Cybersecurity im digitalen Zeitalter der Bauindustrie

DI Elisabeth Gütl
Institut für Baubetrieb und Bauwirtschaft, TU Graz

Die Arbeitsproduktivität im Architektur-, Ingenieur- und Bausektor (AEC) ist rückläufig, während sie sich im gleichen Zeitraum in anderen Branchen fast verdoppelt hat.*

*Referenz: Oesterreich, Thuy & Teuteberg, Frank. (2016). Understanding the implications of digitisation and automation in the context of Industry 4.0: A triangulation approach and elements of a research agenda for the construction industry.

Gründe des geringen Digitalisierungsgrads:

- Traditionelle Branche
- Komplexität der Projekte
- Hoch fragmentierte Lieferkette (viele verschiedene Lieferanten und Zulieferer)

Stand der Forschung Cybersecurity im Bauwesen

Anwendung CVSS für die Vulnerabilitätsbewertung

Vergleich existierender Cybersecurity Frameworks

Blockchain für BIM Common Data Environments (CDE)

Cybersecurity Management Framework für Cloud-Based BIM

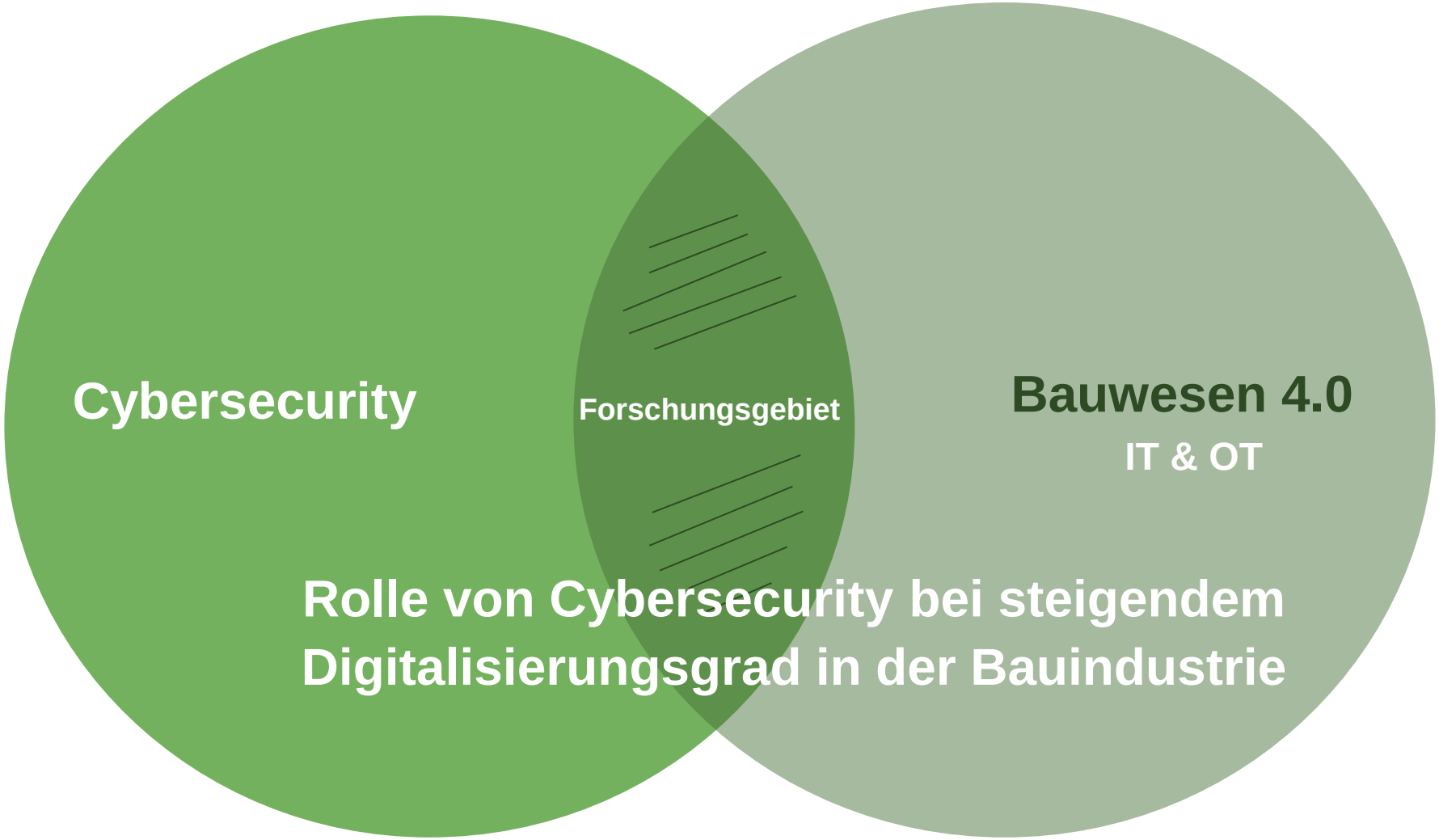
Systematische Literaturrecherche

Bedrohungsmodellierung am Beispiel “3D Concrete Printing System”

Herausforderungen für Cybersecurity im Bauwesen

- Vielfalt an Geräten und Systemen
- Fluktuierende Zugriffsrechte
- Zunehmende Vernetzung von Informationstechnologie (IT) und operative Technologie (OT)
- Datenaustausch mit externen Partnern

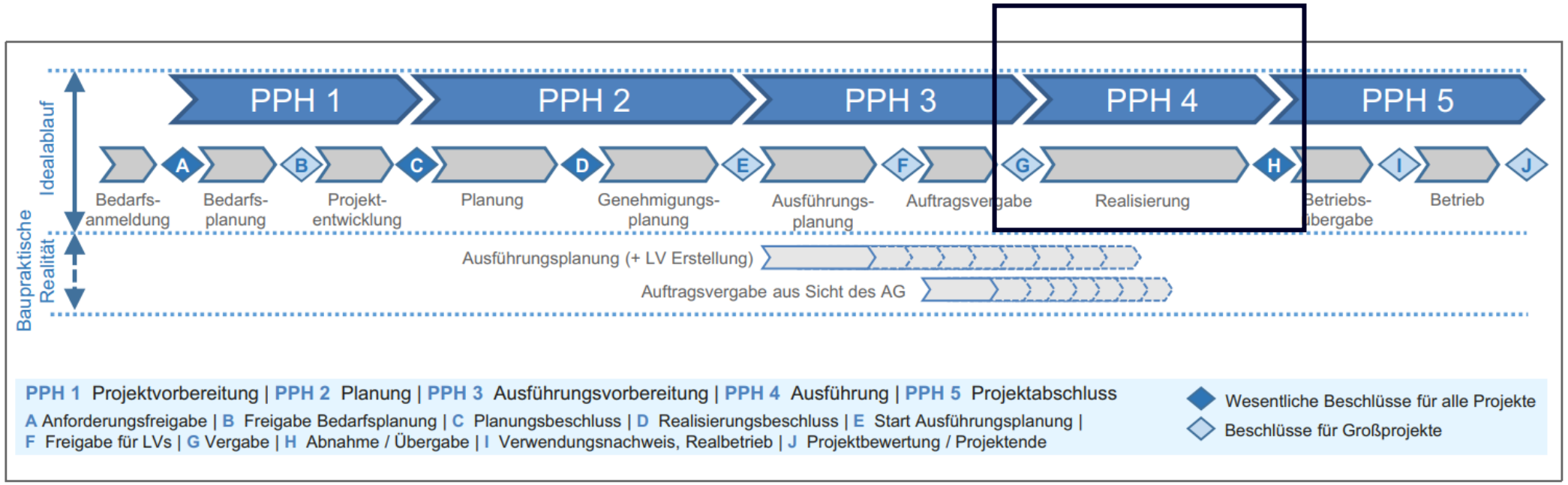
Forschungsgebiet



Vergangene Cyberattacken im Bauwesen

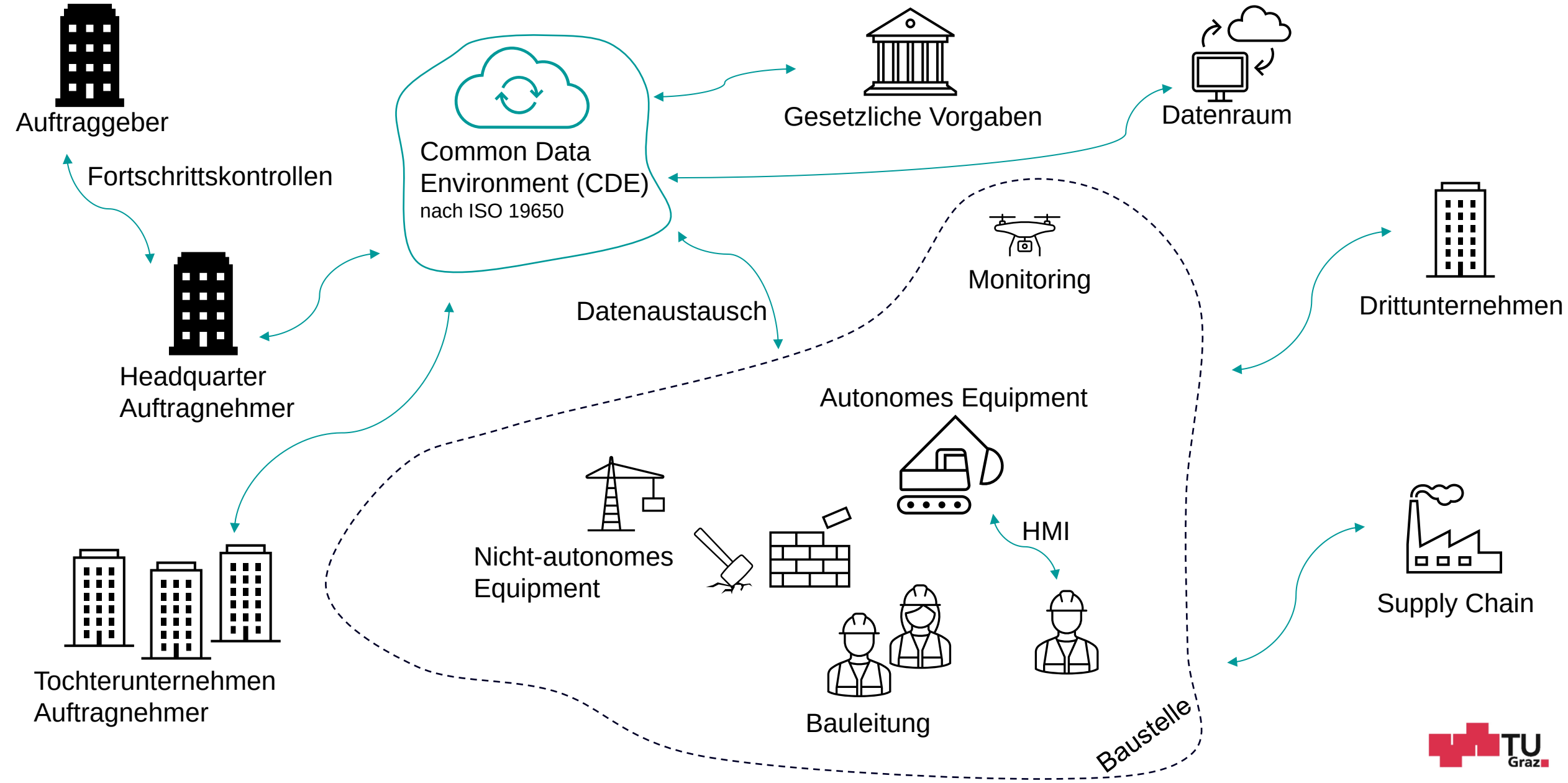
Jahr	Unternehmen	Land	Art des Angriffs	Auswirkungen
2022	Vinci SA	Frankreich	Social Engineering	Fall des Aktienkurses
2020	Bouygues Construction	Frankreich	Ransomware	Diebstahl von 200 GB Daten, Forderung von 10 Mio. Dollar Lösegeld, Abschaltung des Unternehmensnetzwerks
2020	BAM Construct	Großbritannien	Ransomware	Teilabschaltung des Unternehmensnetzwerks
2020	Interserve	Großbritannien	Phishing	Diebstahl von personenbezogenen Daten
2020	Hoffmann Construction	USA	Datendiebstahl	Namen, Adressen, Geburtsdaten, Sozialversicherungsnummern und Informationen zu Sozialleistungen von Mitarbeitern
2019	Bird Construction	Kanada	Ransomware	Diebstahl von 60 GB Daten, darunter sensible Mitarbeiter- und Finanzinformationen

Bauprojektphasen – Fokus: Realisierung



Hofstadler, C., Kummer, M. (2017). Methoden des Chancen- und Risikomanagements in den Projektphasen. In: Chancen- und Risikomanagement in der Bauwirtschaft. Springer Vieweg, Berlin, Heidelberg.

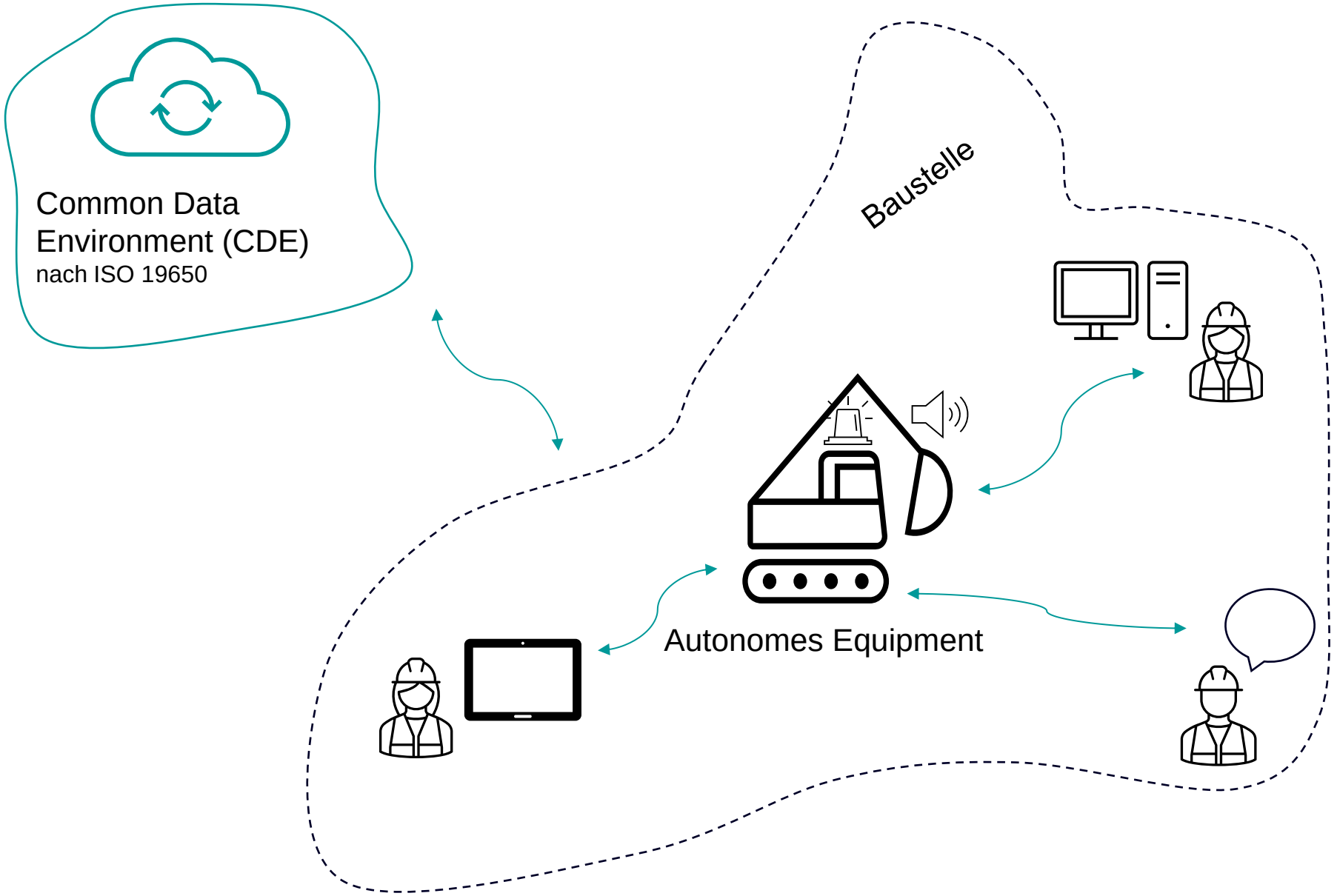
OT und IT in der digitalisierten Bauindustrie



Bedrohungsanalyse

Beispiel

Bedrohungsanalyse - System



Bedrohungsanalyse - Vorgehensweise

Welche Methode wende ich an?

Welche Schutzziele gibt es für mein System?

Welche Assets habe ich?

Welche Gefahren gibt es für mein System?

Bedrohungsanalyse - Methode

Welche Methode wende ich an?

Method	Threat Range	Empiricism	Consistency	Risk - Mitigation	Suitability	Documentation
OCTAVE	Medium	Yes	Yes	Yes	No	Medium
Trike	High	Yes	No	Yes	Yes	Low
PASTA	Medium	Yes	Yes	Yes	No	High
STRIDE	High	No	No	Yes	Yes	High
CORAS	Medium	Yes	Yes	Yes	No	Low
VAST	Medium	No	Yes	Yes	No	High
LINDDUN	High	No	No	Yes	Yes	Medium
hTMM	High	No	Yes	Yes [4]	Yes	N/A [3]
QuantitativeTMM	High	Yes	Yes	Yes [4]	Yes	N/A [3]
CAPEC [1]	Medium	No	N/A	No	No	N/A
ATT&CK [1]	Medium	No	N/A	Yes	No	N/A
IIDIL / ATC	High	No	Yes	Yes	Yes	Low
Security Cards + PnG [2]	Medium	No	Yes (SC) – No (PnG)	No	No	High (SC) – Low (PnG)

[1] CAPEC and ATT&CK are considered threat libraries and do not necessarily provide information as to modeling threats in a system
[2] Security Cards + PnG are essentially a gamification of the threat modeling process and should be used for training and brainstorming purposes only
[3] hTMM and QuantitativeTMM use STRIDE, and therefore we use the STRIDE documentation as a baseline for these TMMs; however, the methods themselves are not as mature as STRIDE
[4] Risk Mitigation based on STRIDE

Mohamed Shibly, Maahir Ur Rahman & García de Soto, Borja. (2020). Threat Modeling in Construction: An Example of a 3D Concrete Printing System. 10.22260/ISARC2020/0087.

Bedrohungsanalyse - Methode

Welche Gefahren beschreibt die Methode?

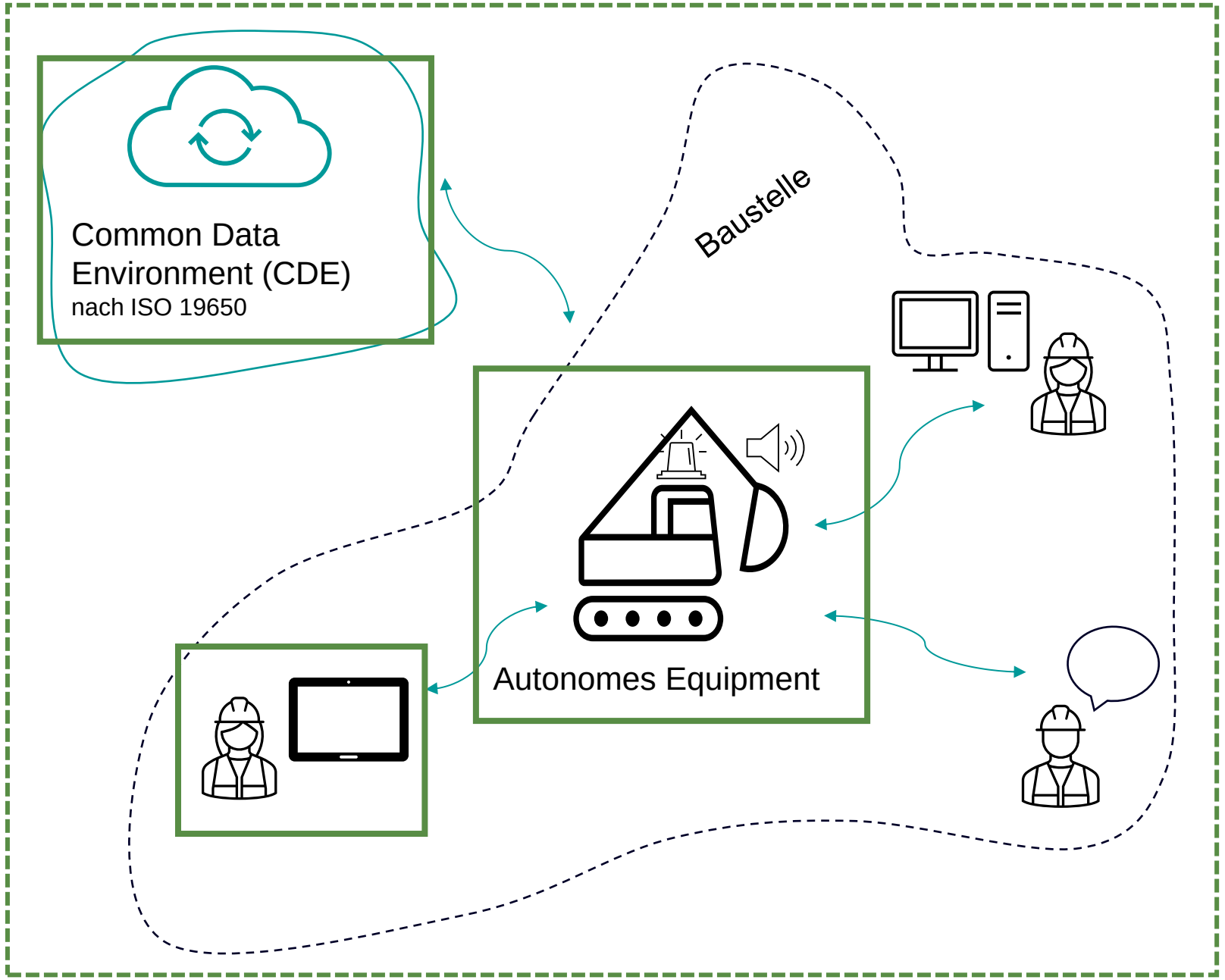
	Gefahr	Beschreibung
S	Spoofing	Identitätsvortäuschung
T	Tampering	Unbefugte Änderung von Daten oder Systemen
R	Repudiation	Möglichkeit eines Benutzers, eine Aktion zu leugnen oder abzustreiten
I	Information Disclosure	Offenlegung von Informationen
D	Denial of Service	Überlastung eines Systems oder Dienstes, so dass er für legitime Benutzer nicht mehr verfügbar ist
E	Elevation of Privilege	Ein Benutzer erhält mehr Rechte als ihm eigentlich zustehen

Bedrohungsanalyse - Schutzziele

Welche Schutzziele gibt es für mein System?

Gefahr	Schutzziele	Definition
Spoofing	Authentifizierung	Verifizierung der Identität eines Benutzers oder Systems, um sicherzustellen, dass sie tatsächlich diejenigen sind, für die sie sich ausgeben.
Tampering	Integrität	Gewährleistung, dass Daten genau, vollständig und unverändert bleiben.
Repudiation	Nichtabstreitbarkeit	Der Versand und Empfang von Daten und Informationen kann durch einen Nachweis nicht geleugnet werden.
Information Disclosure	Vertraulichkeit	Sicherstellung, dass Informationen nur für autorisierte Personen zugänglich sind.
Denial of Service	Verfügbarkeit	Sicherstellung, dass Informationen und Systeme bei Bedarf zugänglich und nutzbar sind.
Elevation of Privilege	Autorisierung	Prozess der Festlegung, welche Rechte und Zugriffe ein authentifizierter Benutzer auf Ressourcen hat.

Bedrohungsanalyse - Assets



Wo ist meine Systemgrenze?

Wie agiert mein System?

Systemgrenze

Bedrohungsanalyse - Assets

Welche Assets habe ich?

Assets
Common Data Environment (CDE)
Autonome Baumaschine
Mensch

Welche Schnittstellen habe ich?

Schnittstellen
Human-Machine Interface
Übertragungspfad in die CDE

Wie kommunizieren meine Assets?

Kommunikationswege
Mobile Geräte und Kontrollstationen
Sprachsteuerung
Visuelle und akustische Signale
Remote Control
Mobilfunk
Sensorik

Bedrohungsanalyse – Beispiel der Ausführung

Asset	Bedrohung durch Tampering (Unbefugte Änderung von Daten oder Systemen)	Auswirkung (Damage Scenario)
Autonome Baumaschine	Veränderung von Sensordaten	Fehlinterpretation der Umgebung
	Manipulation der Steuerungssoftware (Einschleusen von bösartigem Code in Firmware-Updates)	Übernahme der Kontrolle über autonomes Bauequipment
Mensch	Manipulation von Zugangskontrollsystemen	Unerlaubter Zutritt in Systeme oder Bereiche
CDE	Manipulation von Projektdaten	Verlust der Datenintegrität
	Veränderung von Zugriffsrechten und Benutzerkonten	Sicherheitslücken durch unbefugte Zugriffsrechte

TU Graz

Bedrohungsanalyse – Weitere Schritte

- Priorisierung der Risiken
- Analyse der Angriffsvektoren
- Entwicklung von Gegenmaßnahmen
- Investitionen in Cybersecurity-Maßnahmen (ROSI)

Weitere Fragen?

LinkedIn: Elisabeth Gütl