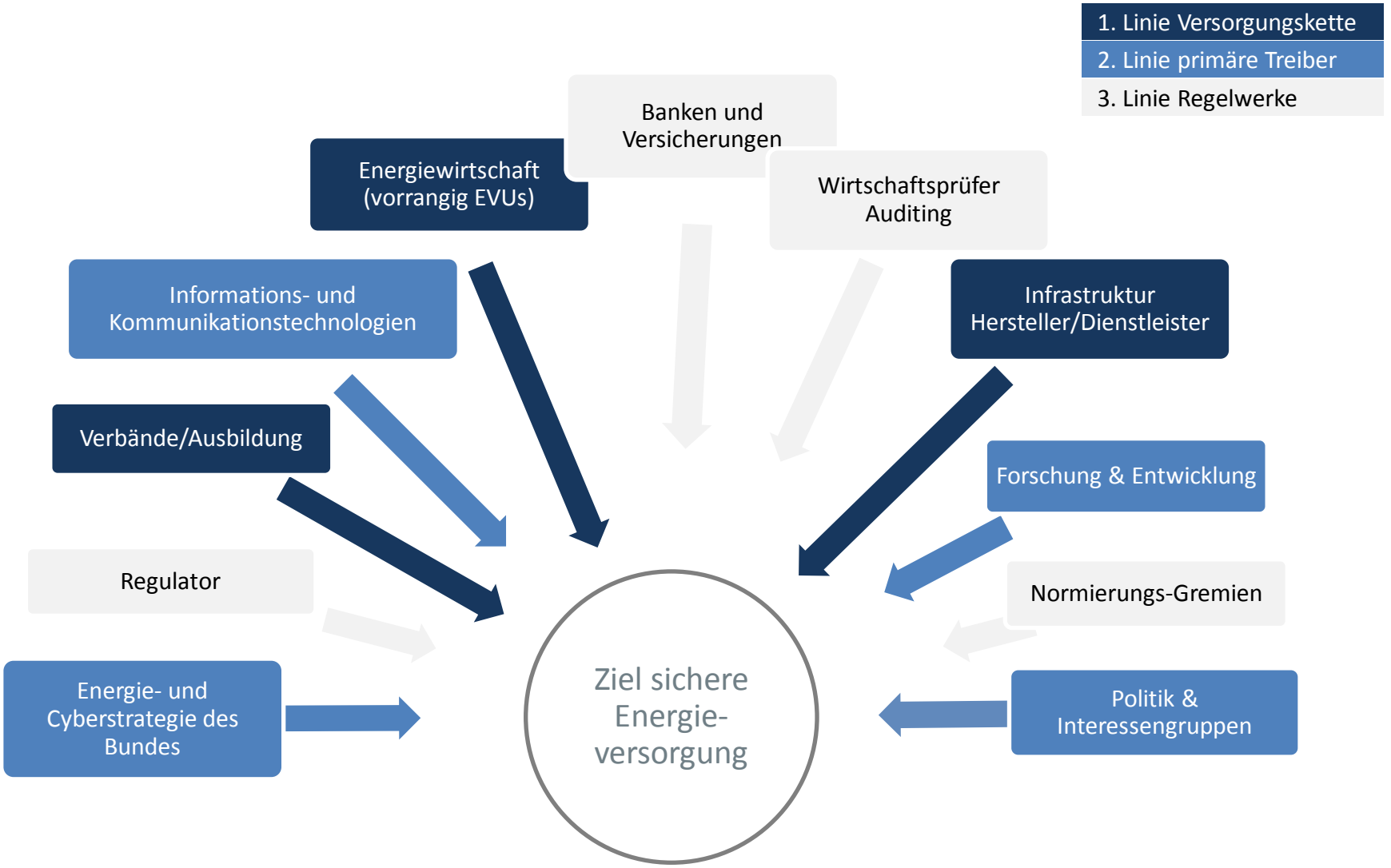
Industrial IT Security

"Herausforderung im 21. Jahrhundert"
Cyber Security in kritischen Energie-Infrastrukturen

KORAMIS

Träger der Energiezukunft

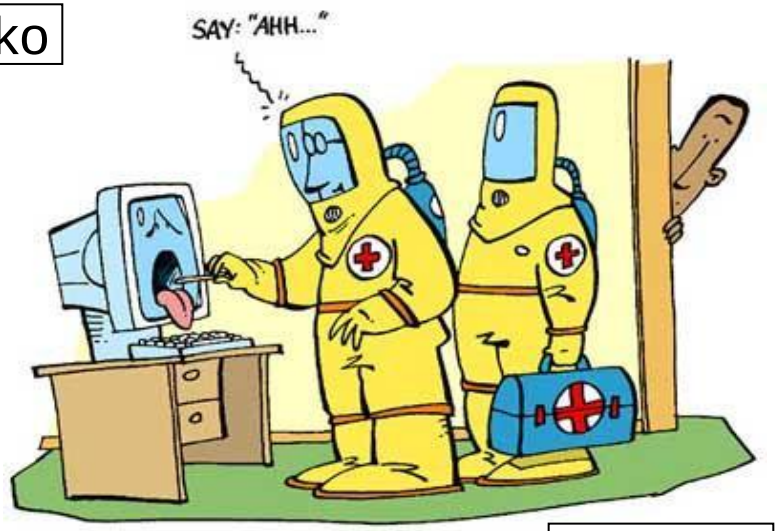


KORAMIS

…die Zukunft ist vernetzt…

…und das Netz schlägt zurück…

Nur Risiko



Konkret

Abstrakt

Chance & Risiko

wer ist denn gerade **online**…

SHODAN

port:161 simatic country:DE

Search

Home | Search Directory | Data Analytics/ Exports | Developer Center | Labs

Add to Directory | Export Data

84.171.106.175

Added on 29.06.2010

Sterbfritz

Details

p54AB6AAF.dip.t-dialin.net

Siemens, SIMATIC HMI, MP377, 6AV6 644-0AB01-2AX0, HW: 0, SW: V 1 0 3

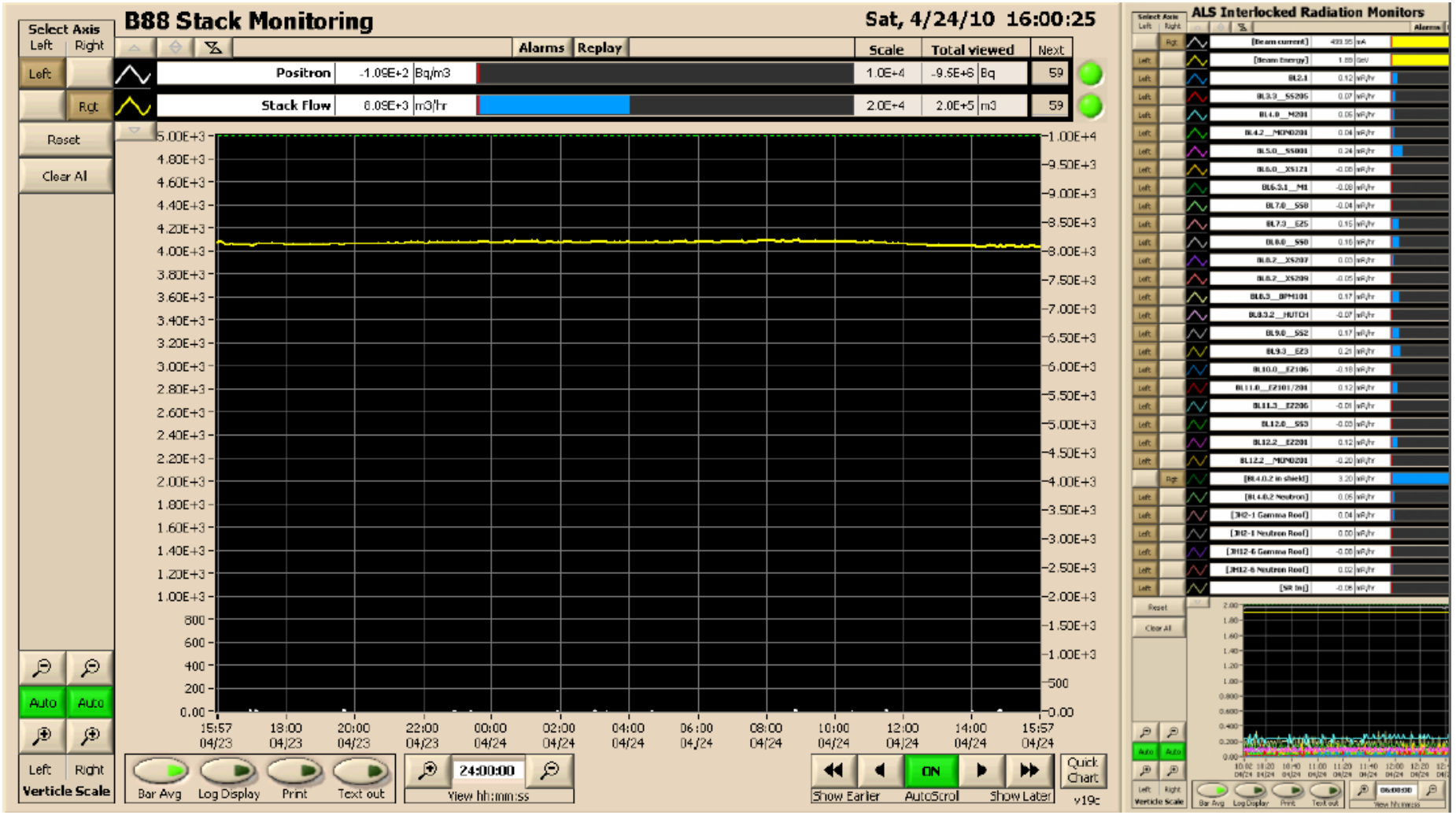
84.171.106.157

Added on 29.06.2010

Sterbfritz

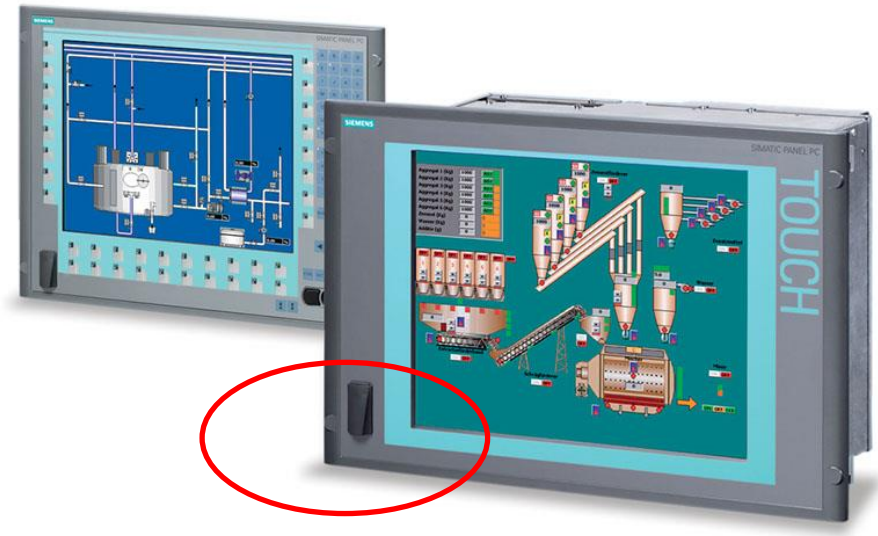
Details

p54AB6A9D.dip.t-dialin.net


B88 Stack Monitoring
Sat, 4/24/10 16:00:25
Select Axis
Left
Right
Reset
Clear Al
Alarms
Replay
Scale
Total viewed
Next
Positron
-1.09E+2
Bq/m3
1.0E+4
-9.5E+8
Bq
59
Stack Flow
6.09E+3
m3/hr
2.0E+4
2.0E+5
m3
59
Auto
Verticle Scale
Bar Avg
Log Display
Print
Text out
24:00:00
View hh:mm:ss
Show Earlier
AutoScrol
ON
Show Later
Quick Chart
v19c
ALS Interlocked Radiation Monitors

Nie mehr das Passwort vergessen…

USB Schnittstellen **verschlossen** und **geschützt…**



Sicherheitslücken: US-Experten kämpfen mit Computerviren in Kraftwerken

Verseuchte USB-Sticks und schwache Passwörter: Selbst kritische Infrastruktur ist nicht sicher vor banalen Webgefahren. Das zeigt ein neuer Sicherheitsbericht des amerikanischen ICS-Cert für Cyber-Vorfälle in Industrieanlagen. Die Experten fanden Viren in Kraftwerken.

…**und darum herum** - **neue** Marktentwicklung mit **Angriff** auf Bestellung…

RUGGEDCOM
INDUSTRIAL STRENGTH NETWORKS™

"An undocumented backdoor account exists within all released versions of RuggedCom's Rugged Operating System (ROS®). The username for the account, which cannot be disabled, is "factory" and its password is dynamically generated based on the device's MAC address."

- Justin Clarke

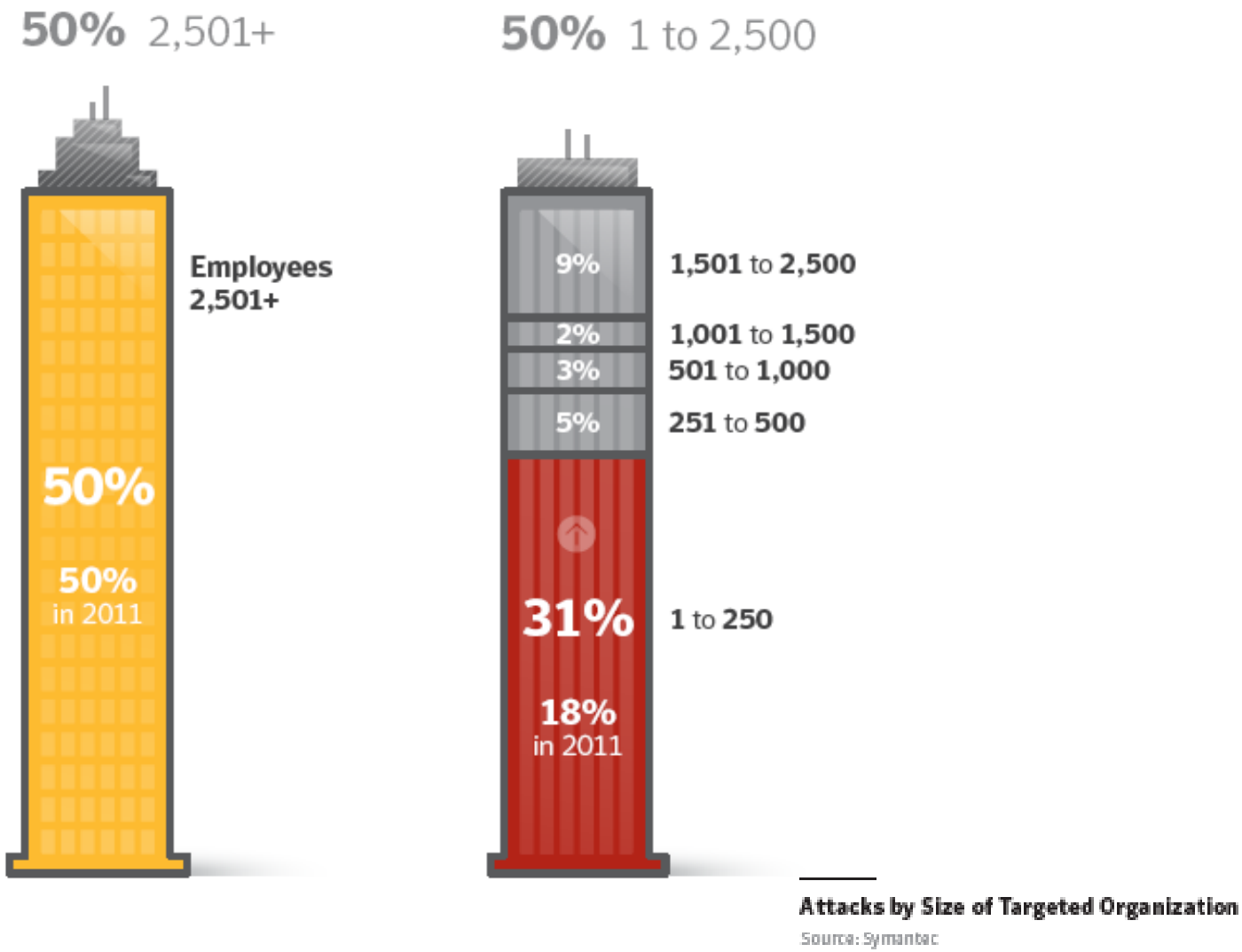
DEL	QTY	UNIT PRICE (Euros)	LINE TOTAL (Euros)
L	1	188,549.00	188,549.00
ML			
L			

Siemens Simatic S7 PLC Exploitation

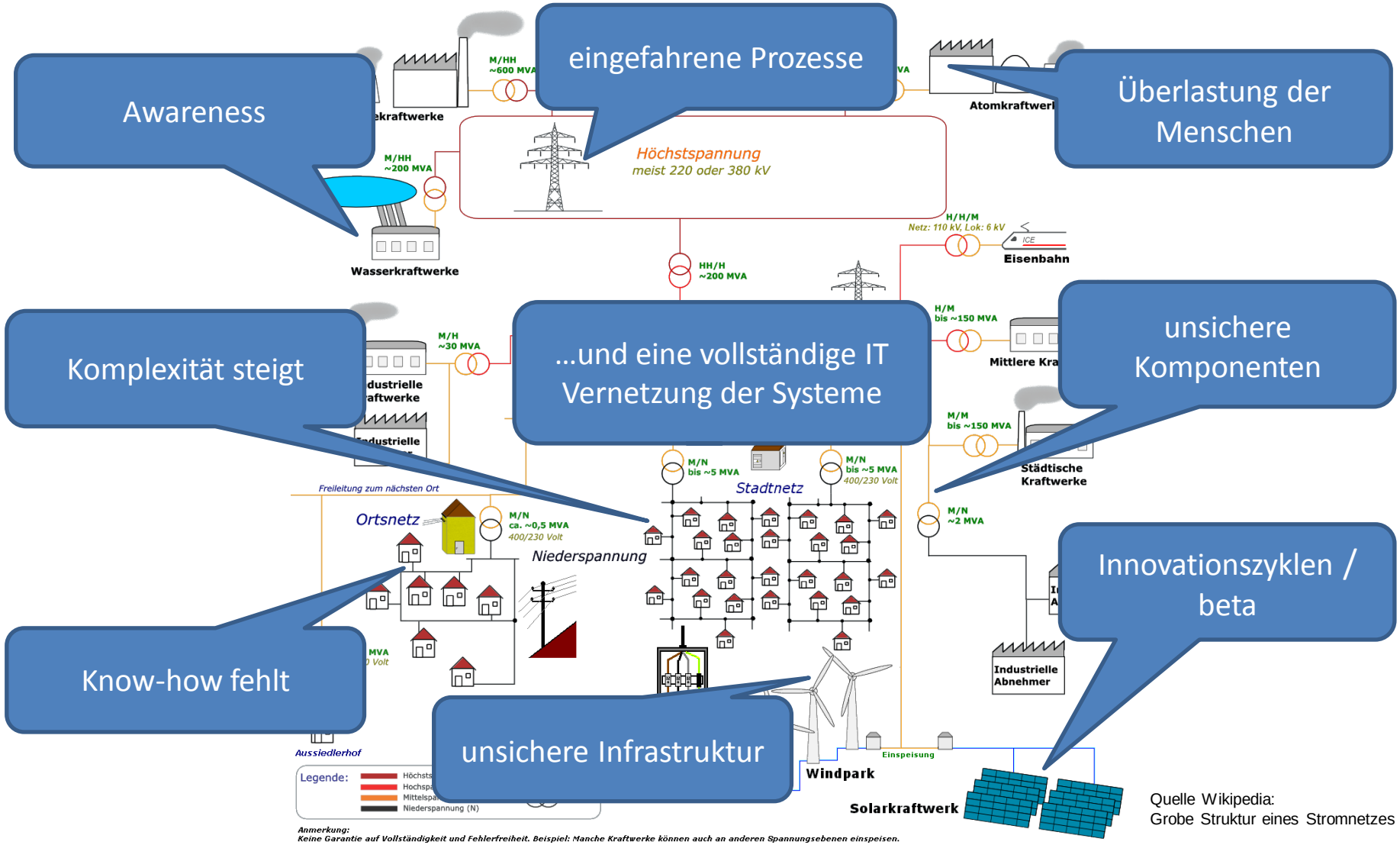
S7-Fu (功夫) with Rapid7 Metasploit
Black Hat USA+2011

	Name	Description	Link
June 10, 2011	ICS-Alert-11-161-01, Siemens SIMATIC S7-1200 PLC Vulnerabilities	This public alert confirms the report of vulnerabilities affecting the S7-1200 and includes information on how to obtain the patch developed by Siemens.	Link
July 5, 2011	ICS-Alert -11-186-01, Password Protection Vulnerability in Siemens SIMATIC Controllers S7-200, S7-300, S7-400, S7-1200.	This public alert confirms that a portion of the vulnerabilities affecting the Siemens SIMATIC S7-1200 (ICS-Alert-11-161-01) also affect other models in the S7 product line.	Link
July 23, 2011	ICS-ALERT-11-204-01, S7-300 S7-400 Hardcoded Credentials	This public alert warns of an unanticipated, publicly disclosed vulnerability. An updated ALERT was subsequently released to clarify products affected (ICS-ALERT-11-204-01A) following ICS-CERT and Siemens analysis.	Link
July 29, 2011	ICS-ALERT-11-204-01A, (UPDATE A) S7-300 Hardcoded Credentials"	This alert updates ICS-ALERT-11-204-01 and contains the known affected products following ICS-CERT and Siemens analysis.	Link
August 3, 2011	ICS-ALERT-11-204-01B, (UPDATE B) S7-300 Hardcoded Credentials	This update alert warns of the public release of hardcoded credentials affecting certain Siemens S7-300 PLCs.	Link

Wen trifft es denn…



Aspekte der IT Security haben sich dramatisch verändert…



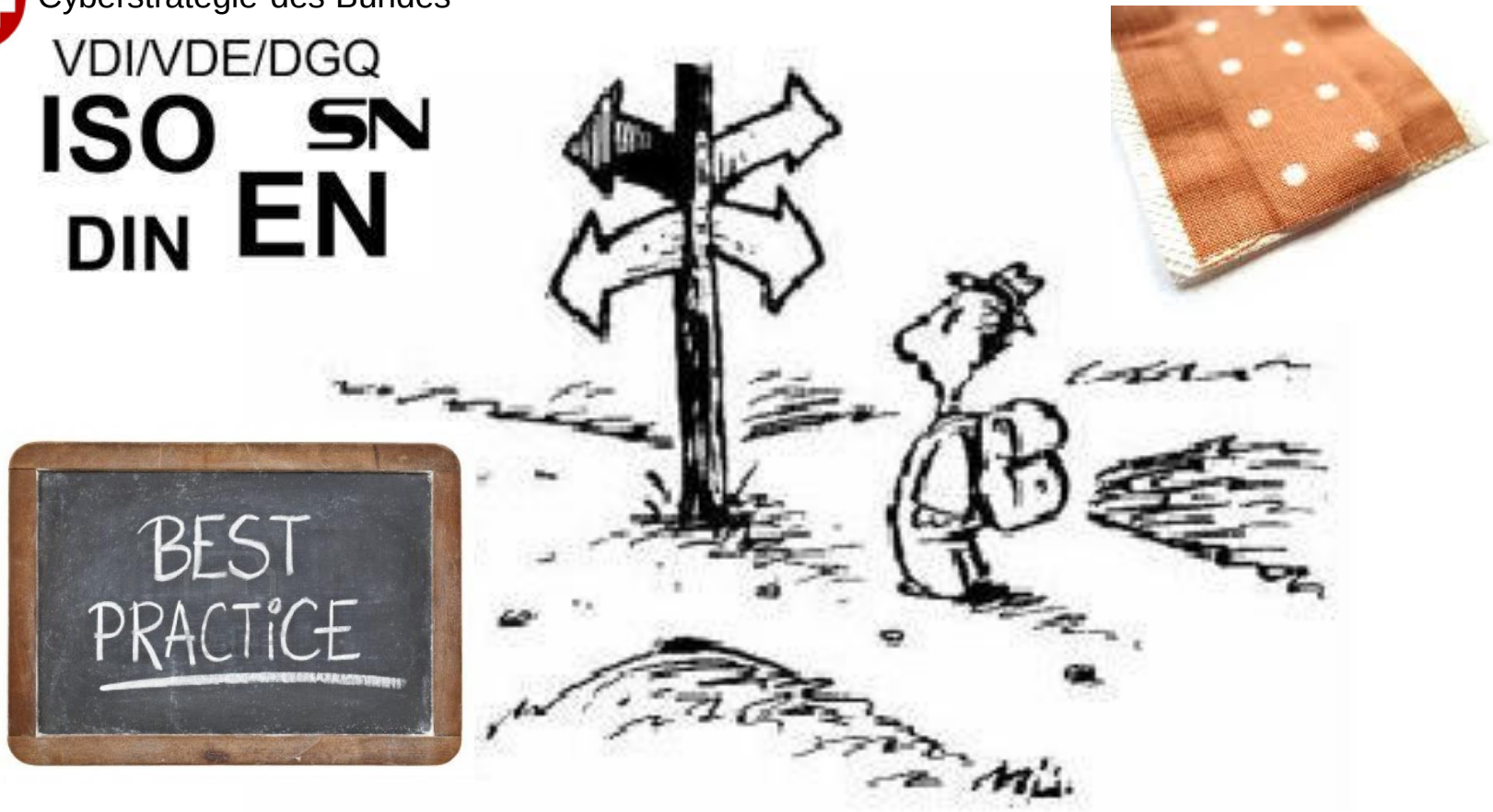
Quelle Wikipedia:
Grobe Struktur eines Stromnetzes

Cyberstrategie des Bundes

VDI/VDE/DGQ

ISO SN

DIN EN



“Ich kann die Bewegung der Himmelskörper berechnen, aber nicht das Verhalten der Menschen.”

Isaac Newton (1643-1727), engl. Physiker, Mathematiker u. Astronom

Social engineering…

ZEIT ONLINE zur Startseite machen

COMPUTERKRIMINALITÄT

Wie Kraftwerke gehackt werden

Ein Kraftwerk zu hacken, ist einfach. Viel zu einfach, wie der Sicherheitsforscher Tyler Klingler vom Unternehmen Critical Intelligence bewies. Bei einer Konferenz über Computersicherheit in Miami zeigte Klingler, wie leicht er an die E-Mail-Adressen auch von wichtig
diese dann
Klick ist der

Die Erfolgsquote war hoch: In einem Unternehmen mit rund 300 Angestellten identifizierte Klinglers Team 23 Mitarbeiter, die mit industriellem Kontrollsystem arbeiteten, von ihnen klickten sieben auf den Link in der E-Mail. Bei einem anderen Unternehmen mit 200 Angestellten klickten von 49 angeschriebenen Mitarbeitern elf auf den Link.

Kontrollfunktionen in Kraftwerken und an Ölpipelines innehatten. In diesen E-Mails verlinkte er vermeintliche Jobangebote und Fortbildungen für gängige Steuerungsprogramme solcher Anlagen. Ein echter Angreifer hätte an dieser Stelle mit Schadcode verseuchte Seiten verlinkt und darauf gewartet, dass ein Mitarbeiter vom Arbeitsplatz aus darauf zugreift.

Ist - Risiko- Schwachstellen-Analyse

Maßnahmen Umsetzungen bedeuten unter ICS Aspekten: **technologische - Herausforderungen**

KORAMIS

ICS Security Steuerung

- ✓ Asset Management
- ✓ Vulnerability Management
- ✓ Security Event & Information Management

ICS Endpoint Security

- ✓ Malware Protection
- ✓ Device Control
- ✓ Patch Management

ICS Infrastruktur Security

- ✓ Netzwerk-Security
- ✓ Remote Access Security
- ✓ Privileged Account Management

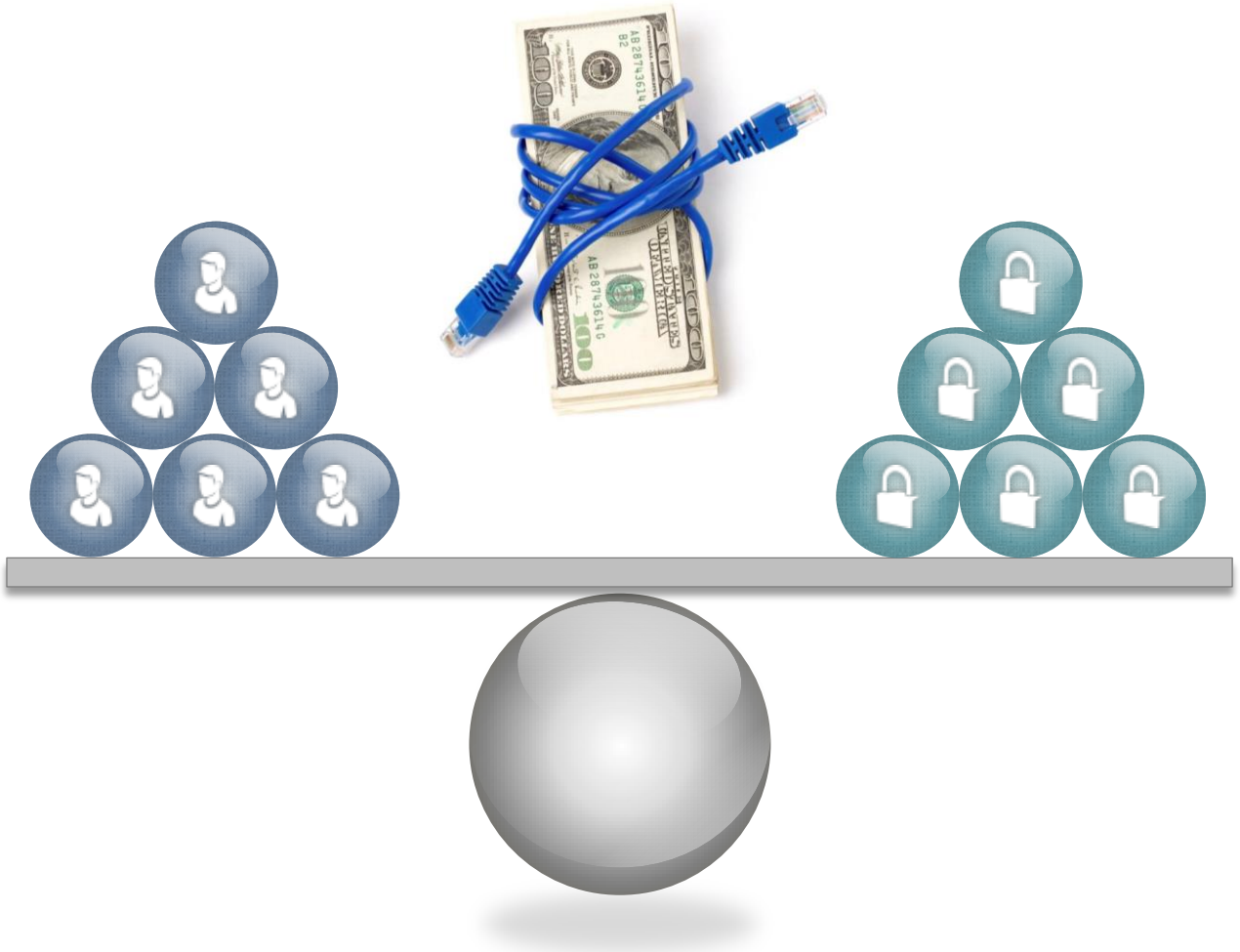
Pilotprojekt bei einem der großen internationalen Energieerzeuger (2008-2012) bzgl. ganzheitlichem Industrial IT Security Ansatz.

Über Beratung, Risikoanalyse, Schulung, Technologie-Integration bis zu Managed Security Services und Einhaltung von Richtlinien (Compliance). **Erstes Industrial Security Projekt dieser Art in Deutschland.**

Pilotprojekt bei einem der größten Energieversorger Deutschlands (2012) bzgl. ganzheitlichem Industrial IT Security Ansatz.

Von Consulting-Dienstleistungen, Industrial Security Strategieentwicklung, Integration von Security-Technologien, Schulungen bis hin **zur automatisierten Compliance-Überwachung**.

Balance wahren zwischen **Organisatorischen** & **Technischen** Maßnahmen



KORAMIS

Auf einen Blick:

Fakten und Zahlen

- Unternehmensverbund mit 80 Mitarbeitern
- 7 regionale Niederlassungen in D und CH
- Seit 1985 Dienstleistungen und Lösungen um und für die Prozessautomatisierung und Netzleittechnik
- Seit 7 Jahren spezialisiert auf Industrial IT Security
- Zertifizierter Consulting und Systempartner von Technologiepartnern im DACH Bereich
- BEST OF 2012 Initiative Mittelstand für Produkt Industrial IT Security (Deutschland)

Schwerpunkte

- EMSR Engineering
- Software- und Systemlösungen
  CA-x Software- und Applikationsentwicklung
- Automatisierungs- und Prozessleittechnik
  Consulting
  System-Integration/-Migration, Service, Wartung
- Industrial IT Security
  Consulting
  Schwachstellenanalyse
  Proof of concept / Evaluierung
  Realisierung und Support von Industrial IT Security-Lösungen
- Aktives Mitglied im VDI/VDE GMA 5.22 Security & DKE Normenkreis, Bayerischen IT Security Cluster
- Kooperation mit Universitäten und Instituten

KORAMIS

Unser Hintergrund in der Automatisierungs- und Prozessleittechnik:

ABB

- Contronic E mit CEK
- Contronic E mit Maestro UX
- Contronic E mit 800xA
- Melody mit Maestro UX
- Melody mit Operate IT B1
- Melody mit 800xA
- Procontrol P14 mit PBS30
- Procontrol P14 mit 800xA
- AC 800M mit 800xA
- Freelance mit Digivis
- Freelance mit 800xA
- S800, S900, AC500

Siemens und andere

- Netzleitsysteme
- Micro-Scada
- PCS7 / STEP 5 / STEP 7
- KUKA
- WinCC / WinCC flexible / proTool
- Industrial NET
- Industrial Ethernet, DP/PA Profibus, Profinet
- Safety Systems
- HIMA / ELOP II
- YOKOGAWA CS3000
- WinMOD, Simit Processing plants simulation

Informationsmanagement und Optimierung

- ABB
  PGIM (ehemals PlantConnect)
- OSIsoft
  PI
- Steinhaus
  TeBIS
- General Physics
  EtaPRO mit Virtual Plant
- Intelligon IFE Systems
- KORAMIS
  Datastorage
  Composer-Redundanz
  X-Terminal Lösungen
  Virtualisierung

KORAMIS GmbH
Quartier Eurobahnhof
Europaallee 5
D-66113 Saarbrücken
Tel.: +49 (0)681 / 968191-0
info@koramis.de
www.koramis.de

KORAMIS AG
Alpenstrasse 1
CH-6304 Zug
Tel.: +41 (0) 41 726 81 17
info@koramis.ch
www.koramis.ch