



Dr. Sebastian Obermeier, ABB Forschungszentrum Baden-Dättwil, 18.3.2015

# Sicherheit kritischer Infrastrukturen

Power and productivity  
for a better world™

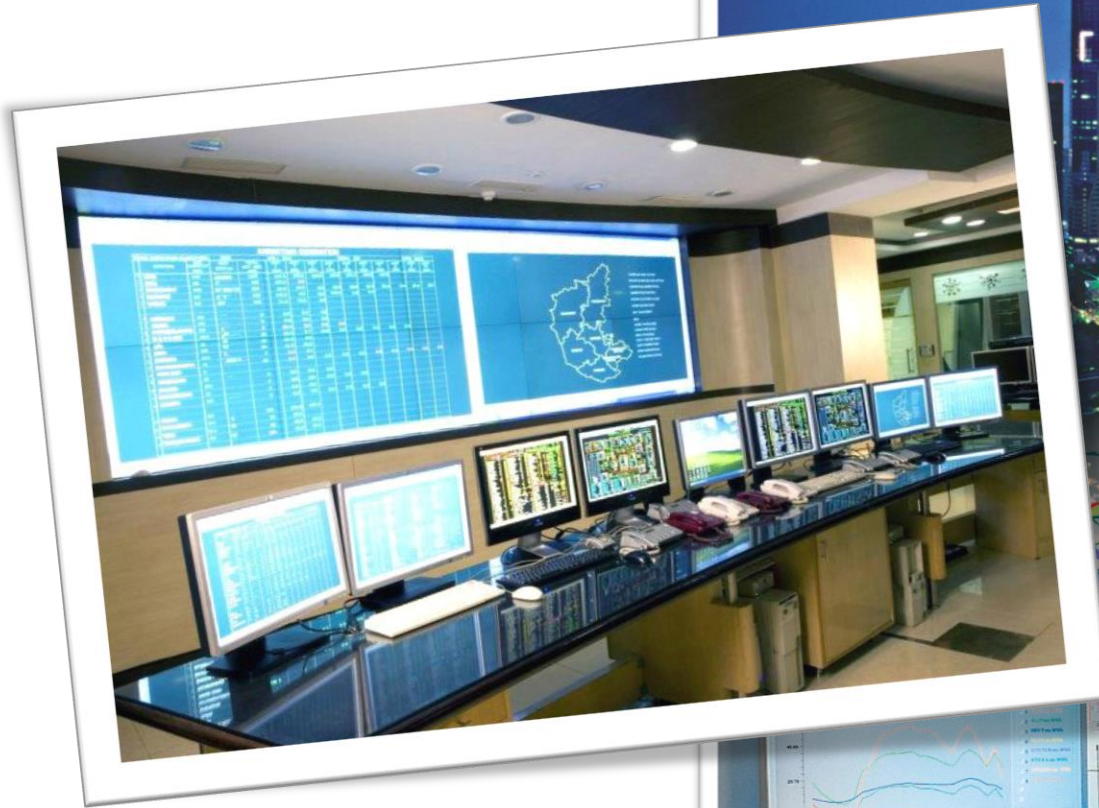


# Embedded Devices

## Software ist eine Kernkomponente



# SCADA and Control Systems Software ist eine Kernkomponente



# Kritische Infrastrukturen

## Begriffe

- Industrial Control System = Leitsystem

Beispiele:

- SCADA (Supervisory Control and Data Acquisition)  
Bezeichnet meist Leitsysteme mit Wide-Area Aspekten

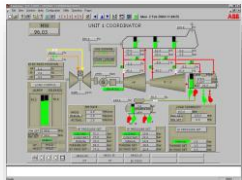
- DCS (Distributed Control System)  
Eher lokaler Natur

- Controller = PLC (Programmable Logic Controller) = SPS  
(Speicherprogrammierbare Steuerung)

- Besitzt Inputs und Outputs, erlaubt Programmierung der Outputs

- Substation = Unterstation = Umspannwerk

- IED (Intelligent Electronic Device) = Controller für Energietechnik



# Beispiele von Cyber Security Vorfällen

## Stuxnet malware is 'weapon' out to destroy ... Iran's Bushehr nuclear plant?

Cyber security experts say they have identified the world's first known cyber super weapon designed specifically to destroy a real-world target – a factory, a refinery, or just maybe a nuclear power plant.

The cyber worm, called Stuxnet, has been the object of intense study since its detection in June. As more has become known about it, alarm about its capabilities and purpose have grown. Some top cyber security experts now say Stuxnet's arrival heralds something blindingly new: a cyber weapon created to cross from the digital realm to the physical world – to destroy something.

At least one expert who has extensively studied the malicious software, or malware, suggests Stuxnet may have already attacked the world's first nuclear power plant, which much of the

### Neuartiges Computervirus soll im Iran Atommeiler beschädigt haben

Von Martin Kilian, Washington, Aktualisiert am 23.09.2010

Experten sprechen bei dem Angriff der Schadsoftware Stuxnet vom "Hack des Jahrzehnts".

The appearance of Stuxnet is large, too encrypted, too complex like taking control of a computer button other than inserting an in of time, money, and software in industrial control software system

Unlike most malware, Stuxnet is data. Industrial control systems reverse engineering Stuxnet, the template for attackers wishing to link not required.

"Until a few days ago, people did Langner, a German cyber-security present his findings at a conference Rockville, Md. "What Stuxnet is to buy an attack like this on the I



Soll Ziel eines hochkomplexen Angriffs geworden sein: Die iranische Atomanlage Bushehr. Bild: Reuters

A gradual dawning of Stuxnet

It is a realization that has emerged

Stuxnet surfaced in June and, by probably created by a team working derived from some of the files in in

## Stuxnet Jahr 2010

Source: NISTIR 7628, Guidelines for Smart Grid Cyber Security, USDoC, 28 september 2010

## Hacker Jahr 2000

## Maroochy Waste Water

- Event
  - More than 750,000 gallons of untreated sewage intentionally released into parks, rivers, and hotel grounds
- Impact
  - Loss of marine life, public health jeopardized, \$200,000 in cleanup and monitoring costs
- Specifics
  - SCADA system had 300 nodes (142 pumping stations) governing sewage and drinking water
  - Used OPC ActiveX controls, DNP3, and ModBus protocols
  - Used packet radio communications to RTUs
  - Boden used commercially available radios and stolen SCADA software to make his laptop appear as a pumping station
  - Causes as many as 46 different incidents over a 3-month period (Feb 9 to April 23)



### Lessons learned

- Change log-ons after terminations
- Investigate anomalous system behavior
- Use secure radio transmissions

## Davis Besse Nuclear Power Plant

- Event
  - August 20, 2003 Slammer worm infects plant
- Impact
  - Complete shutdown of digital portion of Safety Parameter Display System (SPDS) and Plant Process Computer (PPC)



### Recovery time:

SPDS – 4 hours 50 minutes  
PPC – 6 hours 9 minutes

### Lessons learned

- Secure remote (trusted) access channels
- Defense-in-depth strategies, FWs and IDS
- Critical patch installation needs to drive trusted agent status

## Slammer Jahr 2003

NIST  
Institute of Standards and Technology  
Ed. 08 Feb 2010  
file:2008\_SPNkourk.pdf

48

# Realitäts-Check – Cyber Security ist kein Mythos

## Fallbeispiel aus der Industrie



### Industrieunternehmen nutzt ein Produkt ausserhalb der Spezifikation

- IT Abteilung eines Industrieunternehmens implementiert eine Vorschrift, dass Vulnerabilityscans für alle aktiven IP Adressen global ausgeführt werden – mittels kommerzieller Software
- Scans sind in das Produktionssystem vorgedrungen, scannen eingebettete Geräte, die daraufhin ausfallen, nach Reset nicht mehr funktionieren, und daraufhin einen Produktionsstop verursachen
- Hersteller sollte aushelfen

### Folge für Unternehmen

- Ausbreitung schleichend (!) über mehrere Monate, zunächst 1 Gerät betroffen, schließlich über 60
- Produktionsstop, Produktionsziel nicht erreicht
- 9 Stunden Nichtverfügbarkeit in einem 3 Wochen Zeitfenster

### Folge für Hersteller

- Ausgaben ohne Einnahmen
- Möglicher Reputationsschaden
- Fall wurde mit anstehendem Millionenauftrag gekoppelt
- Mögliche Folgekosten für "alle weiteren Security Probleme" mit diesem Gerät

# Wie entwickelte sich Cyber Security zum Problem?

## Historische Entwicklung



Isolierte  
Geräte

Punkt zu Punkt  
Kommunikation

Proprietäre  
Netzwerke

Ethernet/ IP  
Netzwerke

Verbundene  
Systeme

Verteilte  
Systeme

### Moderne Automationssysteme/Prozessleitsysteme:

- Nutzen Standard-IT-Komponenten (Windows, Internet Explorer, DCOM, etc.)
- Nutzen IP basierte Kommunikationsprotokolle
- Sind verbunden mit externen Netzwerken
- Nutzen mobile Geräte und Speichermedien

**Moderne Automationssysteme sind spezialisierte IT Systeme  
→ Bedrohungen der Office IT treffen auch hier zu**

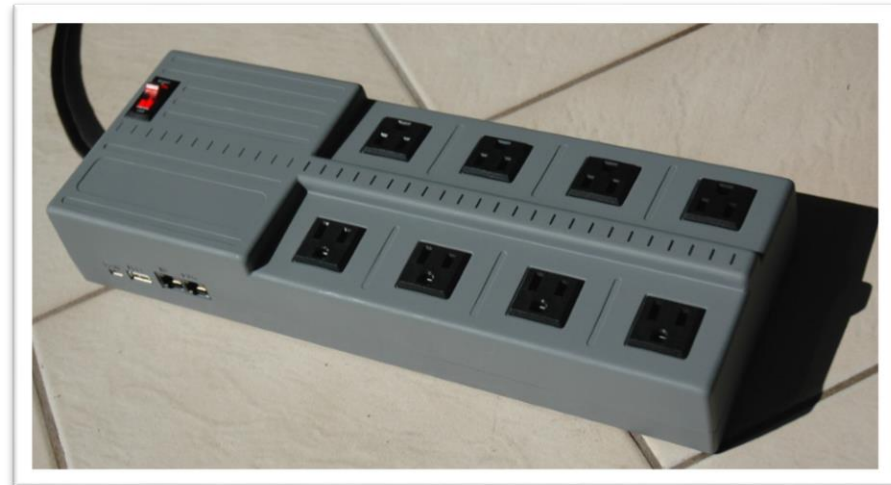
# Mythos isolierte Netze

## Isolation ist nicht gleich Sicherheit

- Physischer Einmalzugriff ausreichend um getarnte Backdoor-Geräte zu installieren
    - Kommerziell verfügbar, günstig
  - Eingebettete PCs mit 3G Modem und vorinstallierte Angriffssoftware
  - Angreifer können aus der Ferne auf das Netzwerk zugreifen
- Isolation bietet keine ausreichende Sicherheit (mehr)
- Bewusstsein dafür noch nicht überall vorhanden



<http://pwnieexpress.com>



**ABB**



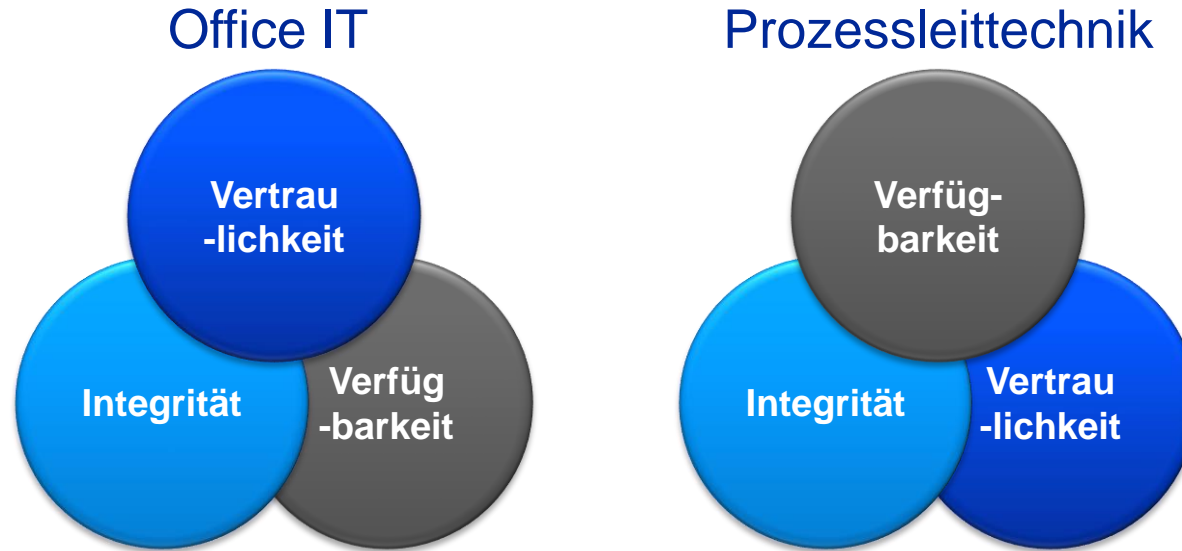
# Cyber Security Herausforderungen

## Unterschiede zur IT Security

	“Traditionelle” Information Technology	Energie- und Automationstechnik
<b>Primäres zu schützendes Objekt</b>	Information	Physischer Produktionsprozess
<b>Risiko</b>	Verlust vertraulicher Informationen, monetärer Verlust	Bedrohung von Leib und Leben, Umweltschäden, monetärer Verlust
<b>Schutzziele</b>	Confidentiality, Privacy	Availability, Integrity
<b>Fokus der Security</b>	Zentrale Server <small>(schnelle CPU, viel Speicher, ...)</small>	Verteiltes System <small>(Limitierte Ressourcen)</small>
<b>Anforderungen an Verfügbarkeit</b>	95 – 99% <small>(accept. downtime/year: 18.25 - 3.65 days)</small>	99.9 – 99.999% <small>(accept. downtime/year: 8.76 hrs – 5.25 minutes)</small>
<b>Lebensdauer</b>	3 – 10 Jahre	5 – 25 Jahre

# Office IT vs. Prozessleittechnik

## Unterschiedliche Prioritäten der Schutzziele



- In der Prozessleittechnik ist die "CIA Pyramide" auf den Kopf gestellt
  - Striktere Anforderungen an Verfügbarkeit, Performanz und sofortigen Zugriff
  - Störungen gefährden Leib und Leben der Mitarbeiter und der Öffentlichkeit sowie die Umwelt

# Angriffstoleranz in der Prozessleittechnik ... beinhaltet Toleranz gegen verschiedenste Fehler



Verschiedene Fehlerkategorien müssen berücksichtigt werden

- die hochgradig voneinander abhängig sind
- die deshalb gleichermassen wichtig sind
- die im System-Entwurf genauso wie im Betrieb berücksichtigt werden müssen

# Office IT vs. Prozessleittechnik

## Warum klassische Ansätze nicht immer funktionieren

- Kontensperre von 10 Minuten nach 3 fehlerhaften Login-Versuchen  
→ Prozessbediener hat im Notfall für 10 Minuten keine Kontrolle!
  - Installation von Patches sobald verfügbar, bei Bedarf Reboot  
→ Neustart des Prozessleitsystems kann Stop der Produktionsanlage bedeuten, evtl. dauert der Neustart der Anlage Tage!
  - Verwendung von Kryptografie zum Schutz von Datenübertragung  
→ Echtzeitanforderungen werden aufgrund mangelnder Rechenkapazität von Feldgeräten verletzt
  - Verwendung von Firewalls und Intrusion Detection Systemen  
→ Welche Firewall hat Protokollfilter für OPC, HART, IEC61850, ProfiNet, Modbus, IEC 60870-5-104...
  - Verwendung von Intrusion Prevention Systemen  
→ Ein False Positive kann fatale Folgen haben!
- Es gibt vieles, was von der Office IT Security übernommen werden kann, aber die Konzepte müssen mit Bedacht angewendet werden**

# Cyber Security

## ...ein Themengebiet für die ABB-Forschung



### ABB Forschungszentrum

- Entwickelt zukunftsweisende Cyber Security-Konzepte und -Technologien
- Authentifizierung, Remote Access, Security Monitoring, Security Engineering, Securityanalysen, Marktanalysen ...
- Evaluiert Security relevante Technologien
- Adaptiert IT Security für industrielle Systeme



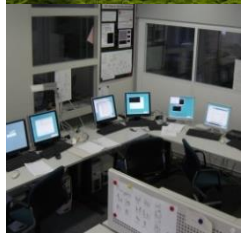
### Forschungsgebiete

- Adressierung von Hochverfügbarkeits- und Performanceanforderungen
- Vereinfachung des Security Engineering
- Analyse der vielfältigen Lösungsansätze in der Industrie



### ABB-Motivation

- Entwicklung und Installation von sicheren Systemen
- Beschleunigung von Industriestandards



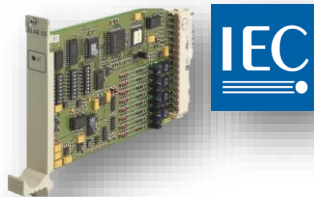
# ABB-Forschung Beispielprojekte

## ESCoRTS

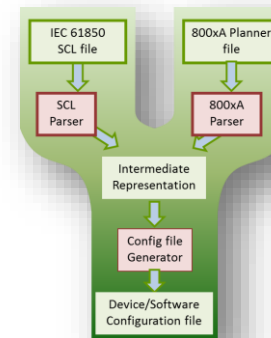
*Unterstützt durch die EU-Kommission*



IEC62351 Performance Evaluation  
*Entwicklung eines Standards*



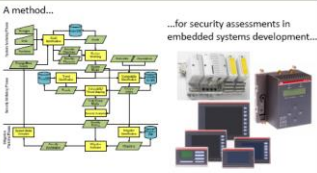
Automated network security configuration  
*Entwicklung eines Konfigurationskonzeptes*



# ABB-Forschung Resultate

ESSAM: Embedded System Security Assessment for Manufacturers


A method... for security assessments in embedded systems development...



Key Features:

- Collaboration Support
- Flexibility and traceability of inputs
- Targeted at design phase
- Meets for system developers and security experts
- No necessary risk quantification required
- Custom definition of security objectives, assets, security measures, threats and vulnerabilities
- Enables ongoing security assessments

...supported by a tool



Security Assessment-Methode gibt einen verifizierbaren Security-Überblick

Audit & Hardening (ASH) - Switch to expert mode

Computer Selection

Computer name: Baseline

Computer IP: 127.0.0.1

Set target parameters

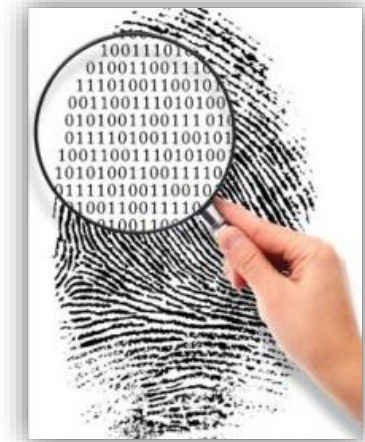
Computer name: CHC-0010017\_Aurora-01

Computer IP: 127.0.0.1

Authentication: Login, Password, Set Credentials and Restore

Name	Actual Settings	Recommended Settings	Insecure Settings
Server session timeout	Never	[12]0-9	[0-9]0-[9]Newer
Account lockout duration	30	[0-9]0-[10]2[0-9]	[3-5]0-9
Maximum password age	90	[0-9]1-[9]10[0-9]	[0]1-9[10]2[0-9]
Minimum password age	1	[1-5]	[0-9]0[1-9]0-9
Minimum password length	8	[8]9[10]11[12]	[1-7]
Lockout observation window	30	[3-9]0-9	[12]0-9
Lockout threshold	6	[5-9]	[1-5]
Password history	4	[5-9]1[10]9	[1-4]None
Automatic Admin logon	0	0	1

Automatisierte Härtung erlaubt eine automatische Verbesserung der Security



Forensik bereitet eine schnelle Erstuntersuchung vor

# Forschungsergebnisse – Forensik Überblick



Im Falle eines Cyber Angriffs ist eine schnelle Untersuchung der Veränderungen eines Gerätes wichtig.

Product	Version	Manufacturer	Similarity	File
IED	IEC61850	ABB	91	C:\Users\schfa...
IED	Baseline 1	ABB	91	C:\Cloones\IED...

Summary  
Processing time= 2105 ms  
Total number of files= 211  
Number of unknown files= 4  
Number of known files using only SHA1 matchings= 207  
Number of known files using sha1 and fuzzy matching= 0  
Number of files or folders with one or multiple alternate data streams attached= 0

Summary of the selection:  
Total number of selected files= 208  
Number of unknown files= 2  
Number of known files using only SHA1 matching= 205  
Number of known files using sha1 and fuzzy matching= 1  
Number of files or folders with one or multiple alternate data streams attached= 0

## Konzept und Prototyp

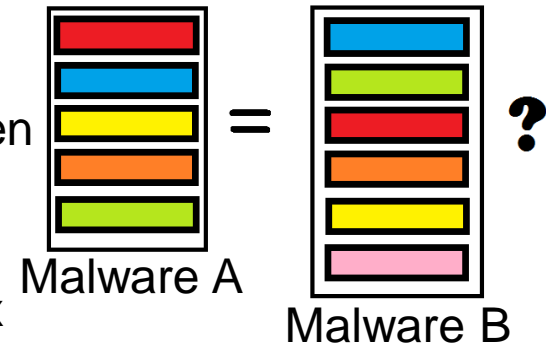
- Erlaubt die Erstellung eines Fingerabdrucks eines kompletten Gerätes, sowie der spätere Vergleich mit diesem Fingerabdruck
- Ähnlichkeitsindex bei Abweichungen erlaubt erste Einschätzung
- Unterstützt durch prototypisches Software Tool



# Forschungsergebnisse – Forensik

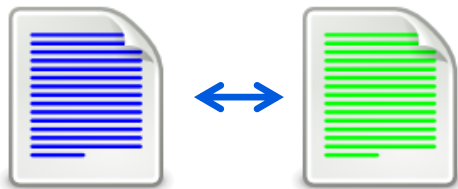
## Nutzung von Fuzzy Hashing

- Reguläre Hashes (Fingerabdruck):
  - Identifizieren ausschließlich komplett identischer Dateien
- Fuzzy Hashes
  - Identifizieren ähnlicher Dateien durch Ähnlichkeitsindex



Ähnlichkeit: z. B. 75 (0-100)

→ nicht erkannt durch reguläres Hashing

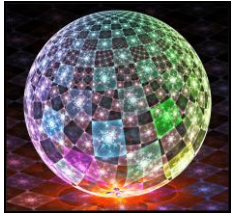


Ähnlichkeit : 0 (0-100)

**Vielversprechende Technologie für heuristische Analyse von veränderlichen Dateien (Logs, Konfigurationsdaten, Produktionsdaten, etc.)**

# Cyber Security im Industrie 4.0 Zeitalter

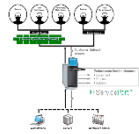
## Kommende Herausforderungen



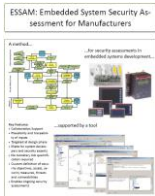
- Charakteristisch für Industrie 4.0:  
Massive Vernetzung der Geräte untereinander
  - 50 Mrd. “Dinge” im Jahr 2020 (Cisco IBSG, 2012)
- Dadurch entstehende, neue Cyber Security-Herausforderungen im Industrie 4.0 Umfeld
  - Security by Design
  - Kontinuierliche Anpassung von Produktionssystemen
  - Vertrauen und Misstrauen von zahlreichen Kommunikationspartnern
  - Unternehmensübergreifende Fertigungsprozesse
  - Cloud
  - Datenschutz: Produktionsdaten, Plagiatsschutz
  - Usability
  - ...

# Zusammenfassung

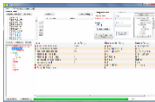
## Sicherheit kritischer Infrastrukturen



- Die Bedeutung und Rolle von Cyber Security für industrielle Automatisierungs- und Steuerungssysteme nimmt zu



- ABB forscht und entwickelt aktiv an Cyber Security- Lösungen für kommende Herausforderungen



- Cyber Security entwickelt sich in verschiedenen Aspekten

- Angriffe
- Technologien
- Szenarios



Power and productivity  
for a better world™

