TeleTrusT
Pioneers in IT security.

TeleTrusT – Bundesverband IT-Sicherheit e.V.

TeleTrusT-Workshop "Industrial Security" 2015

München, 11.06.2015

Quick-Step-Sicherheitsanalyse für Industrie 4.0-Vorhaben

Dr. Patrik Gröhn
exceet secure solutions

Überblick

- Erkenntnisse der exceet M2M-Nutzenstudie (Überblick) – Erfolgsfaktoren und Herausforderungen
- IoT-Nutzenradar und Projektmethodik (Maschine, Prozess, Business)
- Sicherheitsanalyse
- Sicherheitsanforderungen für Industrie 4.0 Vorhaben
- Lösungsansatz exceet secure ecosystem

Hürden und Fallstricke bei IoT Projekten

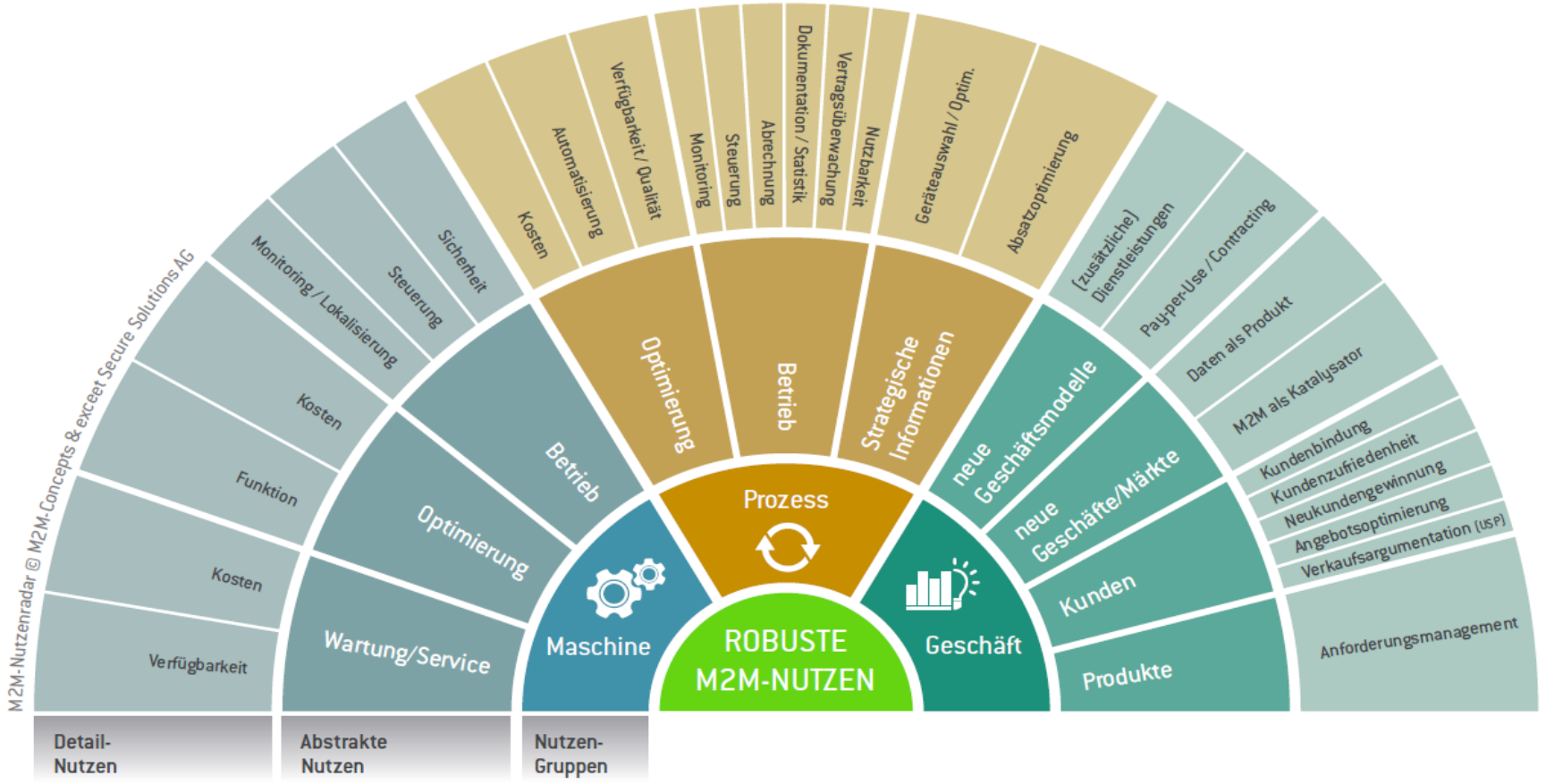
≈ 50%

- **Neu gestartet**
- **Vorzeitig beendet**

1. Falsche Rahmenbedingungen
2. Fehlende Abstimmung: Business & IT
3. Unterschätzte Komplexität (interne Umsetzung)
4. Ausschließlich regionale Vorbereitung
5. Keine Lösungen für Sicherheit & Compliance

Value Engineering

- exceet-Tool zur Nutzenanalyse - Nutzenradar



Sicherheitsanalysen

Verfahren, z.B.

- externes Audit mit Checklisten
- Self-assessment
  - BSI-Grundschutz
  - Gap-Analyse Normen
  - LARS ICS
  - …
- FMEA
- …

Sicherheitsanalyse: Bottom up Verfahren

- Von Ursachen (Gefahr)
- zum Prozess
- zum Risiko
- zur Wirkung
  - Nachteil
    - Es gibt keine logische Ableitung der Risiken und Risikoarten nach Ursachen, die eine Vollständigkeit nachvollziehbar machen würde
    - Aufgrund einer Vielzahl von potentiellen Ursache-Wirkungszusammenhängen kann es keine vollständige Systematisierung nach Risikoursachen geben.
  - Vorteil
    - Verschiedene Wirkungen einer Ursache werden identifiziert z.B. Hackerangriff (Ertragsausfall wegen Produktionsstop aufgrund Serverausfall, erhöhte Kosten für Wiederherstellung)

Sicherheitsanalyse: Top Down Verfahren

Vom Unternehmen (Anlage)
- zu den Hauptgeschäftsfeldern
- zum Output
(Produkt/Dienstleitung)
der Anlage
- über den Prozess
- zum Risiko
- zu Ursachen / Ursachenbereiche

- **Widerspiegelung der Gesamtunternehmenssicht / Gesamtvorhabens**
- **Angesetzt bei der Unternehmens-/ Anlagenleitung**
- **Vorangetrieben in Unternehmensbereiche und Geschäftsfelder**
- **Vorteile:**
  - Gesicherte umfassende Anwendbarkeit
  - Freie Wahl der Tiefe der Identifikation
  - Wenn bei Projektstart eine zu grobe Detaillierungstiefe gewählt wurde, kann immer noch jedes ausreichend gewichtige Risiko verfeinert werden

Integriertes Verfahren

- Identifikation aller Risiken und Ursachen

TOP-DOWN-Verfahren gewährleistet Identifikation aller Risiken

Identifizieren der Risiken und Ursachen (Gefahren) erfolgt in Workshops/Interviews mit den Abteilungen auf Basis eines strukturierten Fragenkatalogs, eines strukturierten Interviewbogens und vordefinierter Ursachenbereiche.

Bottom-Up-Verfahren gewährleistet Identifikation aller Ursachen (und deren Wirkungen)

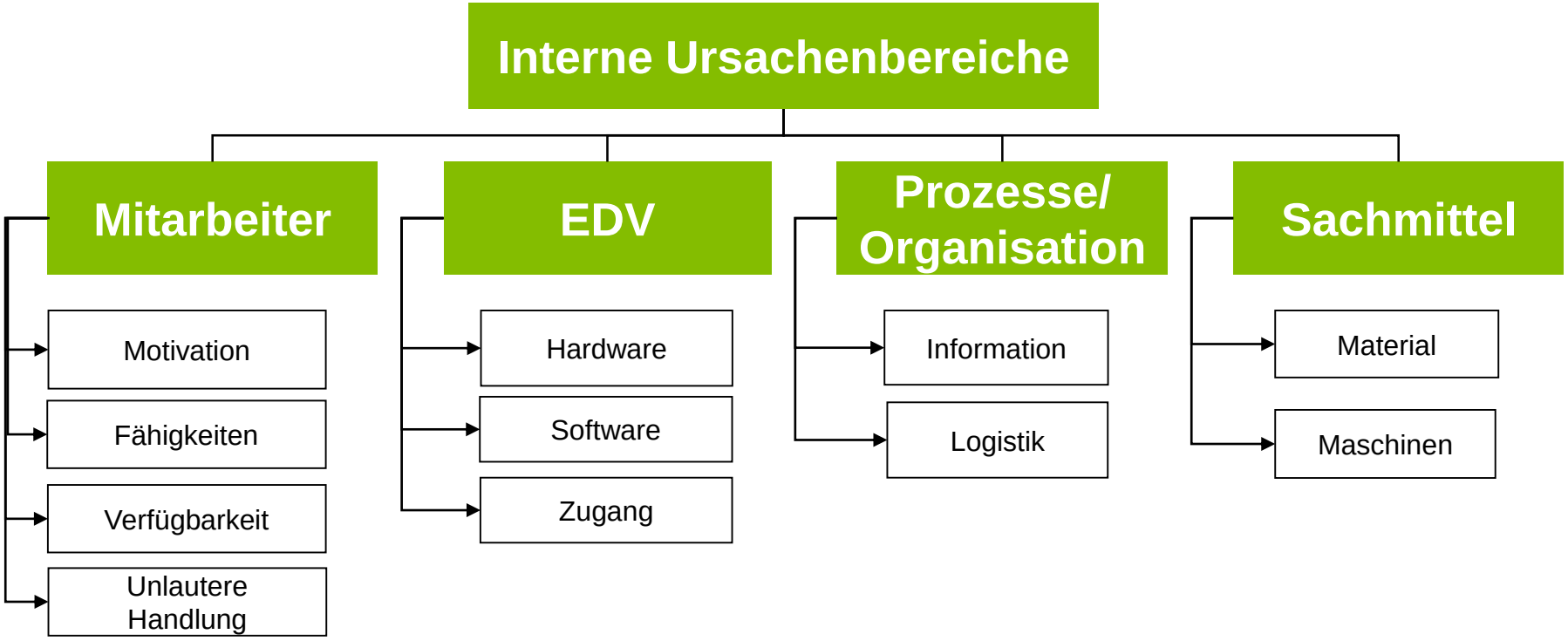
Scope: Identifikation Prozessoutput

- Der Output/das Produkt...
  - wird nicht erbracht
  - wird zu spät erbracht
  - wird falsch erbracht
  - wird unvollständig erbracht
  - wird nicht in gewünschter Qualität erbracht (Berührung mit Qualitätsmanagement)
  - wird richtig erbracht, jedoch nicht wahrgenommen
  - wird richtig, aber unwirtschaftlich erbracht (Berührung mit Kostenmanagement)

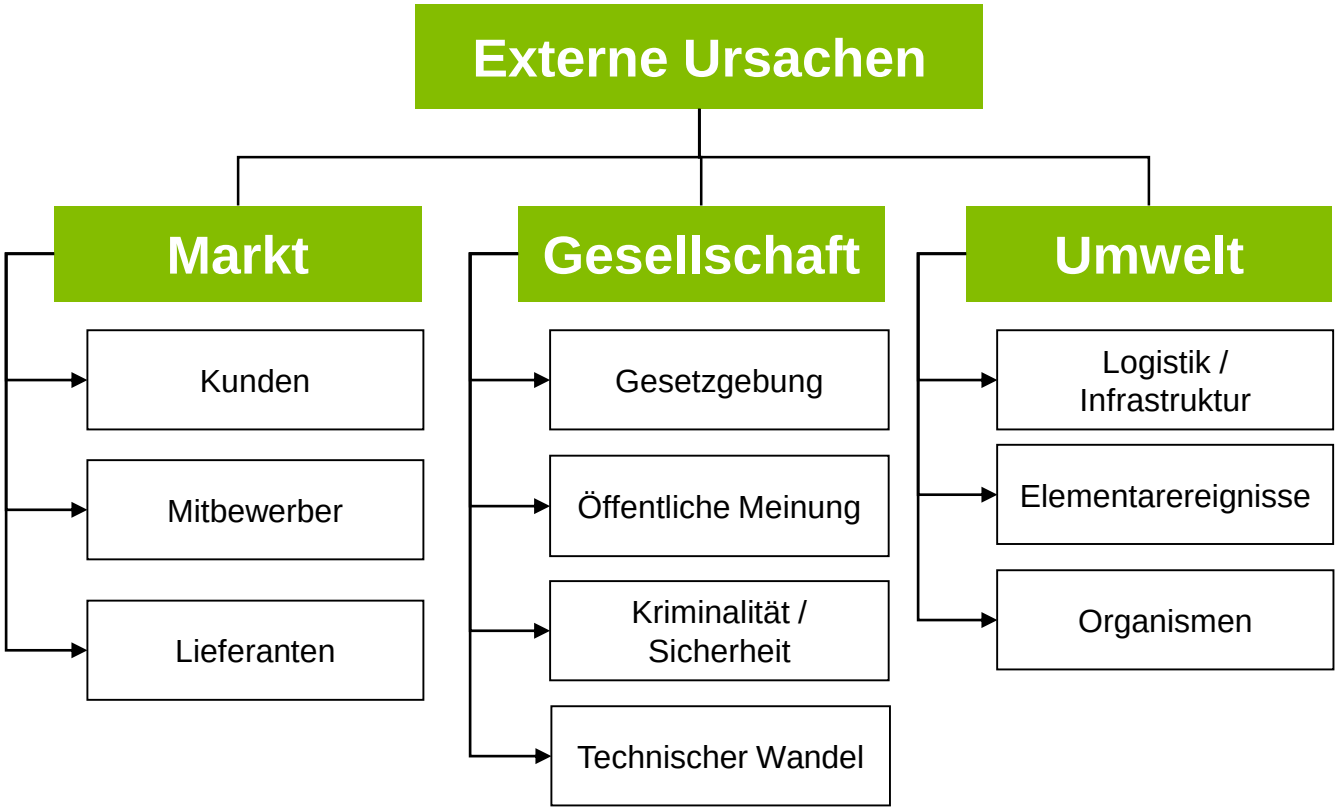
Risiken und Ursachen

- Der Output / das Produkt wird nicht erbracht, weil...
  - z.B. die Server aufgrund Hackerangriff ausgefallen ist
- Der Output / das Produkt wird zu spät erbracht, weil...
  - z.B. das Netzwerk aufgrund externer Angriffe Kapazitätsverluste erleidet
- Der Output / das Produkt wird falsch erbracht, weil...
  - z.B. Mitarbeiter nicht wussten, wie es richtig geht
- Der Output / das Produkt wird unvollständig erbracht, weil...
  - klare Anweisungen zur Qualitätskontrolle des Produkts fehlen
- Der Output / das Produkt wird richtig erbracht, jedoch nicht wahrgenommen weil...
  - ein Konkurrent dasselbe Produkt aufgrund Spionage günstiger auf den Markt bringt

Interne Ursachen (Beispiele)



Externe Ursachen (Beispiele)



Quick-Step Sicherheitsanalyse

Industrial Security - Eventanalyse

RISI — The Database — About — Contact

Last Updated: Wed, January 28, 2015

Title	Year	Industry Type	Country	Brief
Page 1 of 9 pages **1** 2 3 > Last ›				
German Steel Mill Cyber Attack	2014	Metals	Germany	
Russian-Based Dragonfly Group Attacks Energy Industry	2014	Power and Utilities	United States	
Public utility compromised after brute-force hack attack, says Homeland Security	2014	Power and Utilities	United States	
After 'Godzilla Attack!' U.S. warns about traffic-sign hackers	2014	Transportation	United States	
U-2 spy plane caused widespread shutdown of U.S. flights: report	2014	Transportation	United States	
Virus shuts down county highway department network	2013	Transportation	United States	
Signal problems cause train delays	2013	Transportation	United States	
Computer Glitch Leads to Shutdown of Nuclear Reactor	2012	Power and Utilities	United States	
U. S. Power Plant Infected With Malware	2012	Power and Utilities	United States	
U. S. Electric Utility Virus Infection	2012	Power and Utilities	United States	
Software Manufacturing Company Firewall Breach	2012	General Manufacturing	Canada	
Shamoon virus knocks out computers at Qatari gas firm RasGas	2012	Petroleum	Qatar	
Computer Virus Targets Saudi Arabian Oil Company	2012	Petroleum	Saudi Arabia	

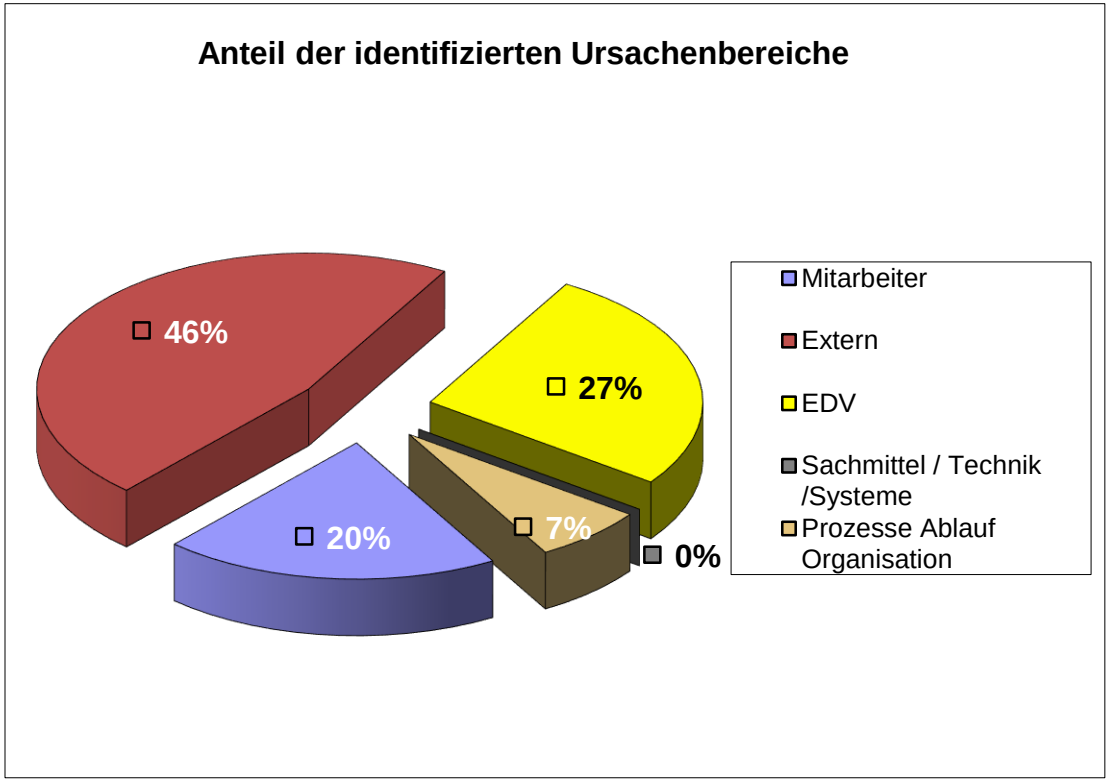
Zuordnung Ursachenbereiche

Quelle: Industrial Security Incidents Database (ISID)

Ergebnis Quick-Step Sicherheitsanalyse

Ursachenbereich	Anzahl
Extern: Elementarereignisse	
Extern: Gesetzgebung / Öffentlichkeit	
Extern: Kriminalität / Sicherheit	6
Extern: Lieferanten	
Extern: Markt	
Extern: Umwelt / Infrastruktur	1
Mitarbeiter: Fähigkeiten	1
Mitarbeiter: Motivation und Sorgfalt	1
Mitarbeiter: Unlautere Handlung	1
Mitarbeiter: Verfügbarkeit	
Prozesse: Ablauf-Organisation	1
Sachmittel / Technik / Systeme	
Systeme: EDV	4

Anzahl analysierter Security Events: 7
Anzahl Ursachen: 15



Security Events erfolgen vermehrt durch das Zusammenwirken verschiedener Ursachen

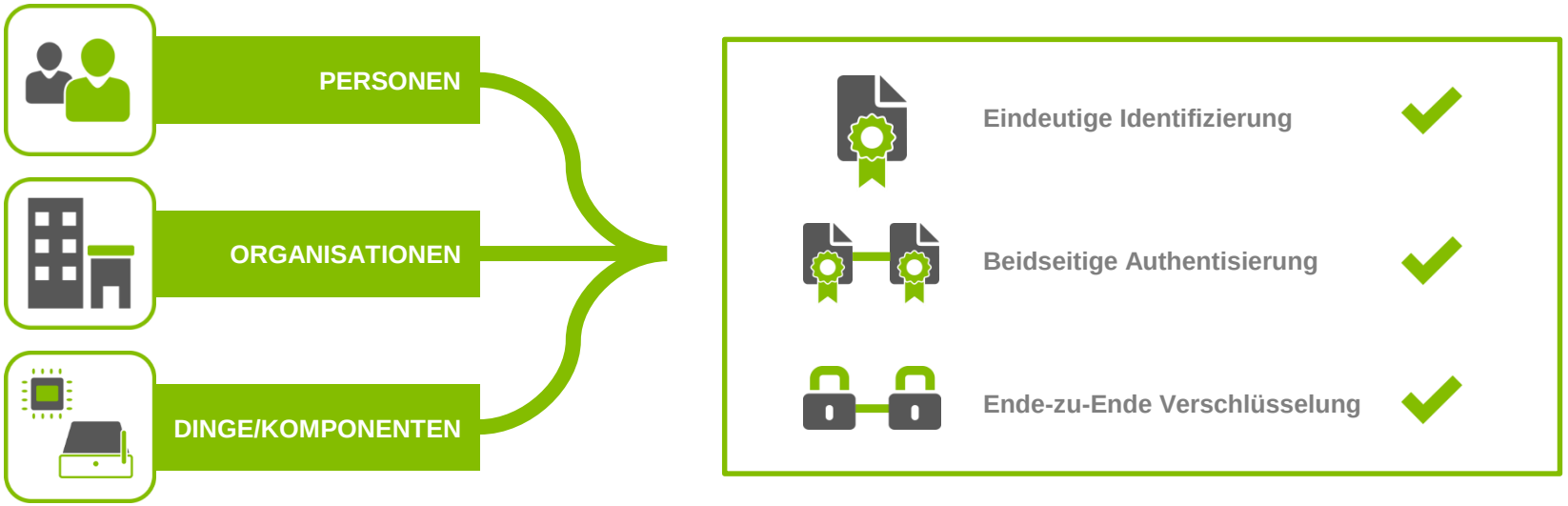
Ergebnisse

- Die Ergebnisse aus Sicherheitsanalysen für Industrie 4.0 - Vorhaben lassen viele Parallelen zu „Smart Grid Security“ erkennen.
  - Industrial Security - Lösungsansatz in Analogie zu Anforderungen aus TeleTrusT-Eckpunktepapier "Smart Grid Security"

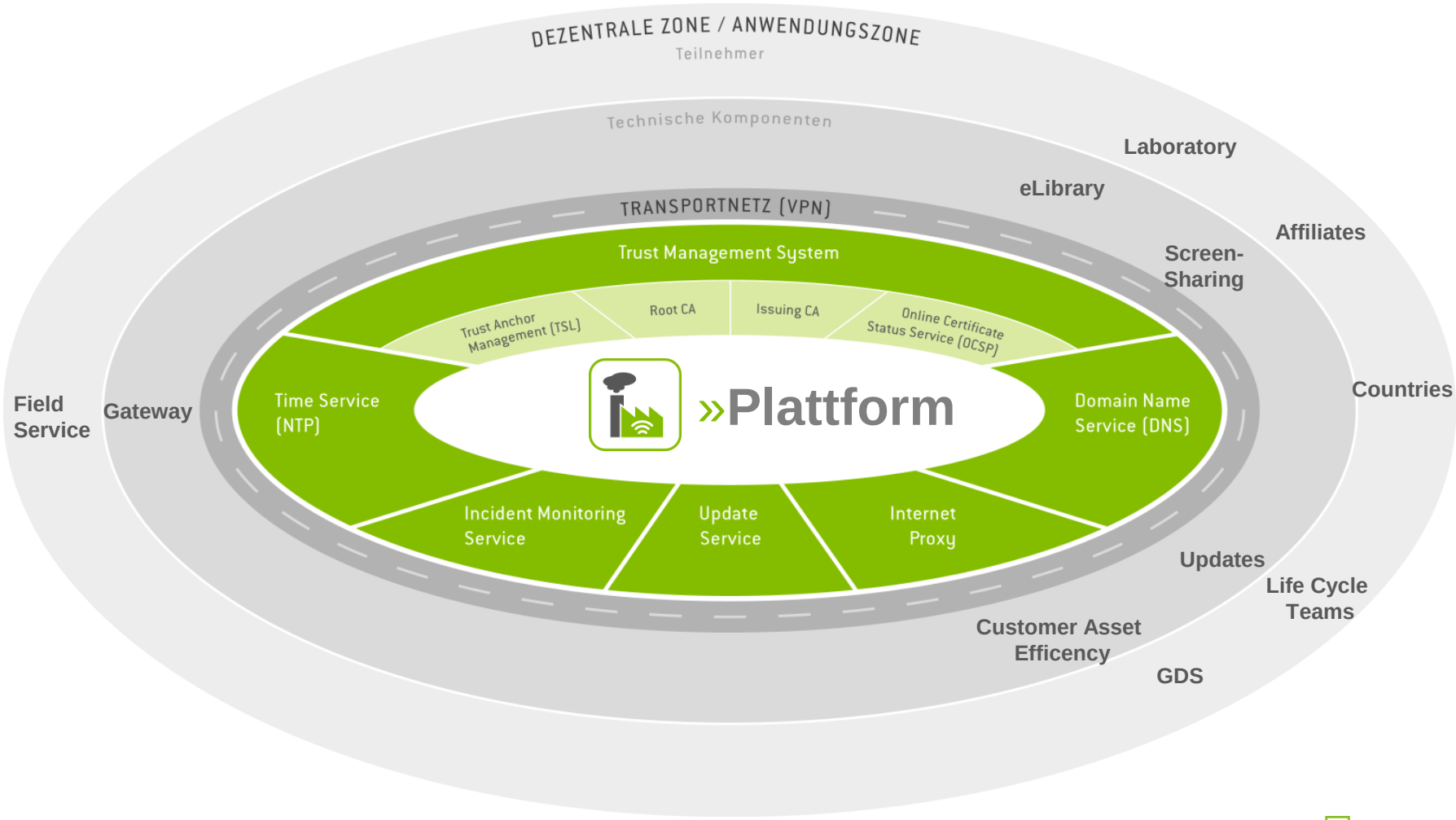
Secure Connected Ecosystem

Im Zeitalter, in welchem Maschinen, Objekte, Personen und Organisationen voll automatisiert Daten austauschen, wird die Sicherheit zum entscheidenden Erfolgsfaktor. Für Professionelle Anwendungen ist daher die Schaffung eines digitalen Vertrauensraums zwingend erforderlich.

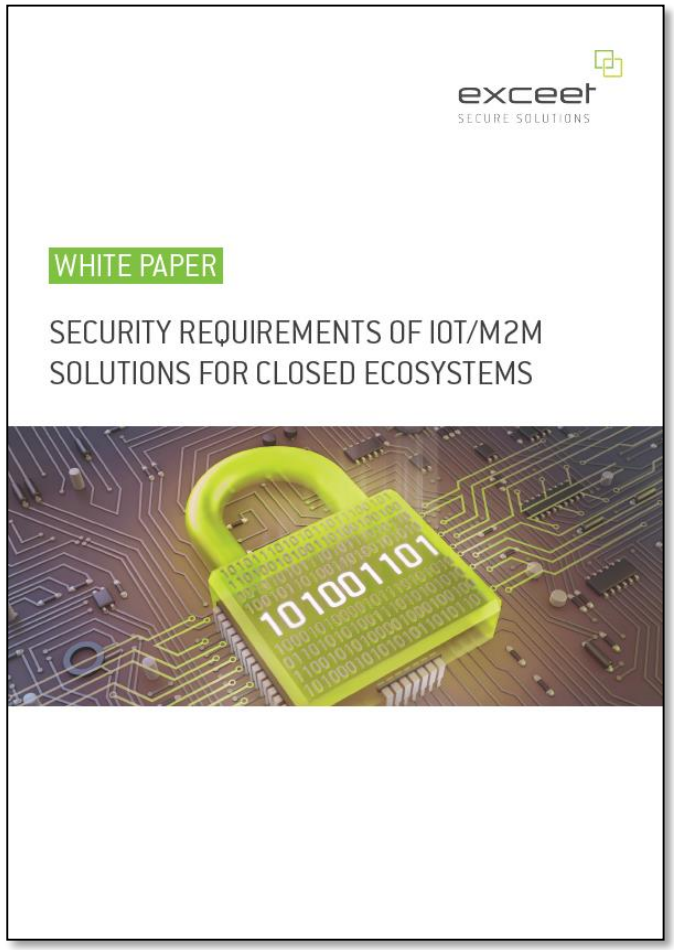
exceet Secure Solutions spricht hierbei von der digitalen Identifizierung und Authentifizierung alle Teilnehmer und Objekte sowie von einer sicheren Ende-zu-Ende-Verschlüsselung jeglicher Kommunikation: Mithilfe des Secure Connected Ecosystem.



Industrie 4.0 – Exceet Secure Ecosystem



Sicherheitsanforderungen in einem geschlossen ECO-System



Overview: Security Requirements

1. Communication Security
2. Device Security
3. Identification of Participants
4. Participant Management
5. Hardware Security Modules
6. Operation
7. Data Ownership

- Vielen Dank für Ihre Aufmerksamkeit!