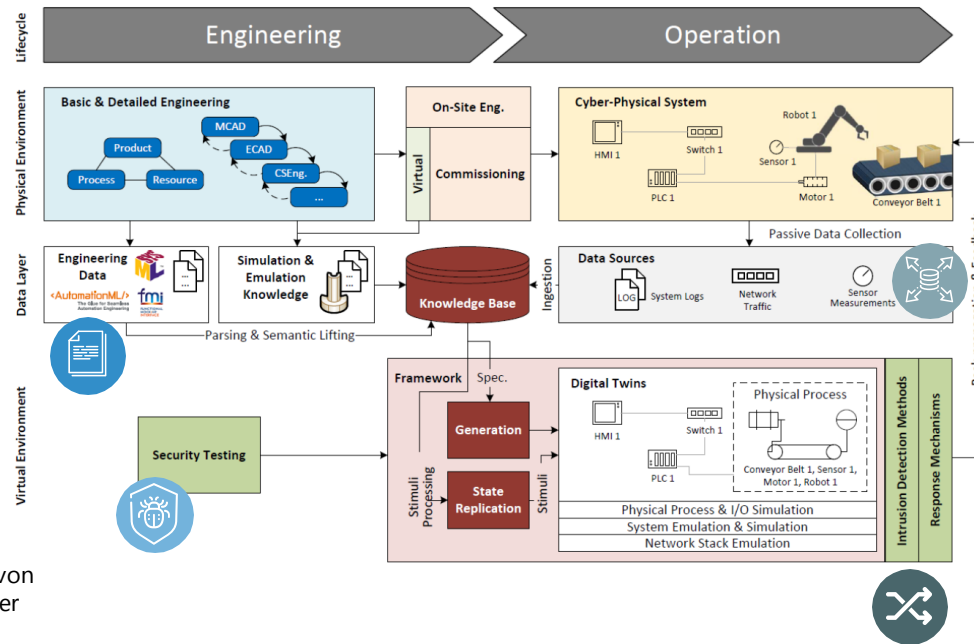
In der Engineering- und Betriebsphase

Engineering Artefakte

Integration bestehender Engineering-Daten zur Erzeugung digitaler Zwillinge.

Security by Design

Überprüfung der Sicherheit von Systemen bereits während der Entwicklungsphase.



Synchronisation

Digitale Zwillinge spiegeln das Verhalten der realen Systeme zeitversetzt wider.

Angriffserkennung

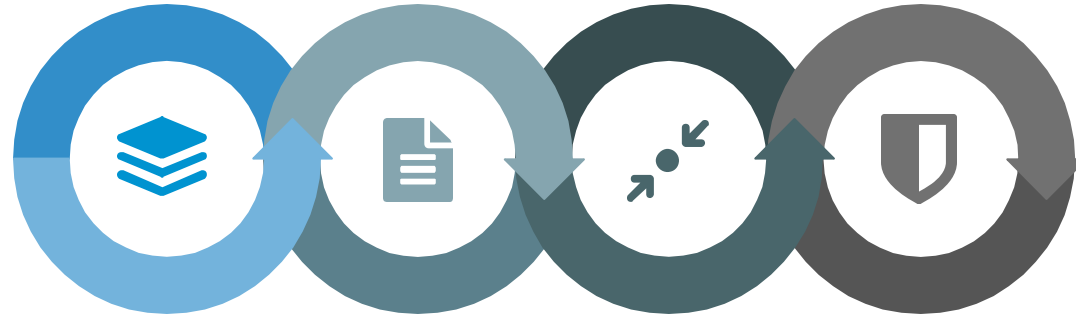
Abweichungen im Verhalten des digitalen Zwillinges deuten potenziell auf einen Angriff oder Fehler hin.

Zusammenfassung und Ausblick

Mit dem digitalen Zwilling zur sicheren Produktion



**Digitaler Zwilling
auch als Angriffsziel
denkbar**



Kernkomponenten

Verbund aus: Emulation der Systeme, des Netzwerk-Stacks und Simulation des physikalischen Prozesses.



Engineering-Artefakte

Bestehende Engineering-Daten und Simulationsmodelle werden genutzt, um digitale Zwillinge zu erzeugen.



Synchronisation

Digitale Zwillinge sollen das Verhalten ihrer physischen Gegenstücke widerspiegeln. Dies erfordert Synchronisationsmechanismen.



Anwendungen

Digitale Zwillinge können zur Angriffserkennung genutzt werden und ermöglichen das Testen potenzieller Gegenmaßnahmen.


Matthias 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



wirtschafts
agentur
wien
Ein Fonds der
Stadt Wien



FWF
Der Wissenschaftsfonds.

 netidee
OPEN INNOVATIONS