

Informationssicherheit in der Automation – ein Überblick

Martin Naedele
ABB Corporate Research



Überblick

Motivation

- Was ist Informationssicherheit?
- Warum ist das Thema relevant für industrielle Anlagen?

Realisierung

- Sicherheitsarchitekturen und -mechanismen
- Realisierungsbeispiel
- Richtlinien und Normen

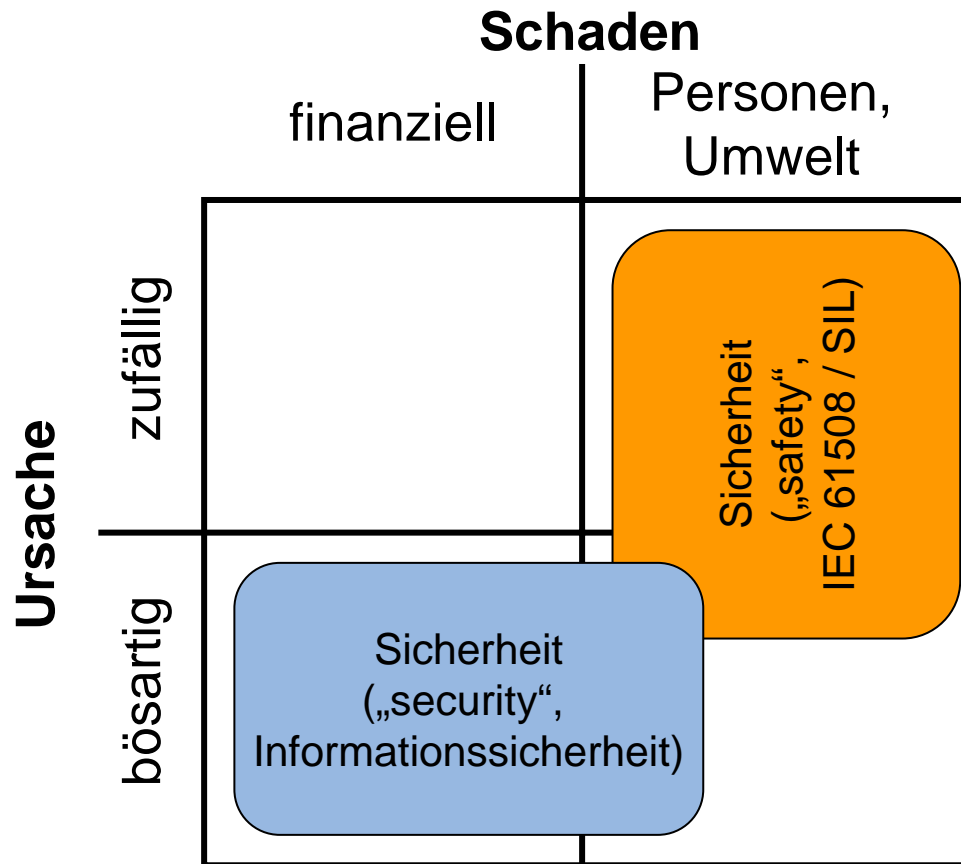


Motivation



Was ist Informationssicherheit?

- Sicherheit (safety) und Sicherheit (security)



Was ist Informationssicherheit?

Sicherheitsanforderungen an ein System können mittels acht generischer **Sicherheitsziele** beschrieben werden:

■ Vertraulichkeit

Confidentiality

■ **Lawsuit Alleges Kraft Foods Sent Spam (22 April 2005)**

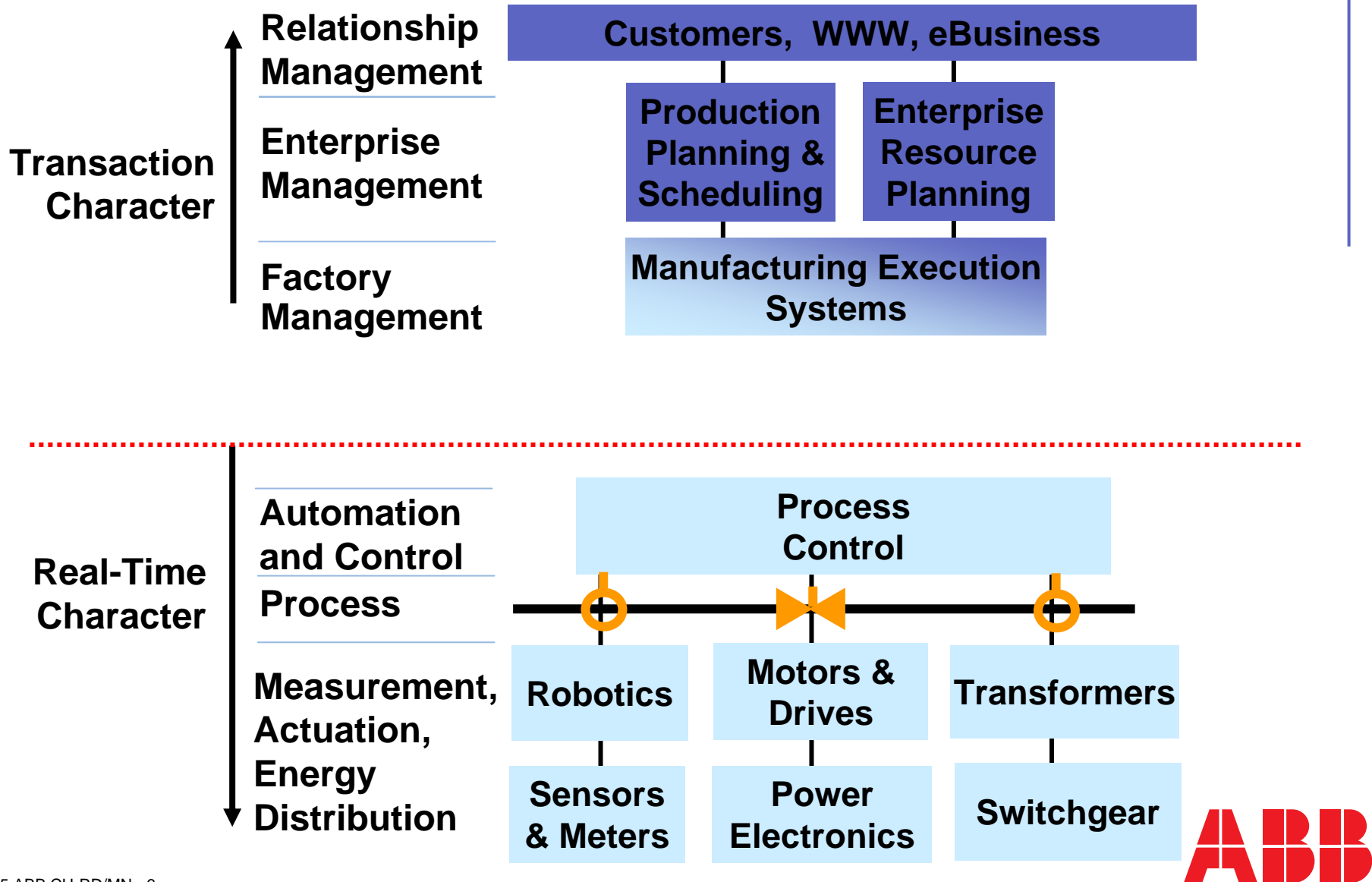
■ The founder of a small California ISP has filed a lawsuit
■ against **Kraft Foods**, Inc., alleging the company is
■ responsible for 8,500 spam email messages in violation of
■ both the federal CAN-SPAM Act and California anti-spam law;
■ the headers of the unsolicited commercial email messages
■ were faked. The attorney representing the man who filed the
■ suit says his client is entitled to **US\$11.7 million in damages.**

■ Schutz Dritter

Third party protection

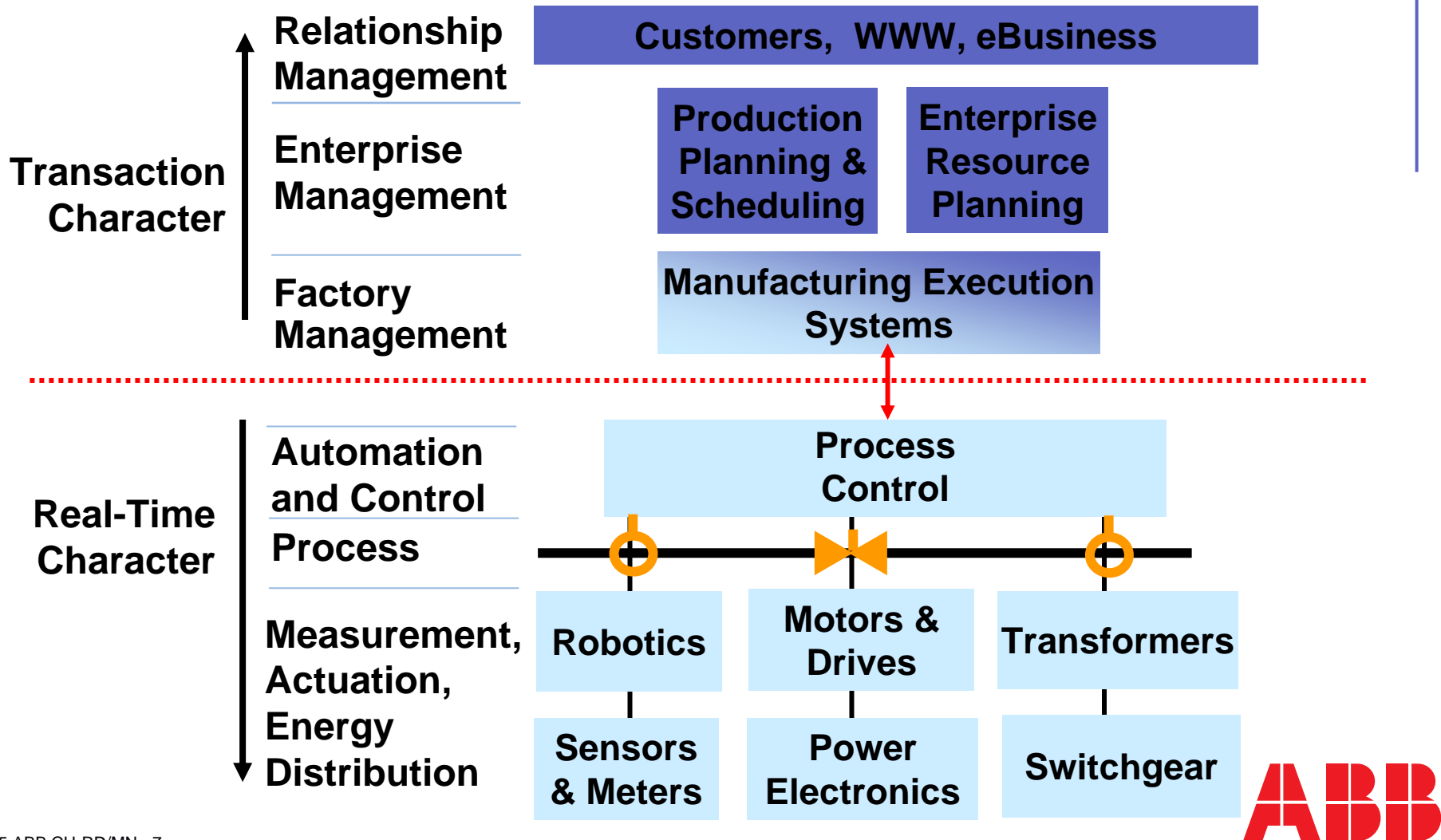


Motivation



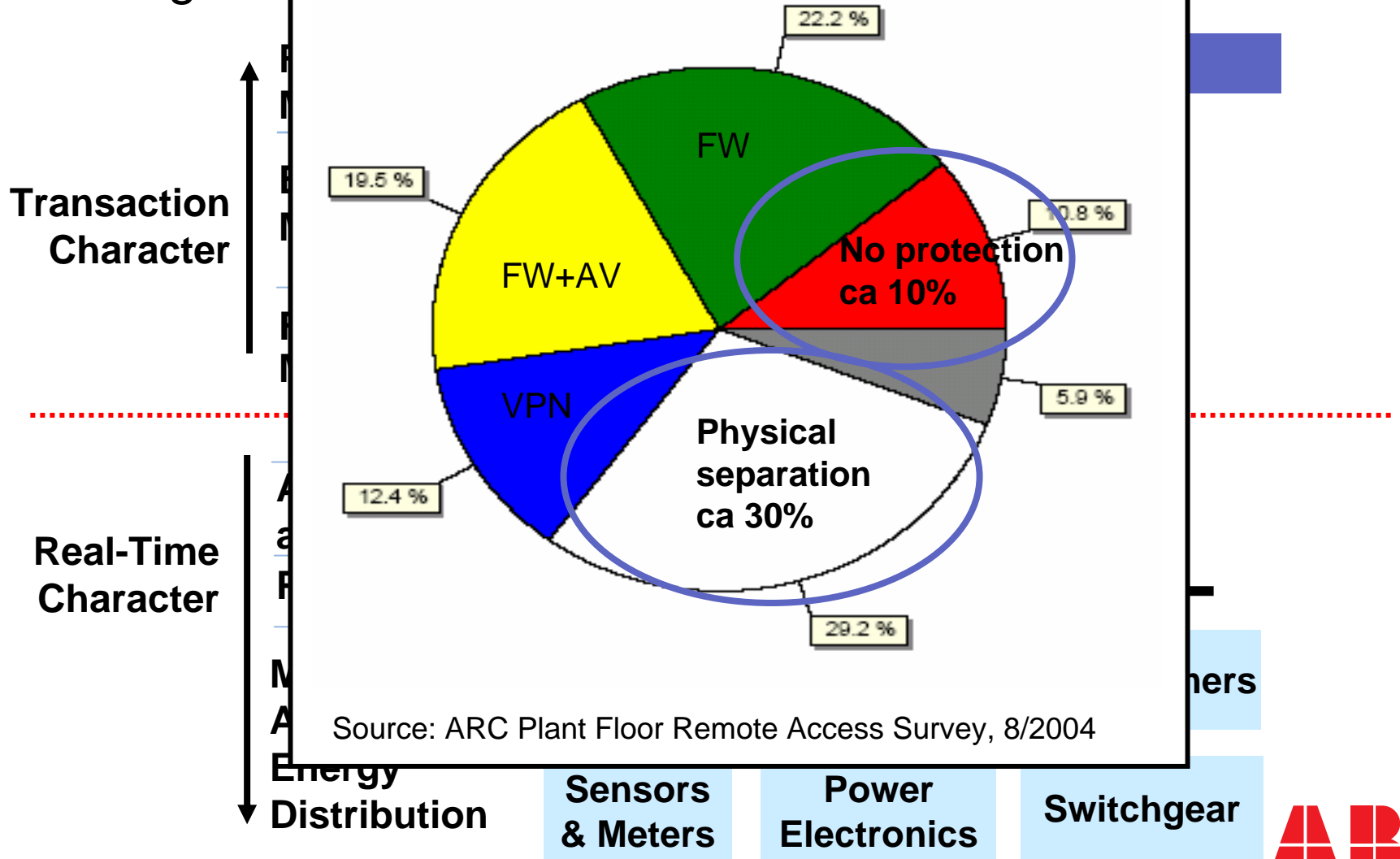
Motivation

- Integration: “device to enterprise”, “sensor to board room”



Motivation

- Integration: “device to enterprise” “control room”



Motivation

The Guardian
UK news

Hacker attack left port in chaos

Busiest US port hit after Dorset teenager allegedly launched electronic s

Rebecca All
Tuesday Oc
The Guardia

A lovesick ha
launching a d
made anti-Ar

Aaron Caffre
halt at the Po
Shaftesbury,
attack to disa

Search this site

Go

Click here

Computer Virus Strikes CSX Transportation Computers

Freight and Commuter Service Affected

tion technology systems
rly today after a computer virus
believed to be a worm virus
systems of other major
ys.

of major applications, including
result, passenger and freight
cluding the morning commuter
ington, D.C., area. Contrary to

Sasser eyed over train outage

Chris Jenkins

MAY 03, 2004

NSW TRAINS authority RailCorp has sent in software engineers to find the source of the outage that left up to 300,000 commuters stranded yesterday, saying the new Sasser worm, which has already spawned two variants, is being evaluated as a possible cause.

A RailCorp spokesman confirmed that software engineers were investigating the problem, which prevented drivers from talking to signal boxes. A virus attack was one possibility being investigated, he said. RailCorp was unable to confirm when the investigation would be complete.

RailCorp chief executive Vince Graham raised the possibility of a virus attack at a press briefing yesterday. "There is no evidence that hacking is an issue here, the viral infection could have been introduced by one of our own people not taking sufficient care," Sydney's *Daily Telegraph* reported

Register

SECURITYFOCUS NEWS

Slammer worm crashed Ohio nuke plant network

By Kevin Poulsen, SecurityFocus Aug 19 2003 2:45PM

The Slammer worm penetrated a private computer network at Ohio's Davis-Besse power plant in January and disabled a safety monitoring system for nearly five ho despite a belief by plant personnel that the network was protected by a firewall, SecurityFocus has learned.

Hacker jailed for revenge sewage attacks

By Tony Smith

Posted: 31/10/2001 at 15:55 GMT

The Register Mobile: Find out what the fuss is about. Take the two week trial today.

An Australian man was today sent to prison for two years after he was found guilty of hacking into the Maroochy Shire, Queensland computerised waste management system and caused millions of litres of raw sewage to spill out into local parks, rivers and even the grounds of a Hvatt

Realisierung



Sicherheitsmechanismen

- Vertraulichkeit Verschlüsselung, VPN
- Integrität kryptographische Prüfsummen
- Verfügbarkeit Redundanz
- Authentifizierung Passwörter, Zertifikate, Biometrie
- Zugangskontrolle “gehärtete” Rechner, Zugriffsrechte, Firewall, AV, Filter/Proxy
- Nachvollziehbarkeit Logs, IDS
- Nachweisbarkeit digitale Signatur
- Schutz Dritter Firewall, AV

Sicherheitsarchitektur

Grundgleichung:

$$d_{\text{Abwehr}} \stackrel{!}{\geq} d_{\text{Erkennung}} + d_{\text{Reaktion}}$$

[nach W. Schwartau]

Basisarchitekturtypen:



Harte Schale

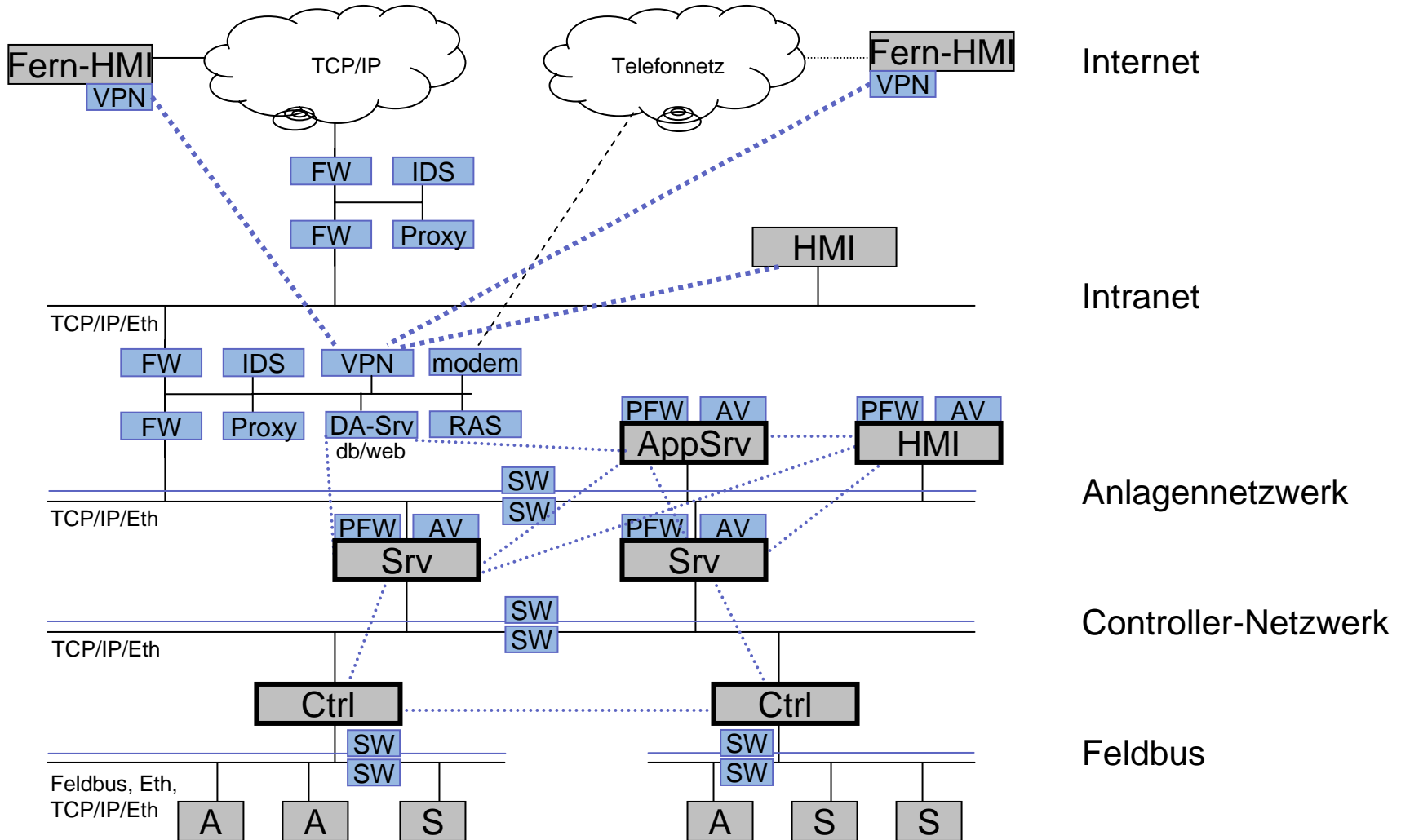
“Unüberwindbare” Mauer, dahinter keine Kontrollen.

Tiefengestaffelte Verteidigung

Für jeden Übergang zwischen zwei Zonen muss der Angreifer Zeit und Mühe aufwenden.



Sicherheitsmechanismen in der Leittechnik



Richtlinien und Normen

■ Ziele

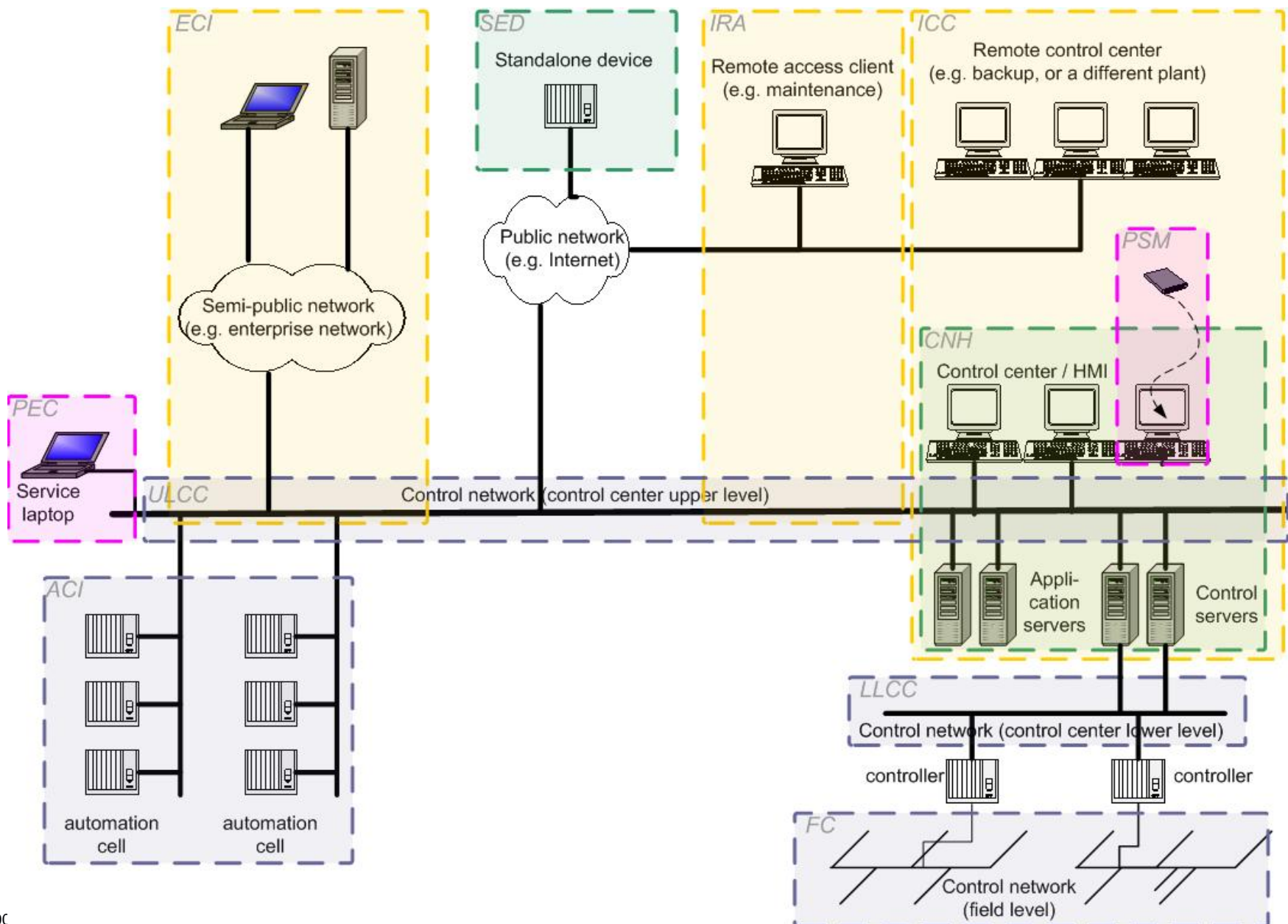
- Konkrete Hilfestellung bei der Sicherung einer Anlage
- Keine zusätzlichen Herstellungs- oder Beschaffungskosten ohne klaren Sicherheitsgewinn

■ Initiativen

- IAONA „Security Data Sheet“ -> Produkte
- ISA sp99 -> Prozesse
 - TR1/TR2 (2004); standard S99 (2006-8?)
- IEC TC65 WG? (ehemals SC65c/WG13) -> Systeme (techn.)
 - Standards IEC ??? (2007) and IEC 61784-4 (2007)



IEC 61xxx - Anforderungskataloge



Zusammenfassung

- Die Gefahr elektronischer Angriffe auf industrielle Leitsysteme ist real.
 - Das Risiko ist heute mit kommerziell verfügbaren Sicherheitsmechanismen recht gut beherrschbar
 - Mehrlagige Verteidigung
 - Normen und Richtlinien werden langsam verfügbar
- allerdings
- Aufwand, Kosten in Installation und Betrieb



ABB



ABB