Dr. Frank Stummer | Rhebo GmbH

IEC 62443 in der Praxis – Aufbau und Betrieb sicherer Steuerungstechnik mit intelligentem Netzwerkmonitoring

Beitrag auf dem Online-Event
IT-Security in der digitalisierten Produktion
Deutsche Messe Technology Academy
1. Juli 2020

IEC 62443: Industrial Communication Networks – Network and System Security

General

- 1-1 Terminology, Concepts and Models
- 1-2 Master Glossary of Terms and Abbreviations
- 1-3 System Security Compliance Metrics
- 1-4 IACS Security Lifecycle and Use-Case

Policies & Procedures

- 2-1 Requirements for an IACS Security Management System
- 2-2 Implementation Guidance for an IACS Security Management System
- 2-3 Patch Management in the IACS Environment
- 2-4 Security Program Requirements for IACS Service Providers

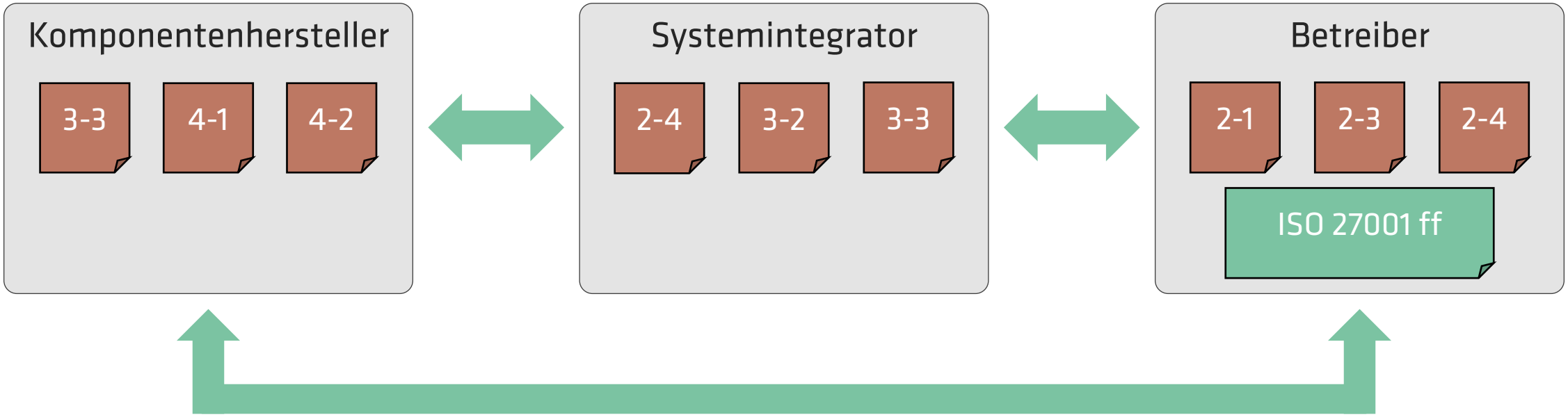
System

- 3-1 Security Technologies for IACS
- 3-2 Security Risk Assessment and System Design
- 3-3 System Security Requirements and Security Levels

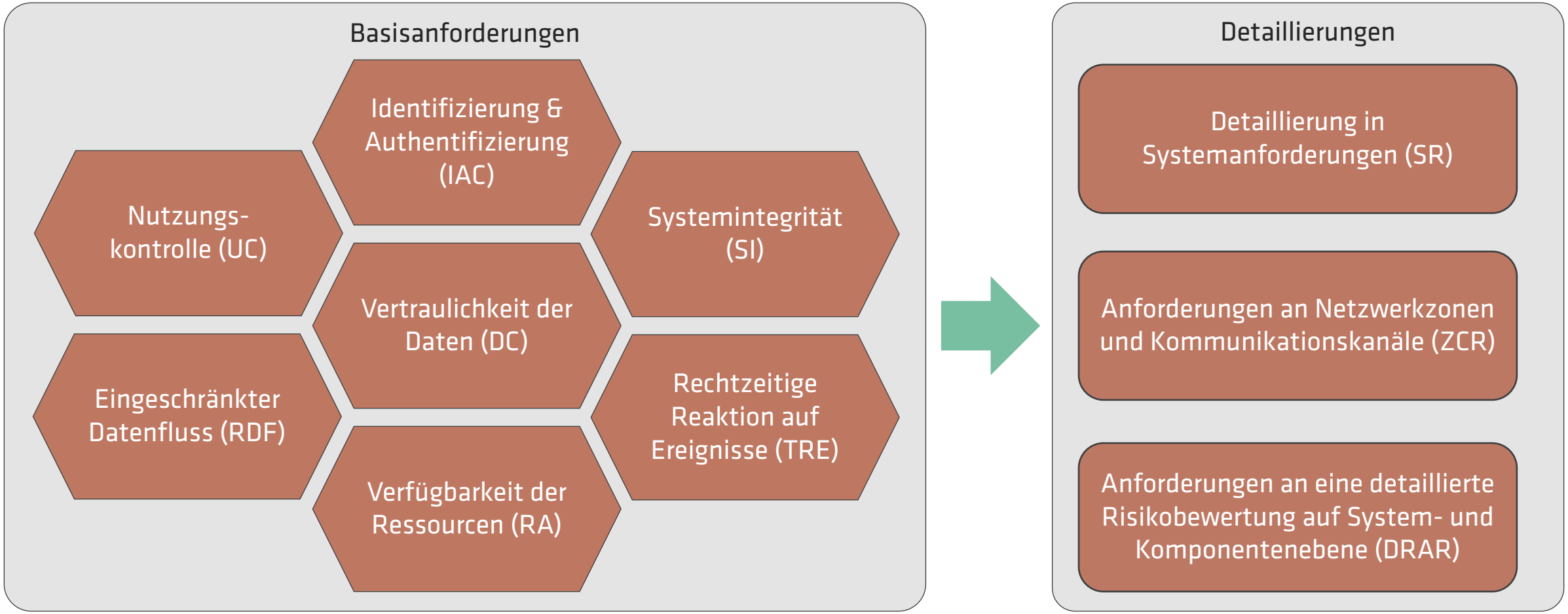
Component & Product

- 4-1 Secure Product Development Lifecycle Requirements
- 4-2 Technical Security Requirements for IACS Components

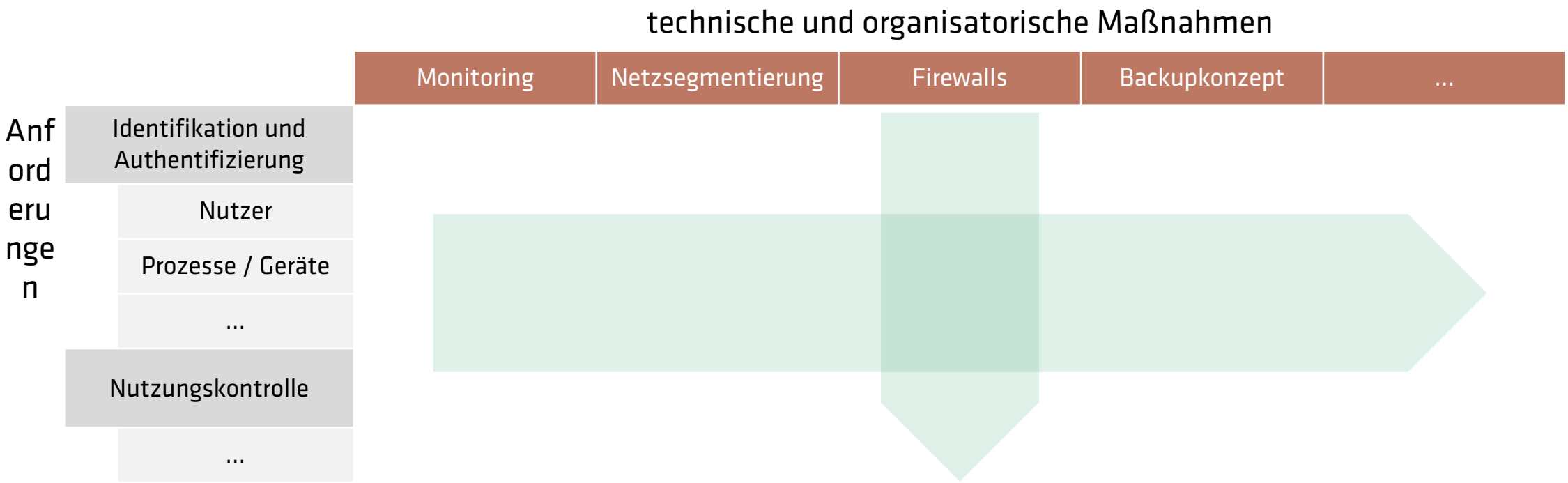
Zusammenspiel der Rollen im Security Lifecycle



Basisanforderungen (FR) und Detaillierungen



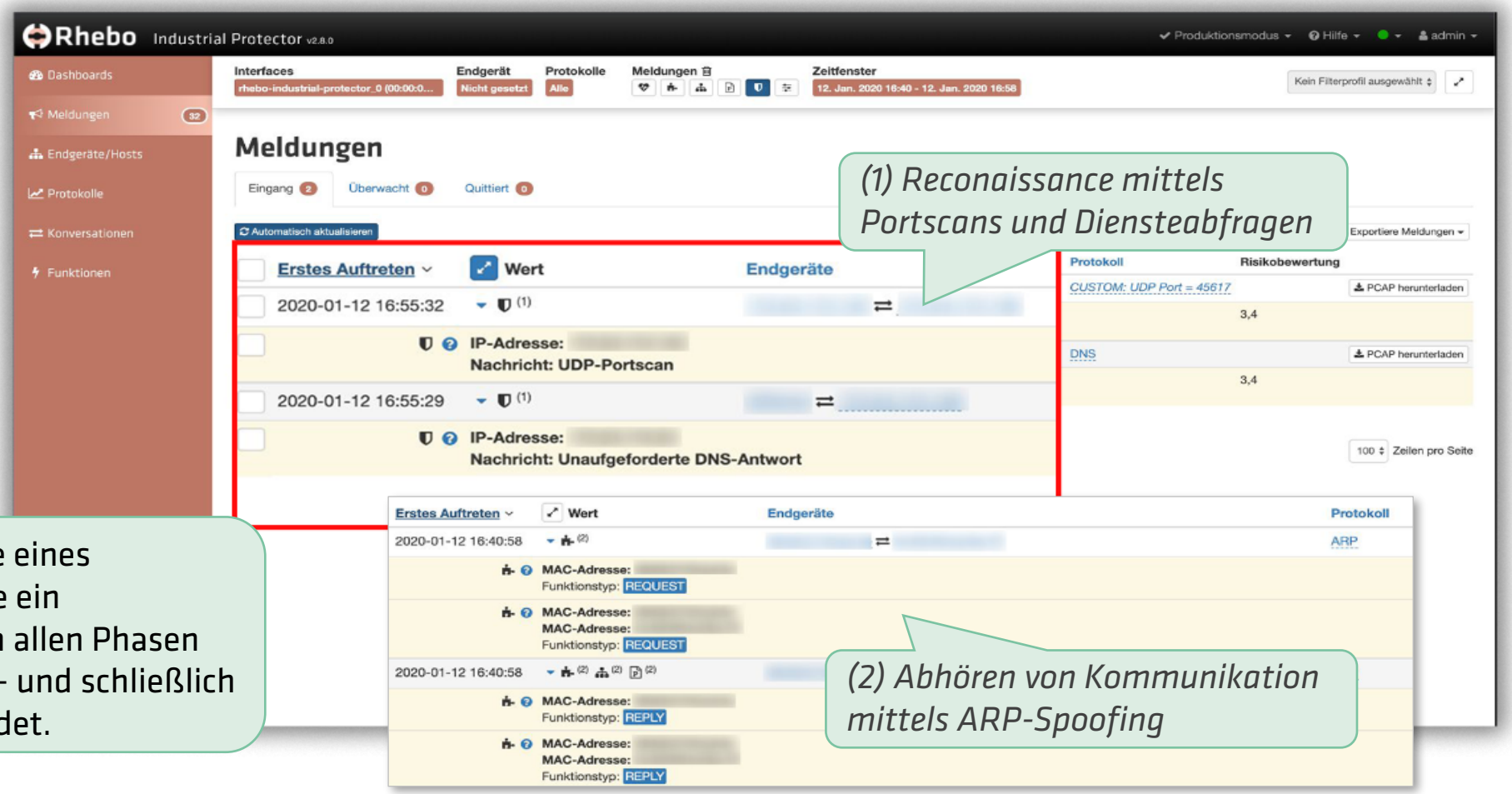
Mapping zwischen Anforderungen und Maßnahmen



Beispiel 1: Erkennung von Schadsoftware

Basisanforderung FR 3
Systemintegrität

Systemanforderung SR 3.2
Schutz vor Schadcode



(1) Reconaissance mittels Portscans und Diensteabfragen

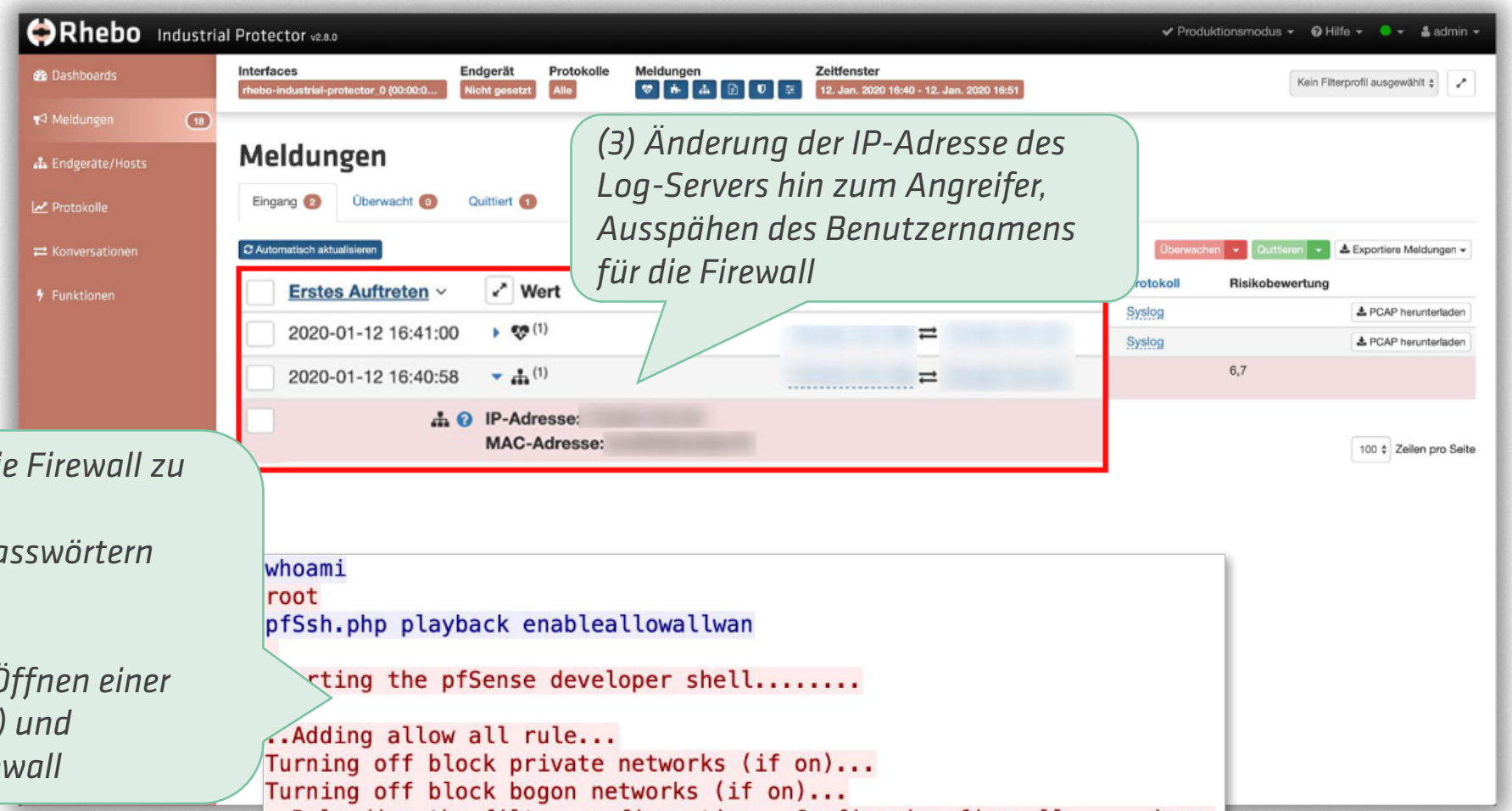
(2) Abhören von Kommunikation mittels ARP-Spoofing

In einer Produktionslinie eines Getränkeabfüllers wurde ein zielgerichteter Angriff in allen Phasen beobachtet, aufgeklärt – und schließlich ohne Schaden abgewendet.

weiter Beispiel 1: Erkennung von Schadsoftware

Basisanforderung FR 3
Systemintegrität

Systemanforderung SR 3.2
Schutz vor Schadcode



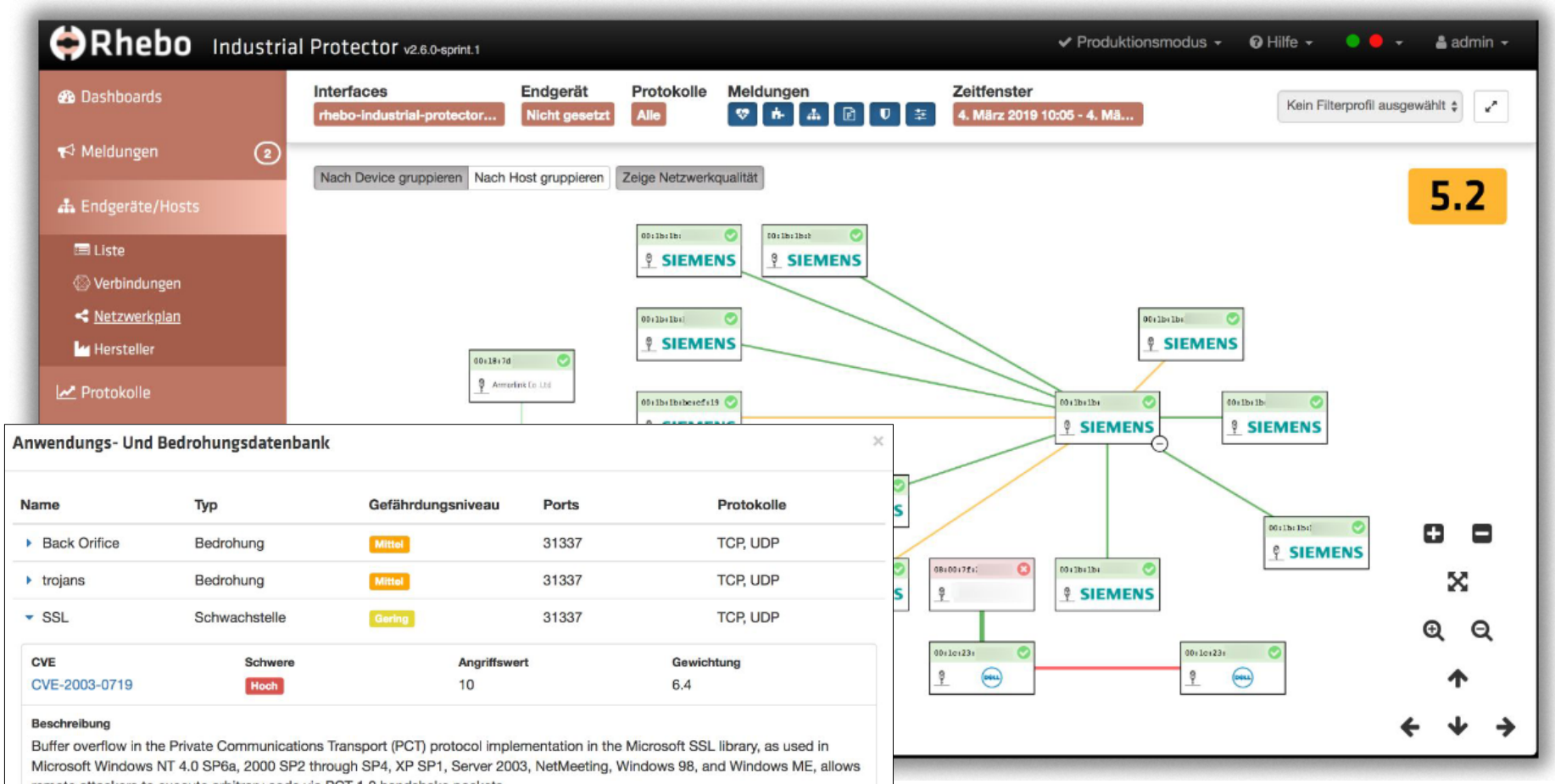
Beispiel 2: Monitoring des Netzwerkes und von Schwachstellen und Bedrohungen

Basisanforderung FR 3
Systemintegrität

Systemanforderung SR 3.2
Schutz vor Schadcode

Basisanforderung FR 5
eingeschränkter Datenfluss

Systemanforderung SR 5.1
Netzaufteilung

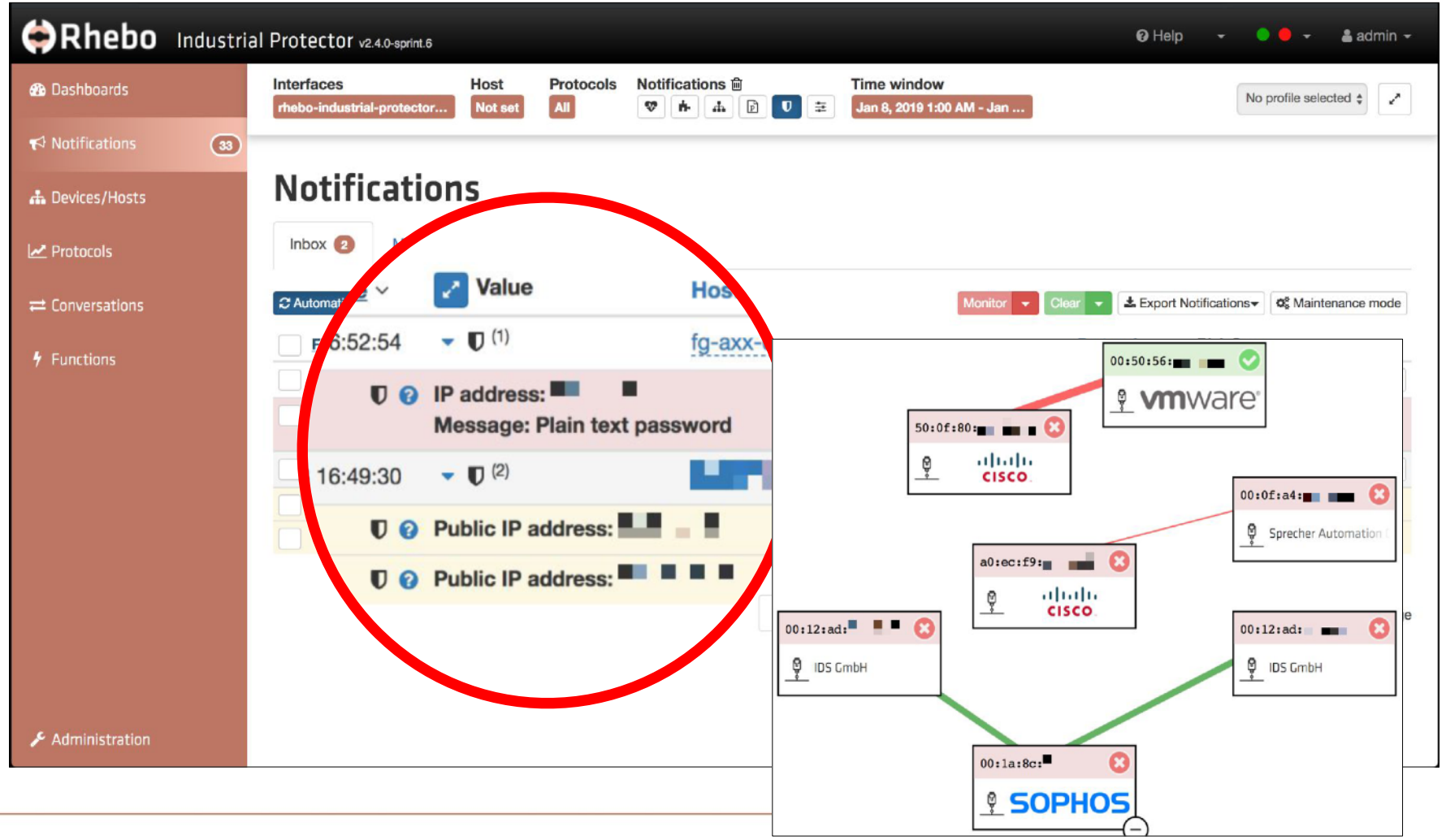


Beispiel 3: unsichere Kommunikation

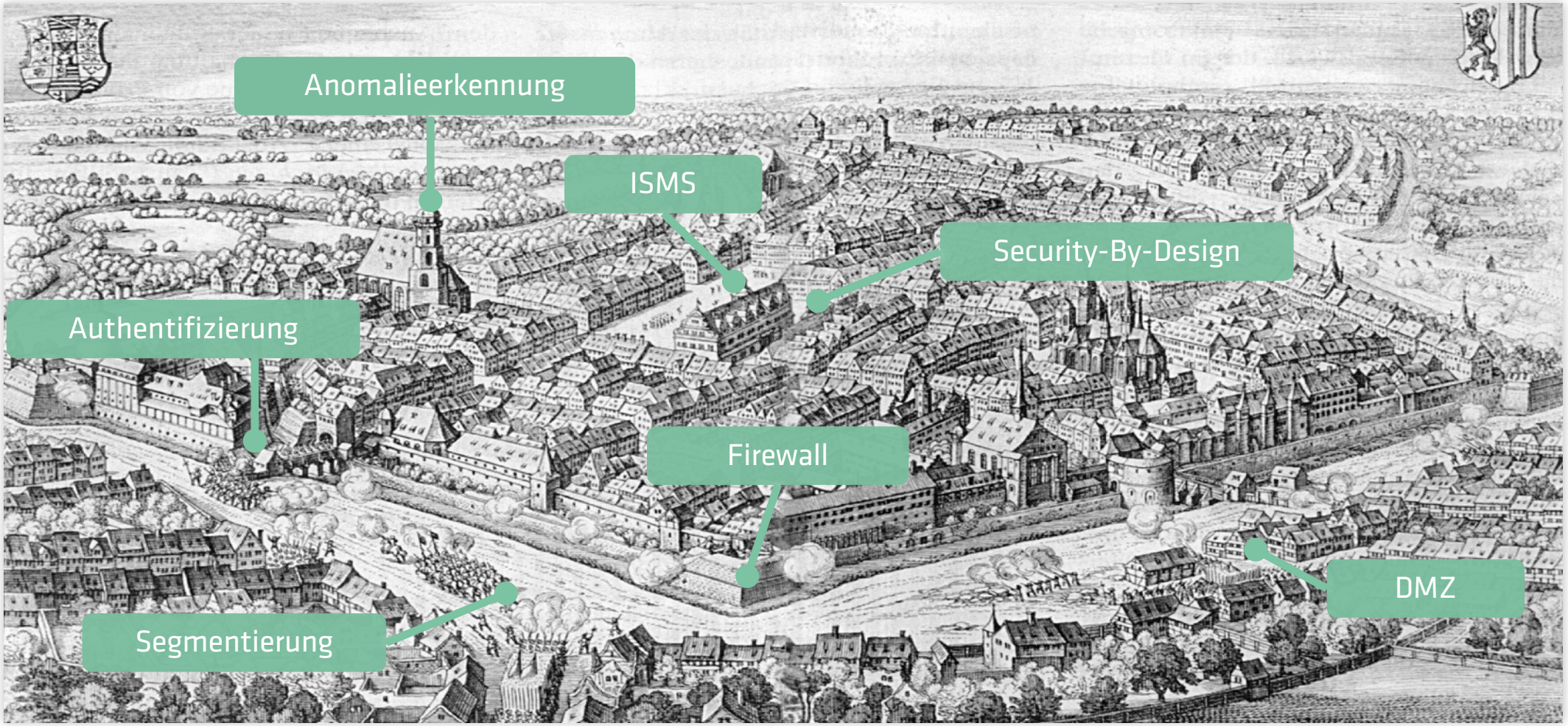
Basisanforderung FR 4
Vertraulichkeit

Systemanforderung SR 4.1
Vertraulichkeit der Informationen

Systemanforderung SR 4.3
Verwendung von Verschlüsselung



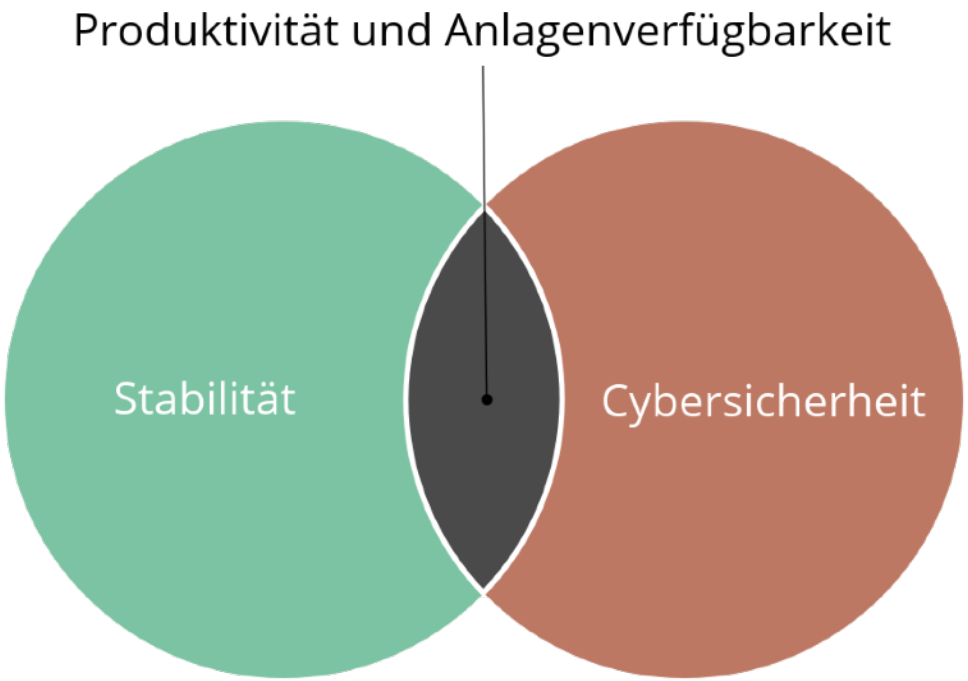
Gestaffelte Tiefenverteidigung (Defence in Depth)



Zeitiges Erkennen
von Gefahren

Reduzieren
von Ausfallzeiten

Vermeiden
von Ausfallkosten



Leitfaden „Die Norm IEC 62443 in der Praxis“

... und weiteres Material
(www.rhebo.com)

Kontaktdaten

Dr. Frank Stummer | Business Development
& Co-Founder

frank.stummer@rhebo.com

+49 176 31046145