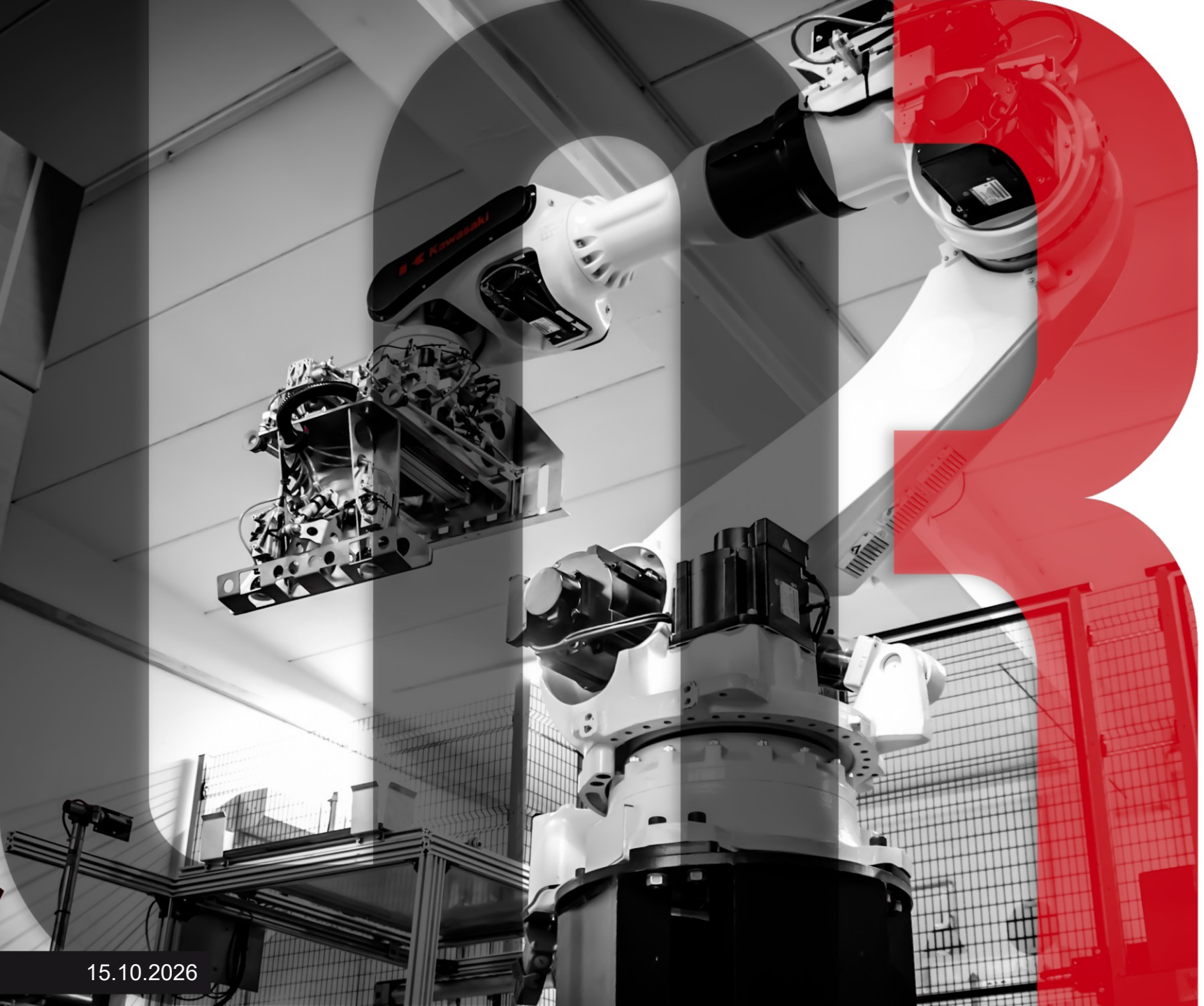


CYBERSECURITY

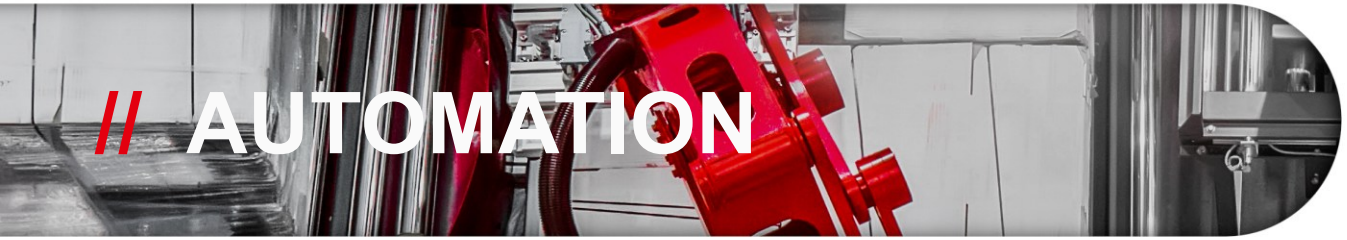
// Risikobewertung im Dreisprung

© Lanfer Automation + Robotics GmbH, Alle Rechte vorbehalten

// Speaker

Scan Me

© Lanfer Automation + Robotics GmbH, Alle Rechte vorbehalten



DAS UNTERNEHMEN

// Lanfer Automation + Robotics

- **40 Jahre** Unternehmensgeschichte
- über **100 Mitarbeitende**
- Teil der **LB GmbH**
- Anbieter **ganzheitlicher Lösungen**
- **440 Kunden** aus allen Sektoren
- selbst **NIS-2-betroffen**

© Lanfer Automation + Robotics GmbH, Alle Rechte vorbehalten

RISIKOBEWERTUNG IM DREISPRUNG

// Inhaltsverzeichnis

Effektive Gegenmaßnahmen auswählen
Vom System auf Bedrohungen schließen
Von der Verantwortung zum Systemmodell
4 Cybersichere Maschine
3 Die Bedrohung
2 Das System
1 Compliance

© Lanfer Automation + Robotics GmbH, Alle Rechte vorbehalten

// Parteien, …

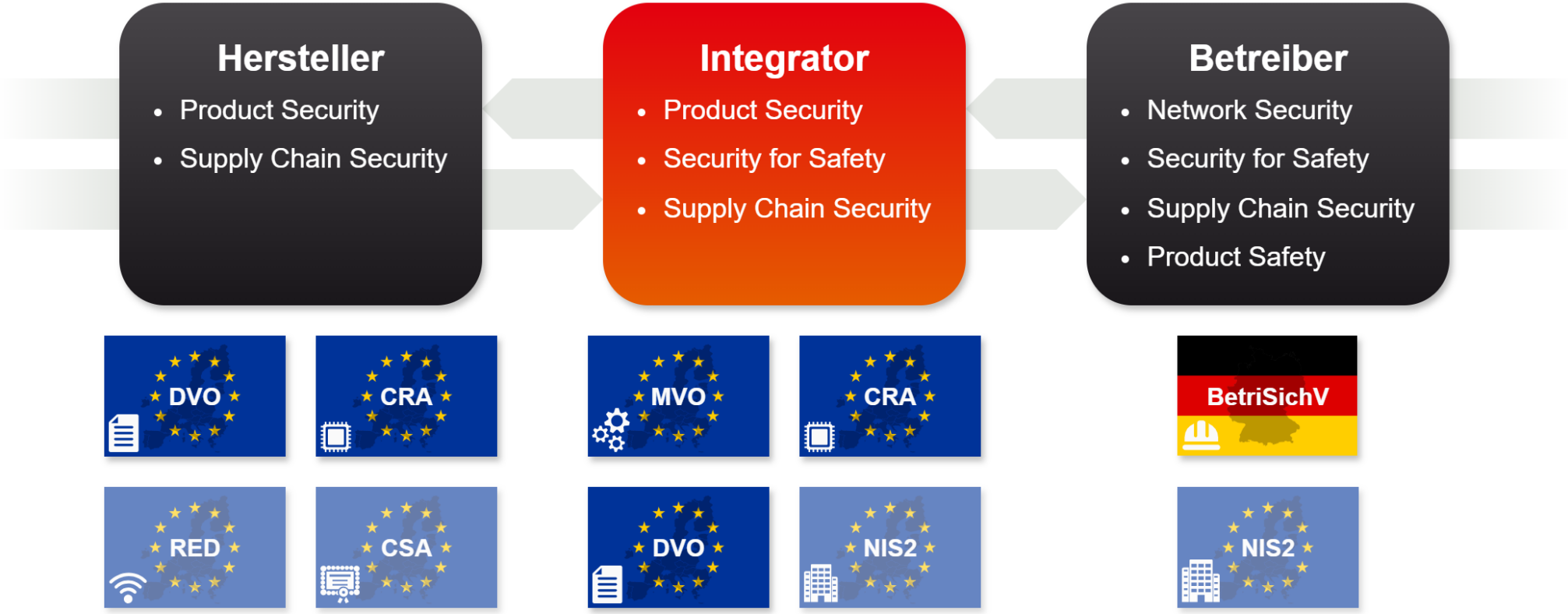
© Lanfer Automation + Robotics GmbH, Alle Rechte vorbehalten

// … ihre Interessen …

© Lanfer Automation + Robotics GmbH, Alle Rechte vorbehalten

COMPLIANCE

// … und Pflichten



© Lanfer Automation + Robotics GmbH, Alle Rechte vorbehalten

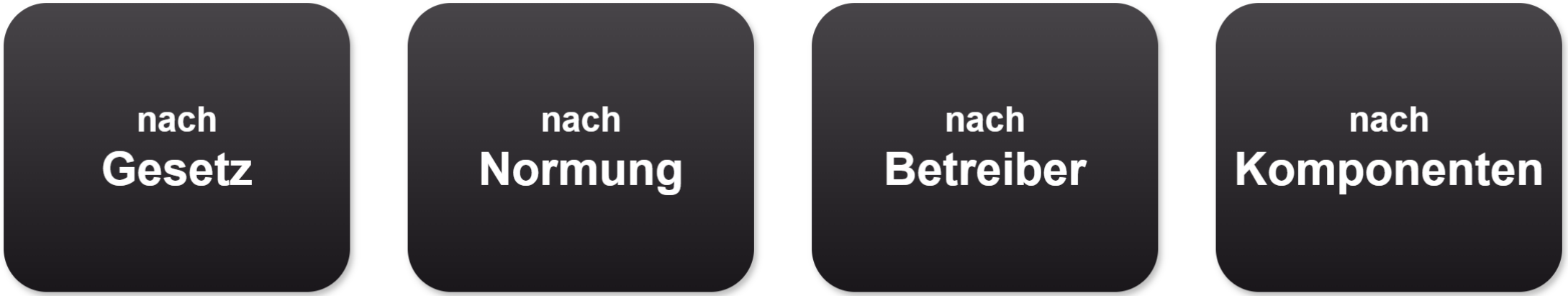
// Methodik der Risikobeurteilung

Allgemeiner Ablauf

DIN EN ISO 12100:2011

© Lanfer Automation + Robotics GmbH, Alle Rechte vorbehalten

// Abgrenzung: der Cybersecurity-Kontext



© Lanfer Automation + Robotics GmbH, Alle Rechte vorbehalten

// Abgrenzung: der Cybersecurity-Kontext

nach Gesetz

- Sichere Schnittstellen zu externen Systemen
- Einsatz cybersicherer Safety-Hardware
- Schutz von Software

nach Normung

nach Betreiber

- Anfertigung einer Software-Stückliste
- Logging von Eingriffen und Veränderungen
- Schutz vor Fremdeinflüssen

nach Komponenten

© Lanfer Automation + Robotics GmbH, Alle Rechte vorbehalten

// Verantwortung nach Rechtslage

Komponente	MVO	CRA	Verantwortung
SPS mit Firmware	als Teil der Maschine	eigenes PDE	Hersteller
Safety-SPS und -Parametrierung	ja	eigenes PDE	Hersteller, **Integrator**
SPS-Anwenderprogramm	als Teil der Maschine	eigenes PDE	**Integrator**
F-Programm	ja	eigenes PDE	**Integrator**
digitale / analoge Signale	nein	nein	—
Sensoren	nein	falls PDE	Hersteller
sicherheitsgerichtete Sensoren	ja	falls PDE	Hersteller
Betriebssystem auf IPC	als Teil der Maschine	eigenes PDE	Entwickler
Router / Switches / Kopplungen	als Anschluss anderer Einrichtungen	wichtiges PDE Klasse I	Hersteller
Umrichter	als Teil der Maschine	eigenes PDE	Hersteller
Anwendungen auf IPC	als Teil der Maschine	eigenes PDE	Entwickler
Gesamtmaschine	**ja**	**PDE aus PDEs**	**Integrator**

PDE = Produkt mit digitalen Elementen

© Lanfer Automation + Robotics GmbH, Alle Rechte vorbehalten

// Abgrenzung: der Cybersecurity-Kontext

nach **Gesetz**

nach **Normung**

nach **Betreiber**

nach **Komponenten**

- Nur sicherheitsrelevante Komponenten
- Bedrohungen schaffen keine neuen Gefährdungen
- einfache I/O müssen nicht betrachtet werden

- Grundanforderungen
- Methodenempfehlungen
- Bewertungskriterium SRSL

© Lanfer Automation + Robotics GmbH, Alle Rechte vorbehalten

// Abgrenzung: der Cybersecurity-Kontext

nach Gesetz

nach Normung

nach Betreiber

nach Komponenten

- Anforderungen des ISMS
- Sektorspezifische Anforderungen
- Anforderungen aus der Gefährdungsbeurteilung

- Attraktivität für Angreifer
- Schnittstellen zu externen Systemen
- betreiberseitige Cybersicherheitsmaßnahmen

© Lanfer Automation + Robotics GmbH, Alle Rechte vorbehalten

// Abgrenzung: der Cybersecurity-Kontext

nach Gesetz

nach Normung

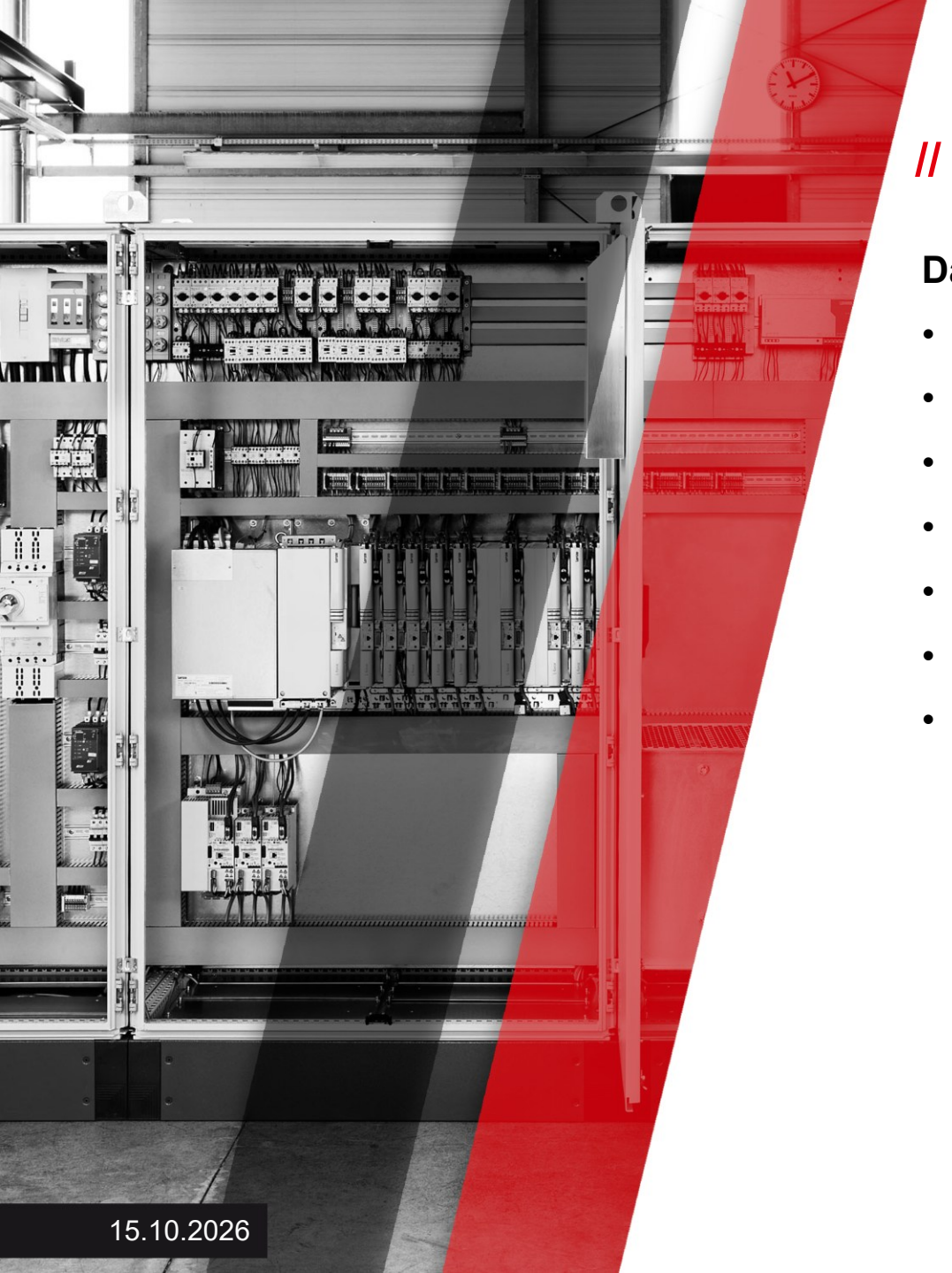
nach Betreiber

nach Komponenten

- CRA-Konformität (Secure by Design & Default)
- Informationen nach EU-Datenverordnung
- Cybersicherheitsfunktionen

- Konfiguration/Parametrierung
- ergänzende Software
- Schnittstellen

© Lanfer Automation + Robotics GmbH, Alle Rechte vorbehalten



DAS SYSTEMMODELL

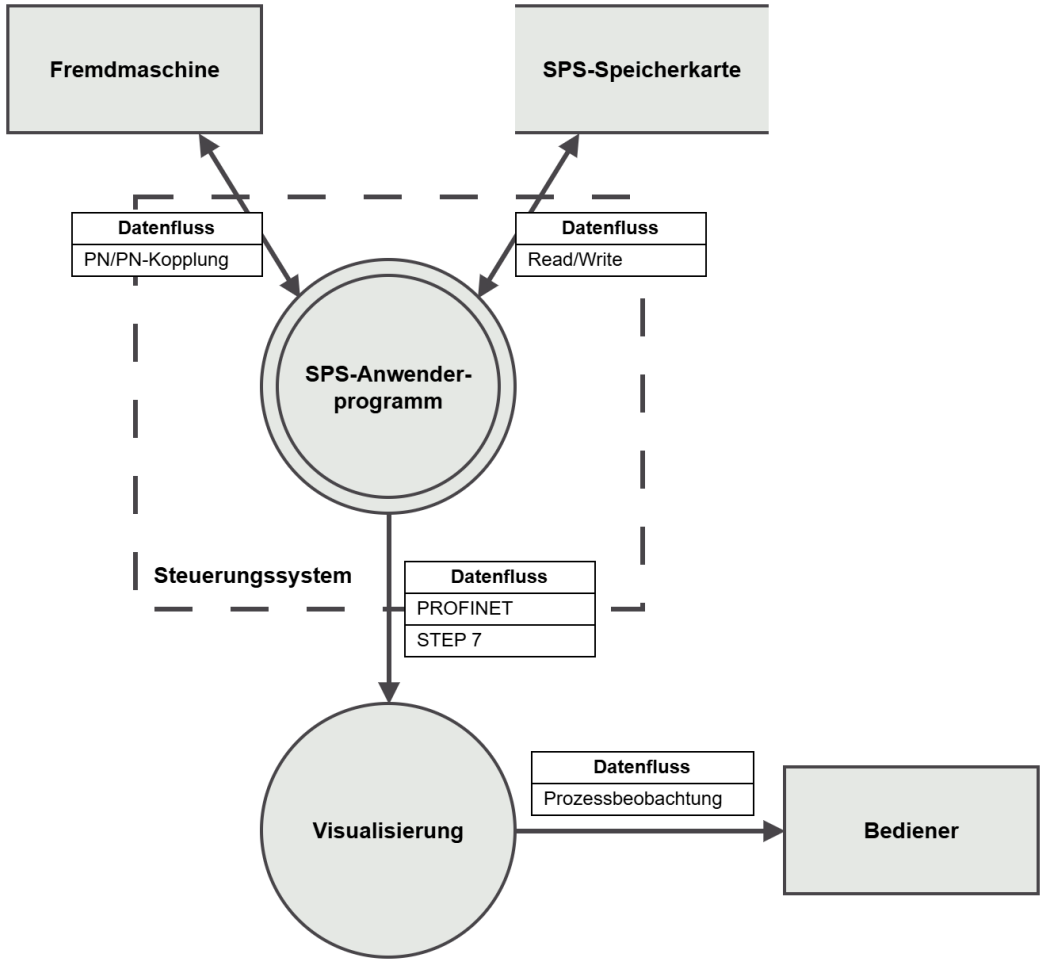
// Bilanz

Datengrundlage

- Anforderungskatalog
- Hardware- & Software-Komponenten
- immaterielle Vermögenswerte (Daten)
- Verantwortlichkeiten
- Schnittstellen
- bestehende Cybersicherheitsmaßnahmen
- Betreiberinformationen

© Lanfer Automation + Robotics GmbH, Alle Rechte vorbehalten

// Datenflussdiagramm (DFD)



Methode

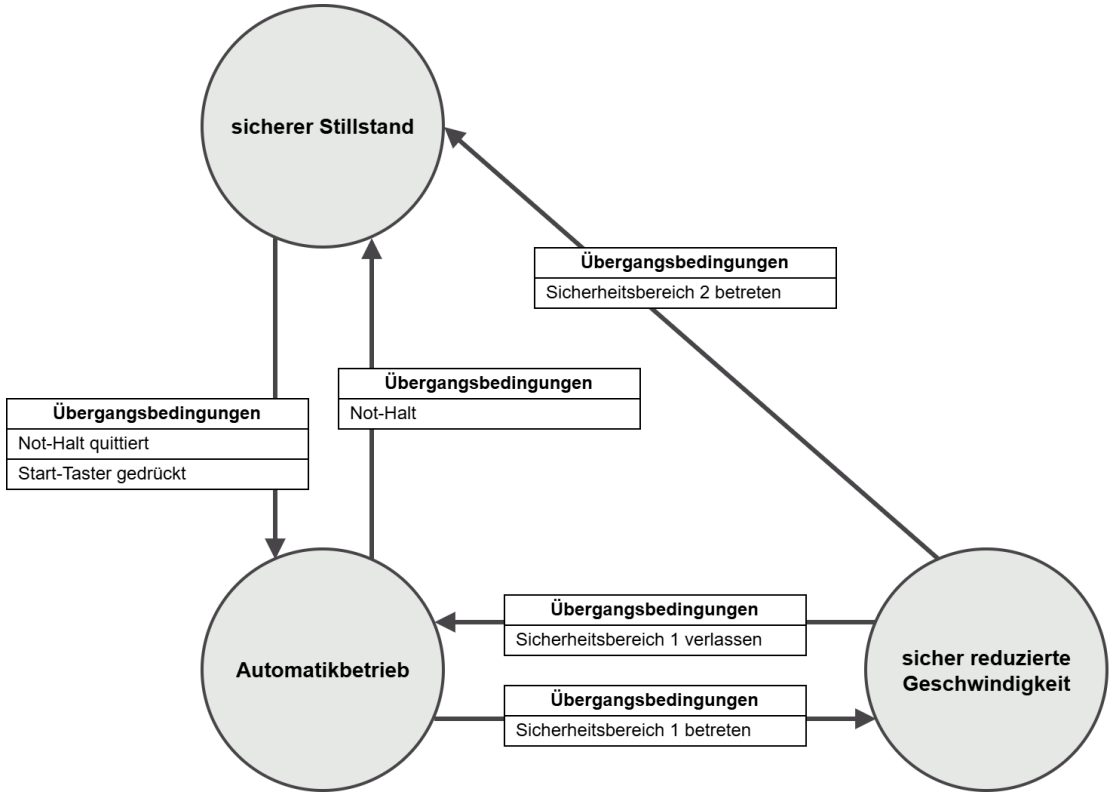
1) Prozesse definieren
2) Externe Systeme festlegen
3) Speicherorte kennen
4) Kommunikationswege eintragen
5) Vertrauensgrenzen ziehen

DFD-Elemente

- Externe Systeme
- Prozesse
- Datenspeicher
- Datenflüsse

© Lanfer Automation + Robotics GmbH, Alle Rechte vorbehalten

// Zustandsmaschine



Methode

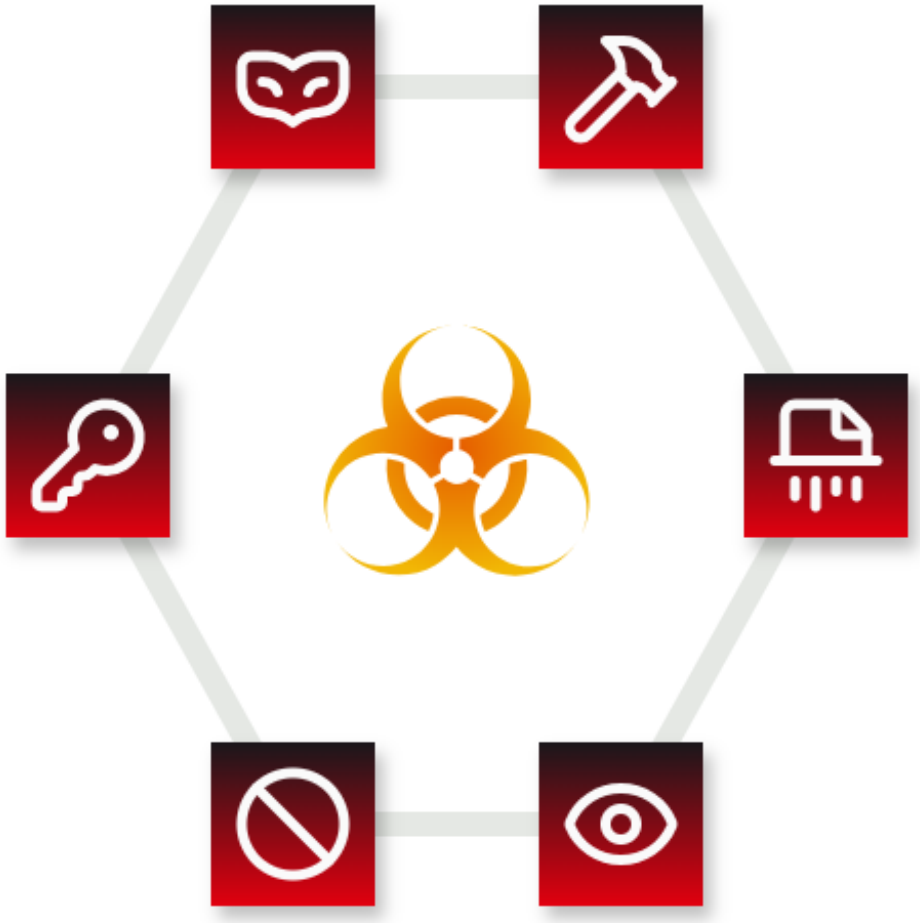
- Prozessabläufe erkennen
- Zustände aufnehmen
- Zustandswechsel einzeichnen
- Bedingungen

Diagrammelemente

- Zustände
- Zustandswechsel
- Übergangsbedingungen

© Lanfer Automation + Robotics GmbH, Alle Rechte vorbehalten

// Bedrohungen identifizieren



STRIDE

- 6 Bedrohungsarten
- 2 Methoden
  - STRIDE-per-Element
  - STRIDE-per-Interaction
- einsteigerfreundlich & Tools verfügbar

STRIDE-per-Element

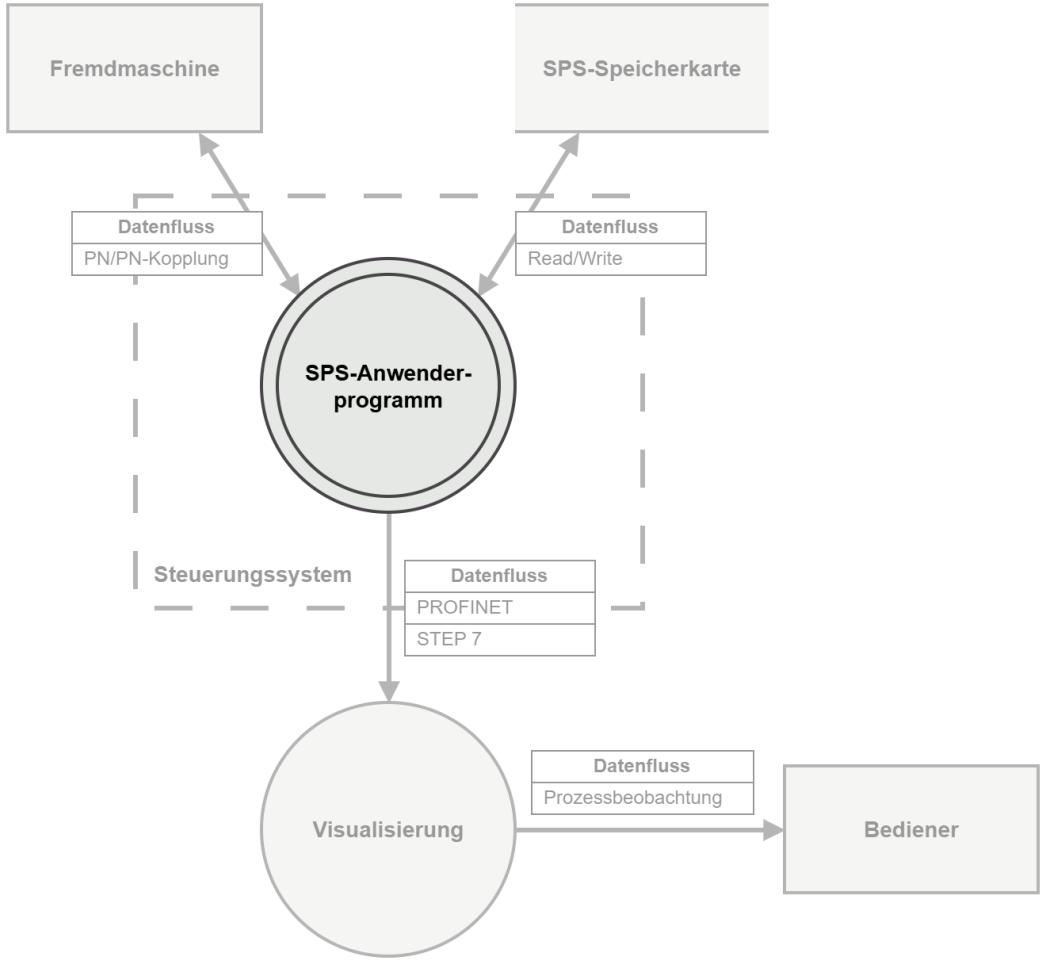
1) DFD als Grundlage
2) jedes Element betrachten
3) jeweils eine Bedrohung finden

Faktor Zeit

1) Zustandsdiagramm auswerten
2) mehrere Tabellen anlegen

© Lanfer Automation + Robotics GmbH, Alle Rechte vorbehalten

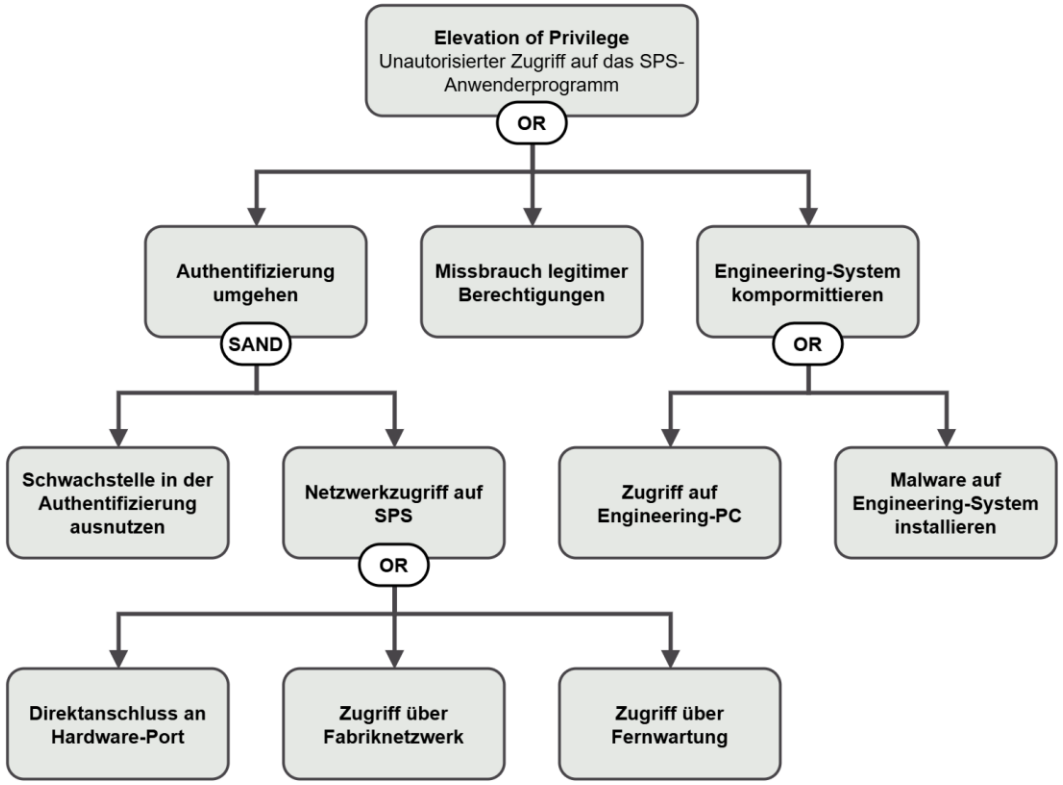
// Beispiel: EoP am SPS-Anwenderprogramm



P1.E1
Unautorisierter Zugriff auf das SPS-Anwenderprogramm

© Lanfer Automation + Robotics GmbH, Alle Rechte vorbehalten

// Bedrohungsszenarien zusammensetzen



Attack Trees

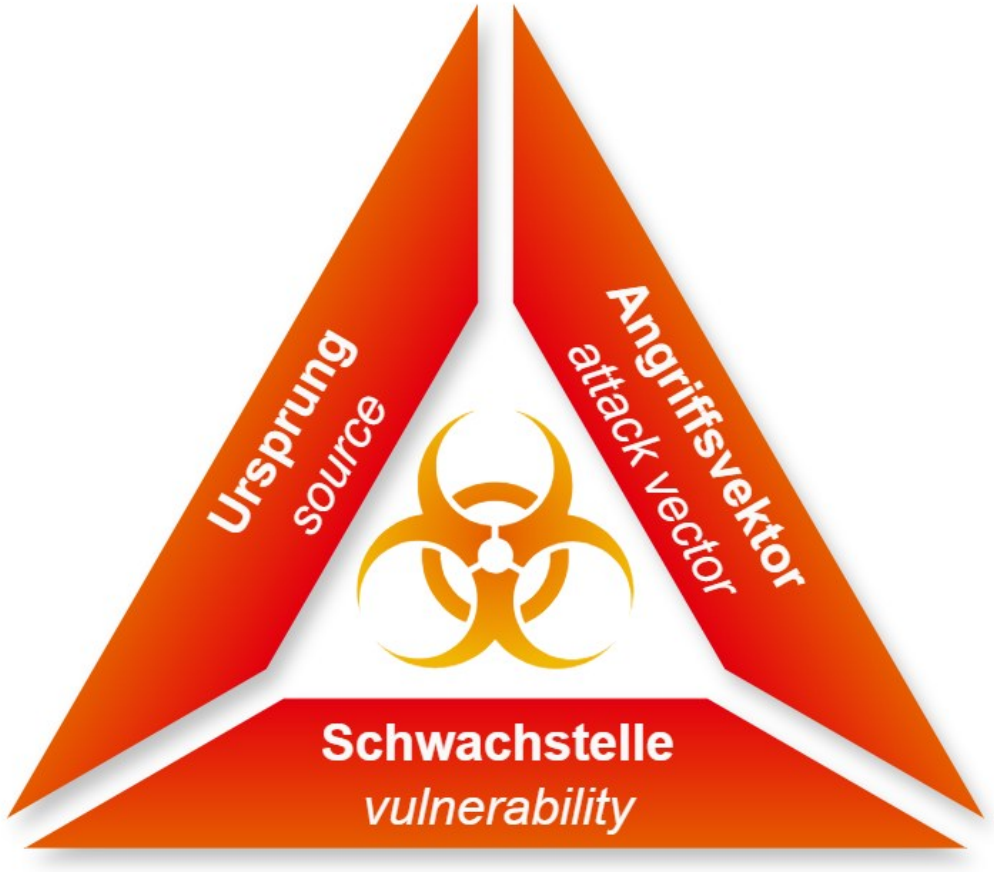
- Ein Ereignis, mehrere Ursachen
- Knoten: Ereignisse, Schwachstellen, Angriffsvektoren, Ursprünge
- Logische Verknüpfung (AND, SAND, OR, XOR)
- Ein Weg ist ein Szenario

Methode

1) Ereignis auswählen
2) Schwachstellen erkennen
3) Exploits recherchieren
4) Bedrohungsursprünge identifizieren
5) Angriffswege verknüpfen

© Lanfer Automation + Robotics GmbH, Alle Rechte vorbehalten

// Risikomodell



Risiko

Das Risiko ist die **Wahrscheinlichkeit**, mit der eine Bedrohung zu einem Vorfall führt, der einen **Schaden in einer bestimmten Höhe** zufügt.

Wahrscheinlichkeit

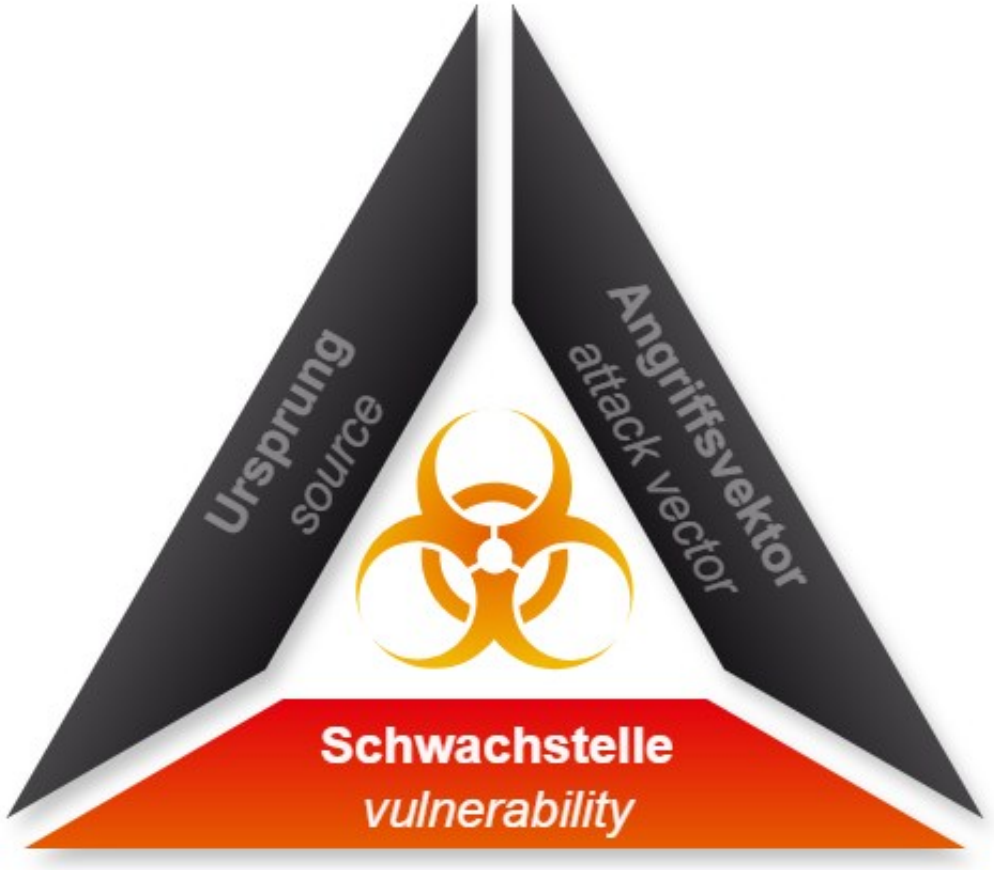
- Erfahrungswerte
- Datenbanken
- Ersatzmaße (prEN 50742: „Angriffspotenzial“)

Schadensausmaß

- Stillstandszeiten
- Kosten
- Personenschäden

© Lanfer Automation + Robotics GmbH, Alle Rechte vorbehalten

// Schwachstellen schließen



Herstellerseitige Maßnahmen

- Authentifizierung & Autorisierung einfordern
- Segmentierung durchsetzen
- sichere Coding-Standards einhalten
- Hardening-Benchmarks berücksichtigen
- Anti-Malware aufspielen
- Monitoring & Logging
- Vorgaben zur Entsorgung

Betreiberseitige Maßnahmen

- Wiederholte Beurteilungen
- Update Management
- Backup Management
- Vulnerability Management

© Lanfer Automation + Robotics GmbH, Alle Rechte vorbehalten

UNSERE SERVICES

// Wo wir Ihnen helfen können

Risk Assessments

- **Schnell-Assessment**
- **Ausführliches Assessment**
- OT-Security-**Workshops**

LAR CyberTalks

- 15-minütige Gespräche zu **Ihren** Fragen
- Fokus **OT-Cybersicherheit** & **Betriebssicherheit**
- für Sie **kostenfrei**

Nächste Termine

27.10.	9 – 11 Uhr
09.11.	14 – 16 Uhr

Booking unter event@lanfer.de

© Lanfer Automation + Robotics GmbH, Alle Rechte vorbehalten

LANFER AUTOMATION + ROBOTICS

Vielen Dank für Ihre Aufmerksamkeit!

Besuchen Sie uns an
// Stand 614

Lanfer Automation + Robotics GmbH
Hoher Weg 13
46325 Borken-Weseke

+49 2862 913 100
automation@lanfer.de
www.lanfer.de

© Lanfer Automation + Robotics GmbH, Alle Rechte vorbehalten