

# 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

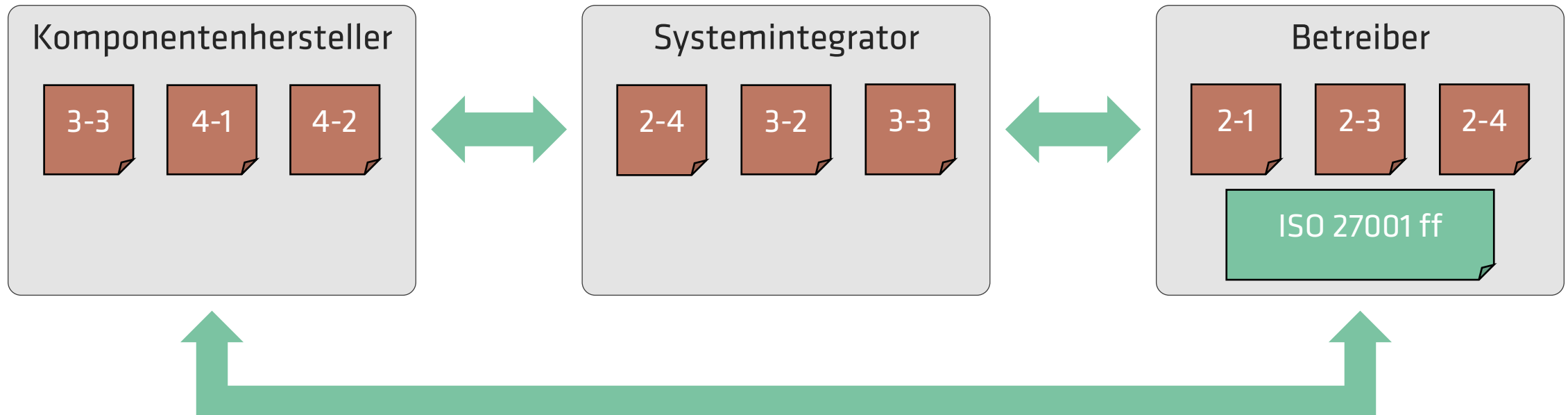
3-3  
System Security Requirements  
and Security Levels

## Component & Product

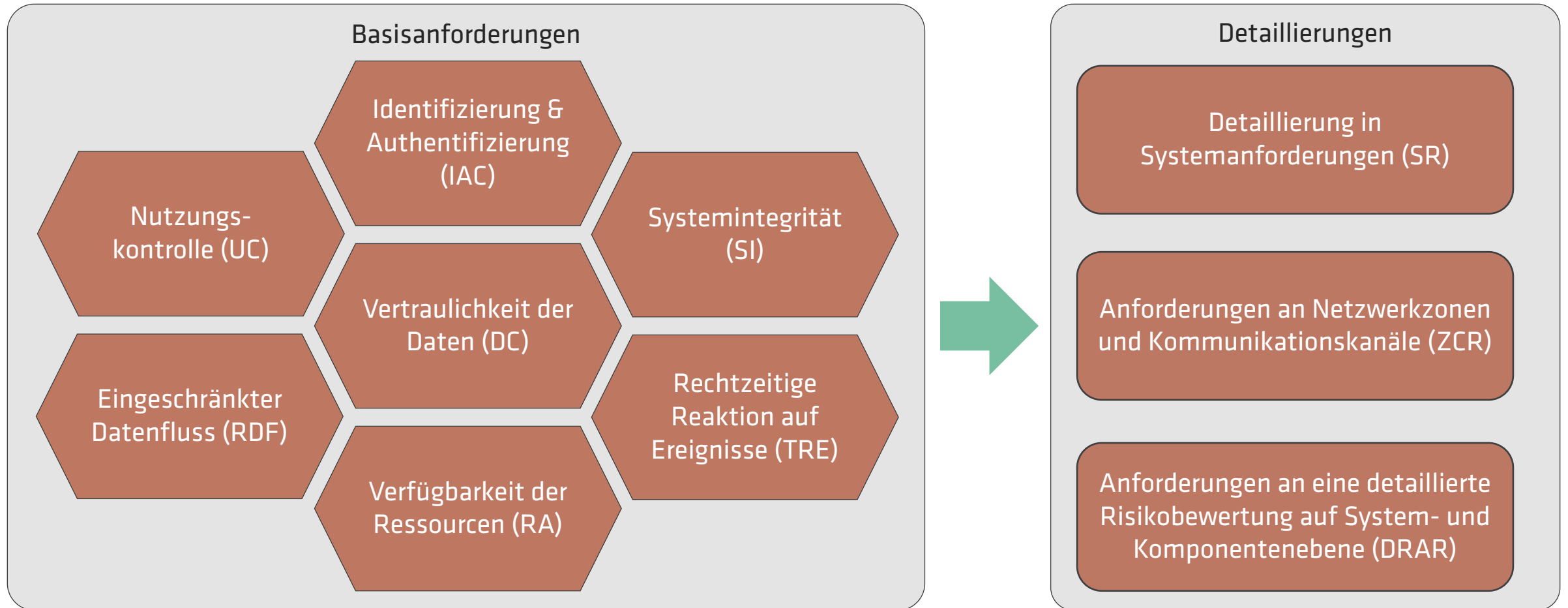
4-1  
Secure Product Development  
Lifecycle Requirements

4-2  
Technical Security  
Requirements for IACS  
Components

# Zusammenspiel der Rollen im Security Lifecycle

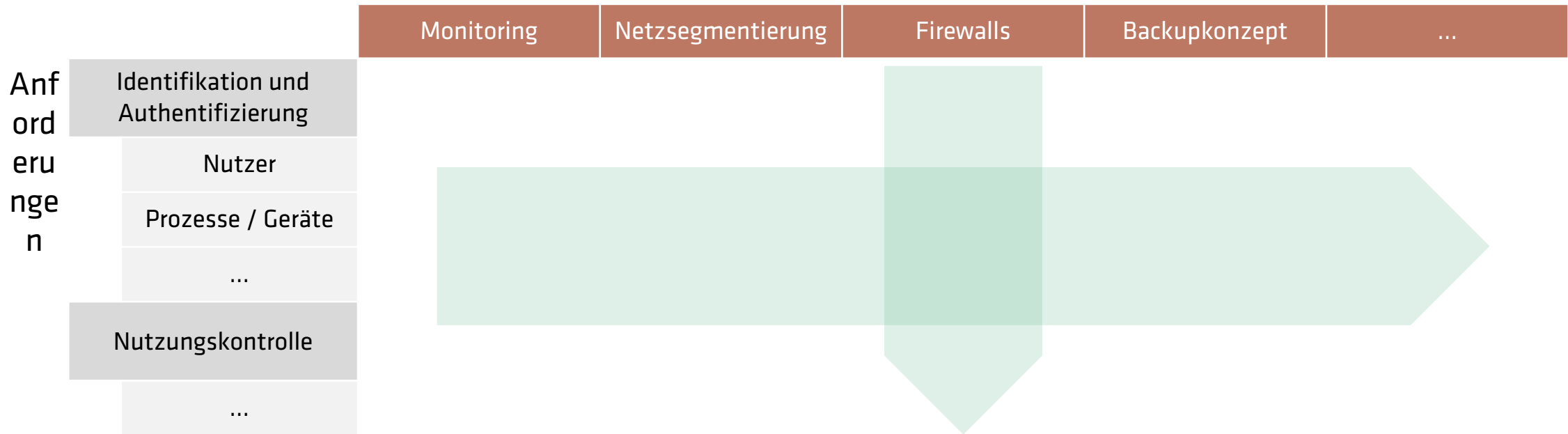


# Basisanforderungen (FR) und Detaillierungen



# Mapping zwischen Anforderungen und Maßnahmen

## technische und organisatorische Maßnahmen



# Beispiel 1: Erkennung von Schadsoftware

Basisanforderung FR 3  
Systemintegrität

Systemanforderung SR 3.2  
Schutz vor Schadcode

(1) Reconnaissance mittels Portscans und Dienstabfragen

(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

The screenshot shows the Rhebo Industrial Protector v2.8.0 web interface. The main content area displays a list of alerts (Meldungen) with columns for 'Erstes Auftreten', 'Wert', 'Protokoll', and 'Risikobewertung'. A red box highlights a specific alert entry for '2020-01-12 16:40:58'. A green callout bubble points to this entry with the text: *(3) Änderung der IP-Adresse des Log-Servers hin zum Angreifer, Ausspähen des Benutzernamens für die Firewall*. Below the alert list, a terminal window shows system logs with the following text: `whoami`, `root`, `pfSsh.php playback enableallowallwan`, `Starting the pfSense developer shell.....`, `..Adding allow all rule...`, `Turning off block private networks (if on)...`, `Turning off block bogon networks (if on)...`, and `..Reloading the filter configuration...Configuring firewall.....done.`

*(4) Verschiedene Versuche, die Firewall zu übernehmen:*

- *Bruteforce mit Default-Passwörtern (erfolglos)*
- *SQL-Injection (erfolglos)*
- *Sicherheitslücke erlaubt Öffnen einer Reverse Shell (erfolgreich) und Umkonfiguration der Firewall*

# 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

**Anwendungs- Und Bedrohungsdatenbank**

Name	Typ	Gefährdungsniveau	Ports	Protokolle
Back Orifice	Bedrohung	Mittel	31337	TCP, UDP
trojans	Bedrohung	Mittel	31337	TCP, UDP
SSL	Schwachstelle	Gering	31337	TCP, UDP

CVE	Schwere	Angriffswert	Gewichtung
CVE-2003-0719	Hoch	10	6.4

**Beschreibung**  
Buffer overflow in the Private Communications Transport (PCT) protocol implementation in the Microsoft SSL library, as used in Microsoft Windows NT 4.0 SP6a, 2000 SP2 through SP4, XP SP1, Server 2003, NetMeeting, Windows 98, and Windows ME, allows remote attackers to execute arbitrary code via PCT 1.0 handshake packets.

aMSN	Schwachstelle	Gering	31337	TCP, UDP
.Net Remoting	Anwendung	Keines	31337	TCP, UDP
Terraria	Anwendung	Keines	31337	TCP, UDP



# Beispiel 3: unsichere Kommunikation

Basisanforderung FR 4  
Vertraulichkeit

Systemanforderung SR 4.1  
Vertraulichkeit der Informationen

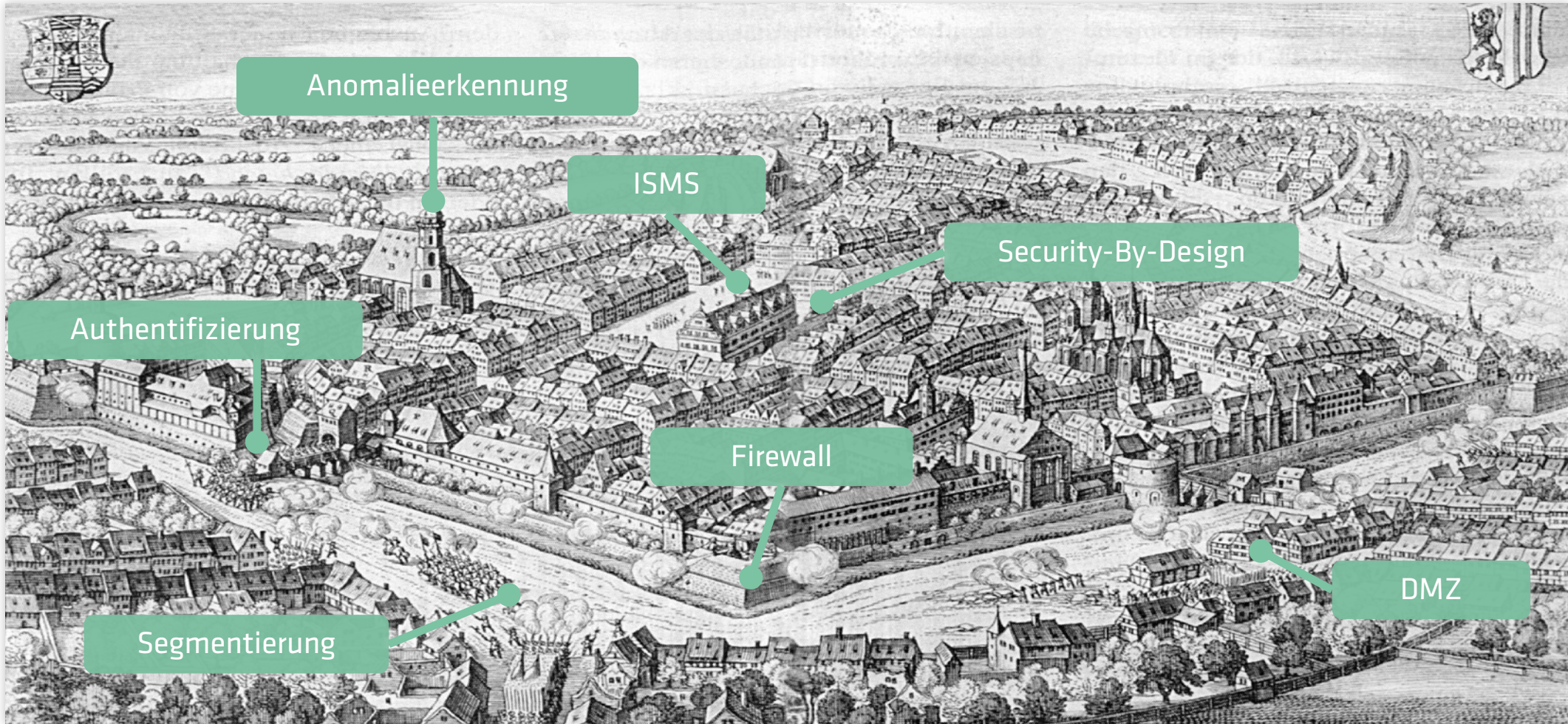
Systemanforderung SR 4.3  
Verwendung von Verschlüsselung

The screenshot displays the Rhebo Industrial Protector v2.4.0-sprint.6 interface. The left sidebar contains navigation options: Dashboards, Notifications (33), Devices/Hosts, Protocols, Conversations, Functions, and Administration. The main content area shows a 'Notifications' section with a table of alerts. A red circle highlights a notification with the following details:

Time	Value	Host
16:52:54	IP address: [redacted]	fg-axx-
	Message: Plain text password	
16:49:30	Public IP address: [redacted]	
	Public IP address: [redacted]	

Below the notification table, a network diagram is visible, showing several devices connected to a central 'SOPHOS' device. The devices include 'vmware', 'Sprecher Automation', and two 'IDS GmbH' devices. The diagram uses colored lines (green and red) to represent connections between the devices.

# Gestaffelte Tiefenverteidigung (Defence in Depth)





**Zeitiges Erkennen**  
von Gefahren



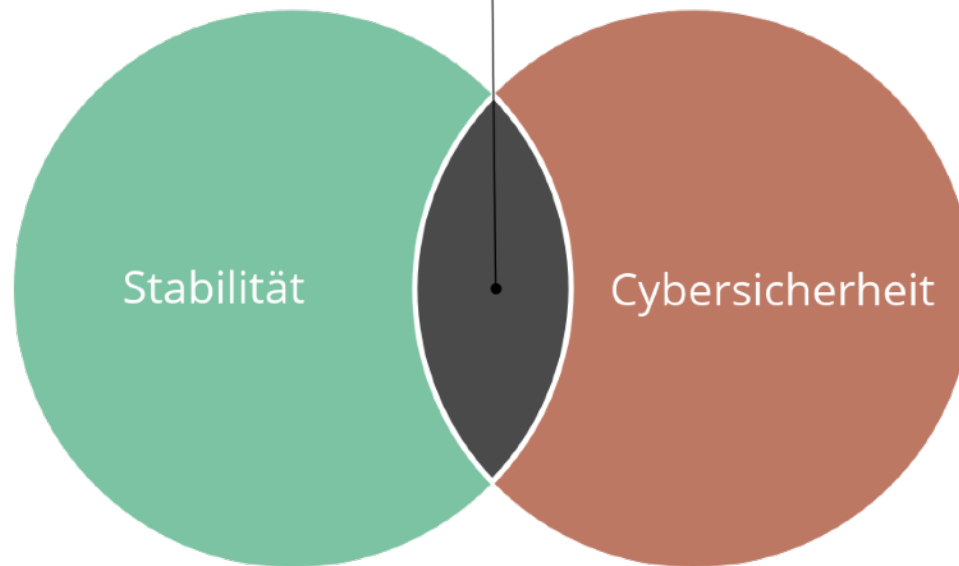
**Reduzieren**  
von Ausfallzeiten



**Vermeiden**  
von Ausfallkosten

---

Produktivität und Anlagenverfügbarkeit





Leitfaden „Die Norm IEC 62443 in der Praxis“

... und weiteres Material  
([www.rhebo.com](http://www.rhebo.com))

# Kontakt Daten



Dr. Frank Stummer | Business Development  
& Co-Founder

 frank.stummer@rhebo.com

 +49 176 31046145