

# Smart Home, Internet of Things ... und andere Katastrophen

*Prof. Dr. Reiner Creutzburg*

Technische Hochschule Brandenburg, FB Informatik und Medien

IT- und Medienforensiklabor

PF 2132

D-14737 Brandenburg an der Havel

[creutzburg@th-brandenburg.de](mailto:creutzburg@th-brandenburg.de)

Cybersicherheitssymposium 31.05.2018

# Prof. Dr. Reiner Creutzburg

- seit 1992 Informatik-Professor an der FH Brandenburg
- Leiter IT- und Medienforensiklabor
- Geprüfter Datenschutzbeauftragter (SGS TÜV)
  - diverse Mandate als Externer Datenschutzbeauftragter
- Geprüfter IT-Sicherheitsbeauftragter (SGS TÜV)
- ISO27001 Auditor (SGS TÜV)
- Certified Ethical Hacker (CEH)
- Computer Hacking Forensic Investigator (CHFI)
- Security Analyst (ECSA)
- Licensed Penetration Tester (LPT)
- ...

Ihr Google-Herzschriftmacher  
hat uns benachrichtigt, dass wir  
hier gleich gebraucht werden



Internet 4.0



Eine Welt ohne Datenschutzbeauftragte. Wollen wir das?



Gesundheitsvorsorge per Handy: Überlegene Technik setzt sich durch



GRESER & LEUZ

Europäische Datenschutzgrundverordnung: Mit dem Datenschutz in Urlaub

# Types of Hackers.



White Hats



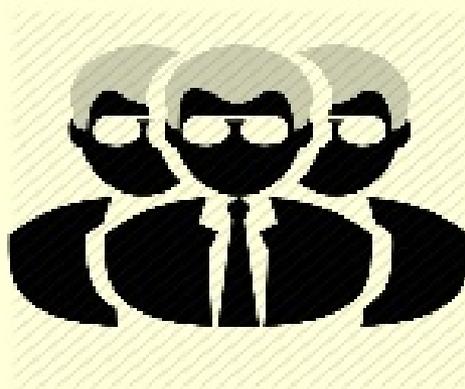
Black Hats



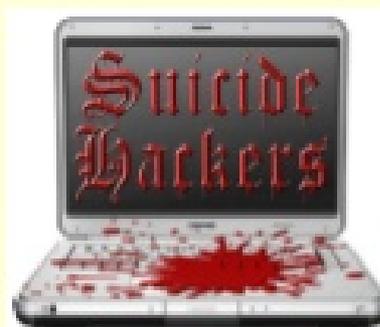
Grey Hats



Script Kiddies



Spy Hackers



Suicide Hackers

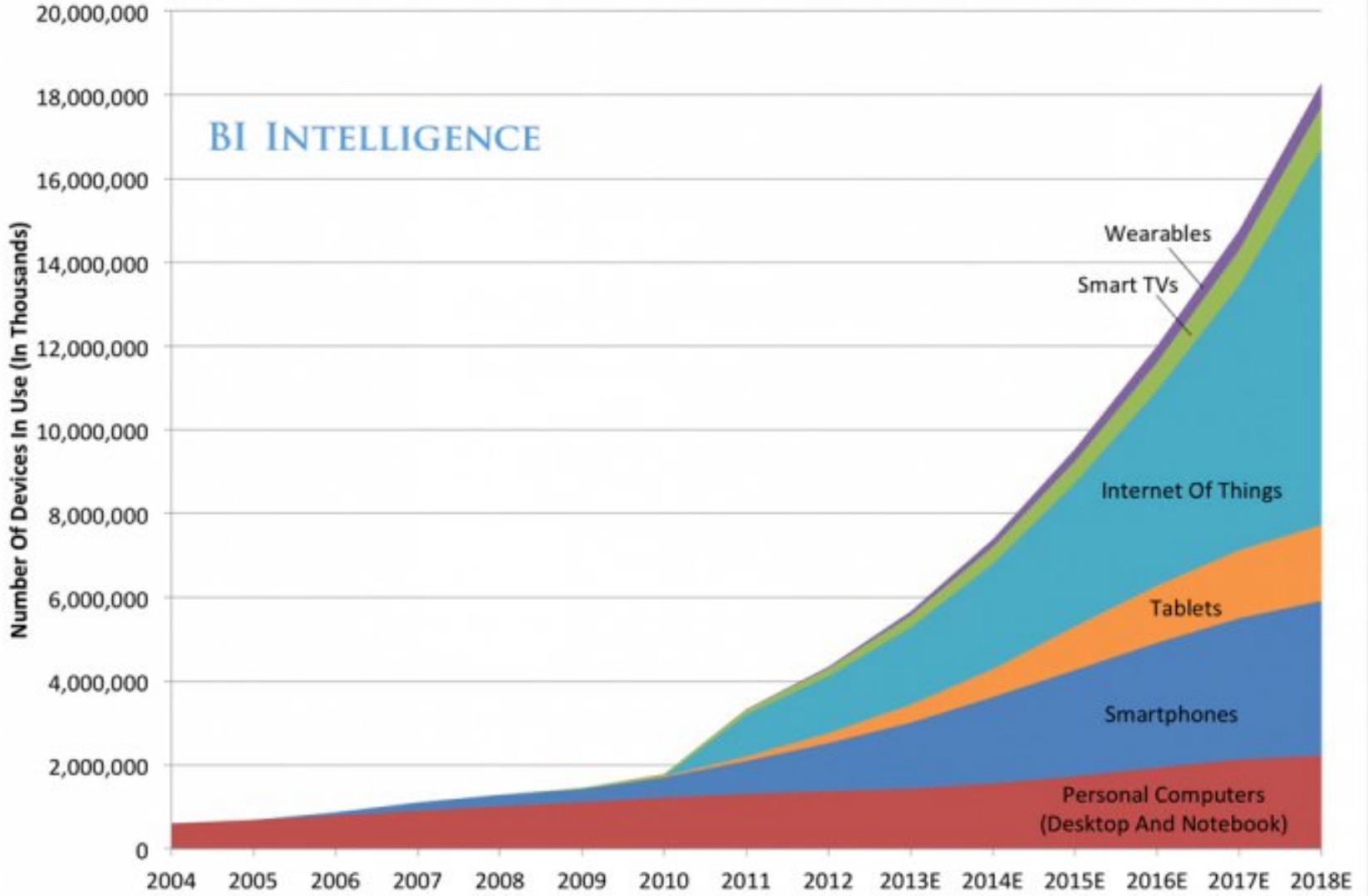


Cyber Terrorist



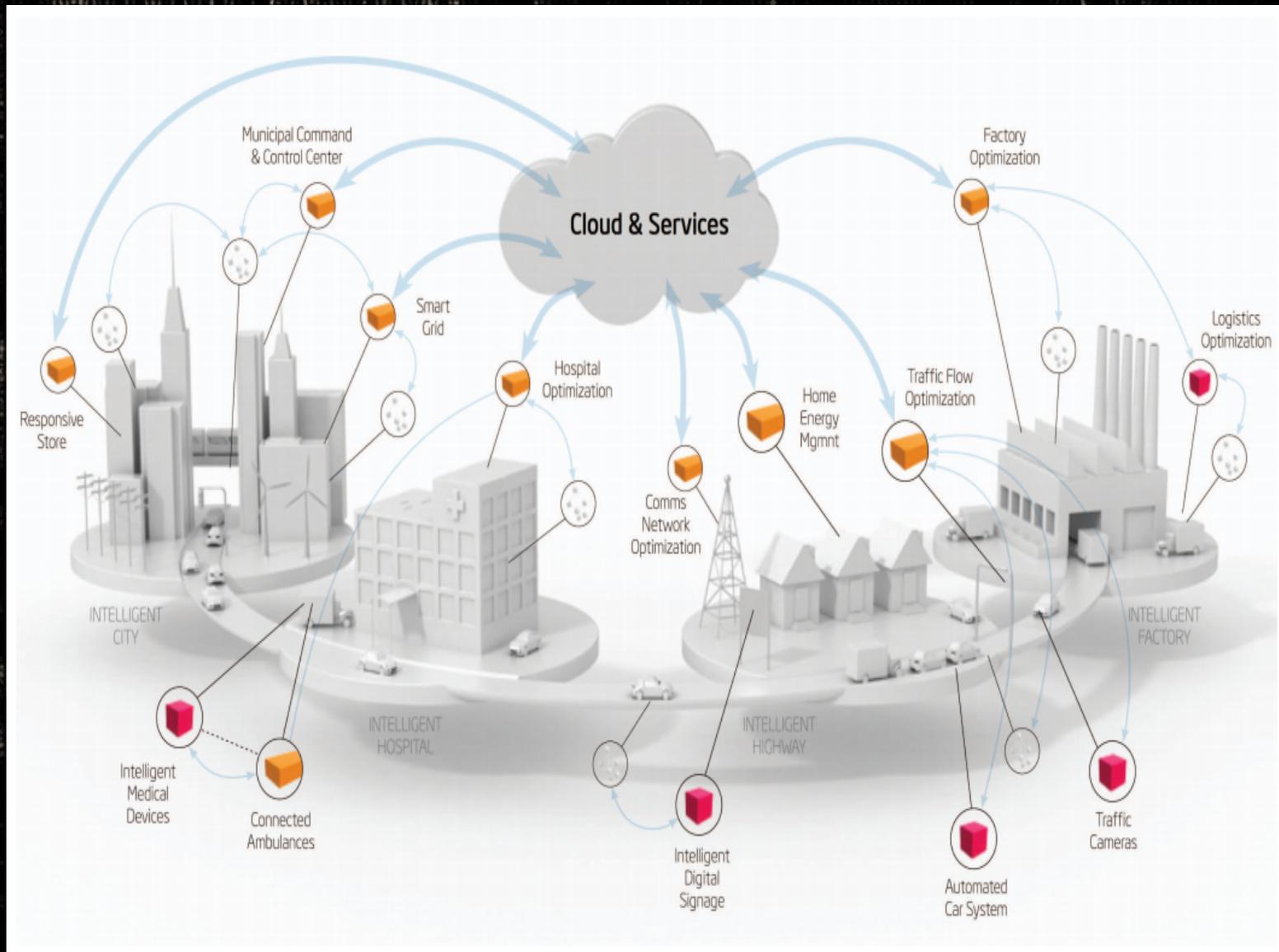
State Sponsored Hackers

# Global Internet Device Installed Base Forecast

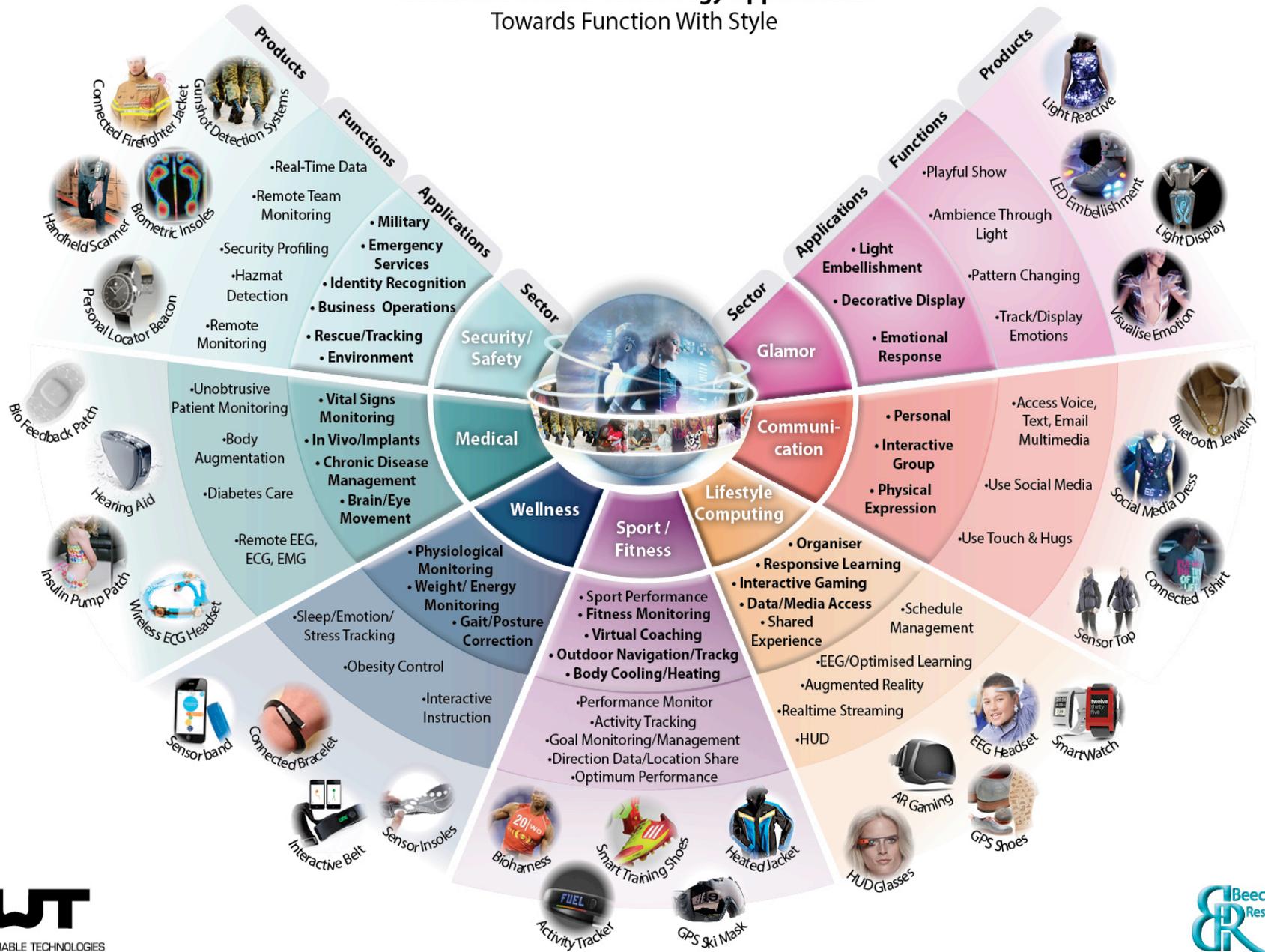


Source: Gartner, IDC, Strategy Analytics, Machina Research, company filings, BII estimates

# Internet der Dinge (Internet of Things)

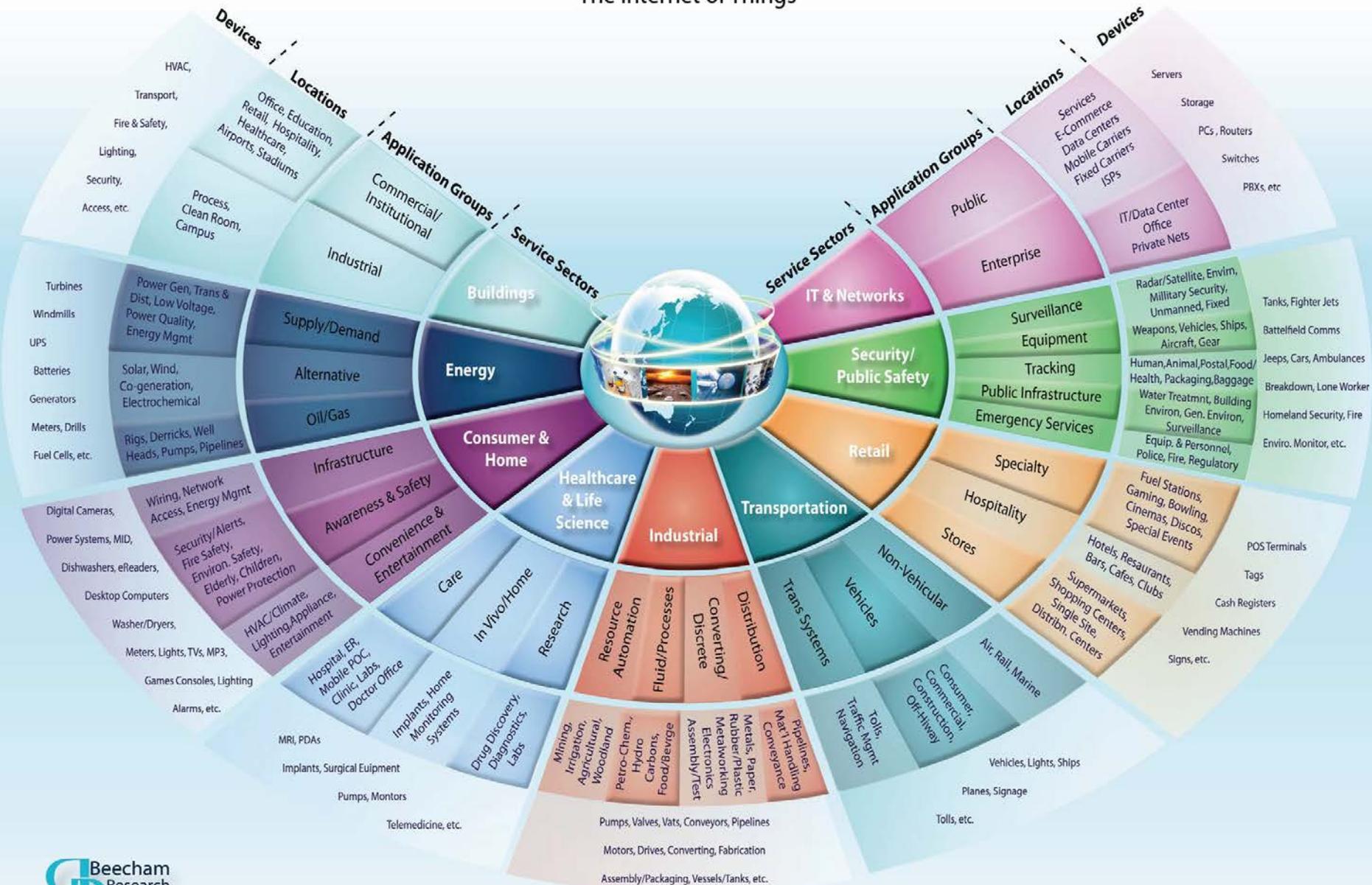


# World of Wearable Technology Applications: Towards Function With Style



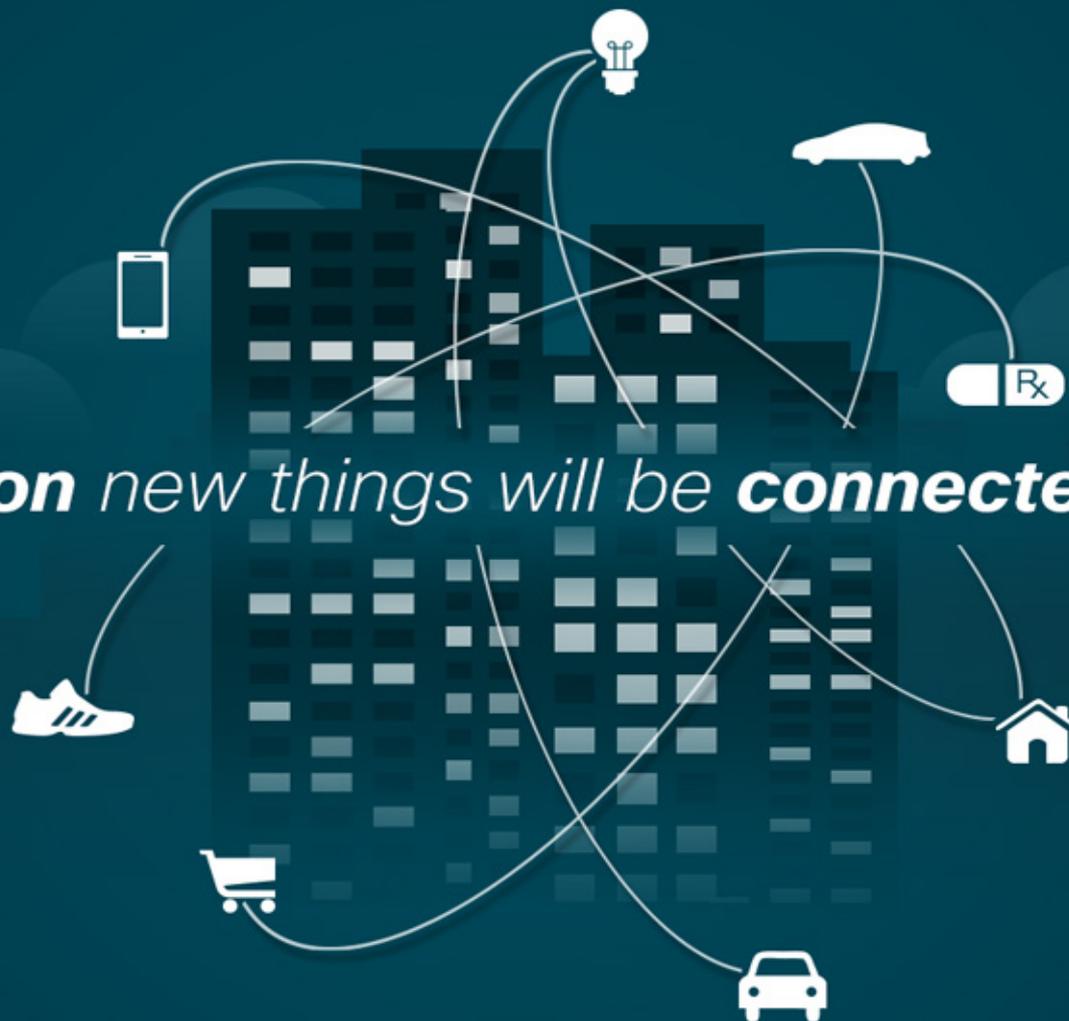
# M2M World of Connected Services

## The Internet of Things



# THE INTERNET **OF EVERYTHING** IS HERE.

As the Internet evolves, so will we.



**37 billion** new things will be **connected by 2020.**

## POPULATION EXPLOSION:

The Internet of Things will include

**26 BILLION**

units installed by 2020.\*

## REVENUE EXPLOSION:

The Internet of Things product and service suppliers will generate incremental revenue exceeding

**\$300 BILLION**

by 2020.\*

## VALUE EXPLOSION:

The Internet of Things will result in

**\$1.9 TRILLION**

in global economic value-add through sales into diverse end markets.\*

\* Source: Gartner, Forecast: The Internet of Things, Worldwide, 2013, 18 November 2013

# 5 TIPS FOR MONETIZING THE \$1.9 Trillion INTERNET OF THINGS

## 1 Simplify

Build a single device model that contains all capabilities and capacity then use licensing and entitlement management to configure.

## 2 Differentiate

Drive more value from your device with software and monetize all aspects of your solution.

## 3 Drive Revenue

Device + software + licensing helps drive new, recurring revenue streams.

## 4 Grow Market

Move into new markets quickly by slicing and dicing your product by features, capacity, and more.

## 5 Protect Your IP

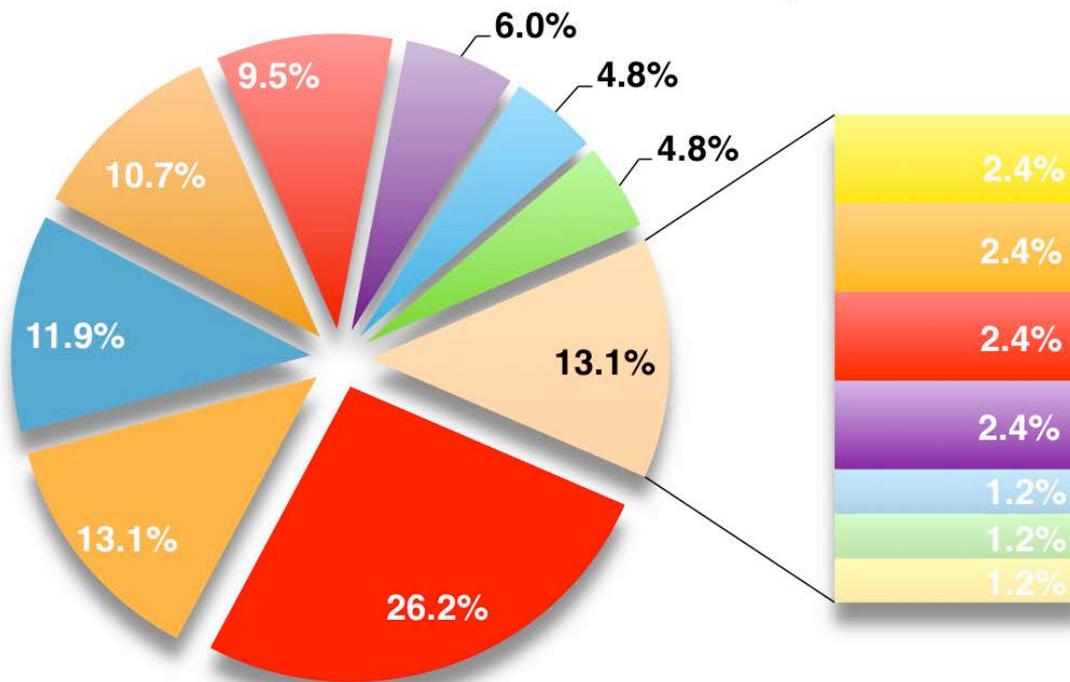
Protect your devices and applications against IP theft with licensing.

# Cybercrime – www.hackmageddon.com

Ref	Date	Author	Target	Description	Attack	Target Category	Attack Category	Country
1	Apr 1			NullCrews hacks a legacy help desk system of the government contractor Klas Telecom, and leaks several accounts and passwords.	SQLI	Industry: Telco HW	H	US
2	Apr 1	?		Email marketing service Mad Mimi is hit by a DDoS attack. Shortly after, they receive an email from someone who asked for 1.8 Bitcoins to stop launching attacks.	DDoS	Industry: Email Marketing	CC	US
3	Apr 1	YMH		A Yemeni hacker going with the handle of "YMH" defaces the official website of Egyptian Armed Forces Training Authority (mtc.edu.eg).	Defacement	Military	CC	EG
4	Apr 2	Probably Onion		ProbablyOnion hacks a job seeker website (bigmoneyjobs.com) and dumps over <b>36,000</b> accounts online.	SQLI	Industry: Job Seeking	CC	US
5	Apr 2	?		A DDoS attack takes down the Kansas Interactive Testing Engine (KITE, ksassessments.org), Kansas' new online student testing system.	DDoS	Education	CC	US
6	Apr 2	HeavenN		A hacker called HeavenN hacks aurelis.hr and dumps 532 email addresses, usernames, and passwords.	SQLI	E-Commerce	CC	HR
7	Apr 3	?		German authorities confirm that they are investigating the theft of around <b>18 million</b> e-mail accounts and passwords, affecting all major German Internet service providers.	Botnet	Several Categories	CC	DE
8	Apr 3	?		Health services provider Kaiser Permanente notifies roughly <b>5,100</b> members that their personal information may be at risk after malware was discovered on a server used by the Kaiser Permanente Northern California Division of Research.	Malware	Industry: Health Services	CC	US
				NullCrew and TheHorseMenLulz team				

# Angegriffene Ziele

**Distribution of Targets**  
February 2015



- Industry
- Single Individuals
- Organization
- Government
- Education
- Finance
- >1
- News
- Bitcoin Exchange
- Hobby
- Internet Services
- Online Services
- Adult Site
- Airline
- Web Comic

5. Februar 2015, 16:43 Sicherheitsexperte Kaspersky

# Darauf haben es Hacker abgesehen



In Rechenzentren speichern Firmen wichtige Informationen - für Hacker sind sie besonders wertvoll (Foto: picture alliance / dpa)

- Das Geschäft mit Cybersicherheit wird wachsen. Denn aus alltäglichen Gegenständen werden Computer - und diese sind hackbar.
- Der IT-Experte Kaspersky warnt davor, dass Hacker bereits neue Ziele in Angriff nehmen, kritische Infrastruktur gehört dazu. Darunter fällt zum Beispiel Steuerungsanlagen für Stauseen.

## ANZEIGE



### Jetzt Zukunftsbonus sichern

Mit der eigenen Solaranlage Strom erzeugen und speichern

[Hier klicken](#)



### DAX-Absturz in Kürze

8 Aktien, die Sie sofort verkaufen müssen. Gratis-PDF!

[Hier exklusiv lesen.](#)



### Der neue Doblò Cargo

Alles beginnt bei Ihnen. Der neue

# Security risk of medical devices in IT networks - the case of an infusion pump unit

Jenny Knackmuß<sup>a,b</sup>, Thomas Möller<sup>b</sup>, Wilfried Pommerien<sup>a,c,d</sup>, and Reiner Creutzburg<sup>a</sup>

<sup>a</sup>Brandenburg University of Applied Sciences, Department of Informatics and Media  
P.O.Box 2132, D-14737 Brandenburg, Germany

<sup>b</sup>Assecor GmbH, Storkower Str. 207, D-10369 Berlin, Germany

<sup>c</sup>Städtisches Klinikum Brandenburg GmbH, Zentrum für Innere Medizin II, Hochstr. 29,  
D-14770 Brandenburg, Germany

<sup>d</sup>Medizinische Hochschule Brandenburg CAMPUS GmbH, Fehrbelliner Straße 38  
D-16816 Neuruppin, Germany

Email: {knackmus|pommerien|creutzburg}@fh-brandenburg.de,  
{thomas.moeller|jenny.knackmuss}@assecor.de,  
w.pommerien@mhb-fontane.de

## ABSTRACT

Nowadays, wearable and implantable medical devices are being increasingly deployed to improve diagnosis, monitoring, and therapy for various medical conditions. Compared to other types of electronics and computing systems, security attacks on these medical devices have extreme consequences and must be carefully analyzed and prevented with strongest efforts. Often, the security vulnerabilities of such systems are not well understood or underestimated. The aim of this paper is to demonstrate security attacks that can easily be done in the laboratory on a popular infusion pump on the market, and also propose defenses against such attacks.

**Keywords:** medical device security, security of medical devices, hacking medical devices, hacking infusion pumps, infusion pump, wearable medical devices

# Suchmaschine Shodan



The image shows a screenshot of a web browser window. The address bar displays the URL [t3n.de/news/shodan-erschreckendste-455939/](http://t3n.de/news/shodan-erschreckendste-455939/). The page header features the t3n logo and navigation links for Newsticker, Magazin, Fragen & Antworten, Jobbörse, Shop, and Marktplatz. The main content area has a large heading: **Shodan: „Die erschreckendste Suchmaschine des Internets“**. Below the heading is a paragraph of text: **Als „erschreckendste Suchmaschine des Internets“ bezeichnet CNN das Projekt Shodan. Und tatsächlich lassen sich mit ihr teils haarsträubende Sicherheitslücken finden. Dabei geht es vor allem um Geräte, die ohne ausreichenden Schutz mit dem Internet verbunden sind. Manchmal ist das zum Lachen, manchmal aber auch zum Fürchten.** A second paragraph follows: **Das „Internet der Dinge“ ist als Schlagwort inzwischen bestens bekannt und es ist schon sehr viel mehr mit dem Internet verbunden, als man mancher glauben würde. Die Suchmaschine Shodan zeigt das und zeigt dabei auch, wie sorglos in manchen Fällen damit umgegangen wird. „Wenn Leute etwas nicht auf Google finden, glauben sie, dass niemand es finden könne. Das ist falsch“, sagte Shodan-Macher John Matherly dem Nachrichtensender CNN. Während Google sich nur für URLs interessiert, behält Shodan mehr im Blick. Informationen von über 500 Millionen mit dem Netz verbundenen Geräten und Diensten sammelt die Suchmaschine pro Monat ein**



simatic



Explore

Contact Us

Blog

Enterprise Access

New to Shodan?

Login or Register

Exploits 74

Maps

TOP COUNTRIES



Germany	303
Italy	286
Poland	184
United States	171
Spain	170

TOP SERVICES

Siemens S7	1,173
SNMP	1,018
NetBIOS	22
Modbus	20
SMB	5

TOP ORGANIZATIONS

Deutsche Telekom AG	182
Telecom Italia Mobile	134
Telefonica de Espana	128
Orange	92
Telecom Italia	42

TOP PRODUCTS

Microsoft ESMTMP	7
Microsoft SQL Server	6
TightVNC	1

Showing results 1 - 10 of 1,651

89.202.203.242

Interoute Communications Limited  
 Added on 2015-03-17 23:56:25 GMT  
 United Kingdom  
[Details](#)

Copyright: Original Siemens Equipment  
 PLC name: SIMATIC 300(RBG01)  
 Module type: CPU 315F-2 PN/DP  
 Unknown (129): Boot Loader A%  
 Module: 6ES7 315-2FJ14-0AB0 v.0.6  
 Basic Firmware: v.3.2.10  
 Module name: HRL-CPU-201  
 Serial number of module: S C-E3VC49142014  
 Plant identification:  
 Basic Hard...

37.80.24.177

Telekom Deutschland GmbH  
 Added on 2015-03-17 20:37:41 GMT  
 Germany  
[Details](#)

Siemens, SIMATIC NET, SCALANCE M874-3, 6GK5 874-3AA00-2AA2, HW: Version 1, FW: Version V01.01.00, SVPE9132427

88.220.49.80

Exatel S.A.  
 Added on 2015-03-17 19:16:54 GMT  
 Poland  
[Details](#)

Siemens, SIMATIC, S7-200

212.10.179.84

d40ab354.rev.stofanet.dk  
 Telia Stofa A/S  
 Added on 2015-03-17 18:41:20 GMT  
 Denmark, Vamdrup  
[Details](#)

Siemens, SIMATIC, S7-200

87.181.15.189

p57B50FBD.dip0.t-ipconnect.de  
 Deutsche Telekom AG  
 Added on 2015-03-17 18:36:35 GMT  
 Germany, Burgrieden  
[Details](#)



**94.218.16.137** dslb-094-218-016-137.094.218.pools.vodafone-ip.de

City **Ostfildern**

Country **Germany**

Organization **Vodafone DSL**

ISP **Vodafone DSL**

Last Update **2015-03-21T14:39:08.657411**

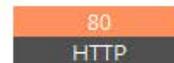
Hostnames **dslb-094-218-016-137.094.218.pools.vodafone-ip.de**

ASN **AS3209**

## Ports



## Services

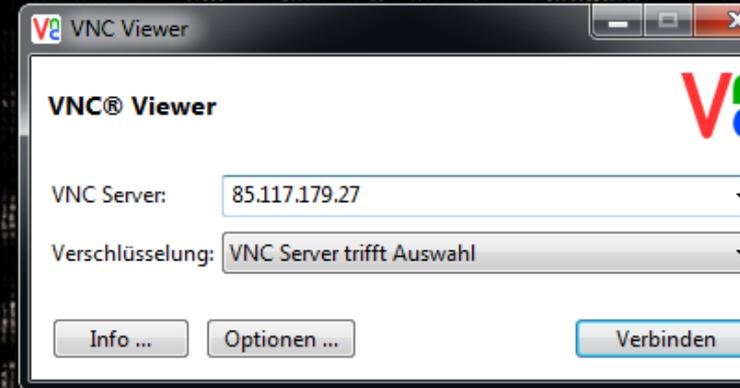


**dvr1614n web-cam httpd**

HTTP/1.1 200 OK  
Connection: close  
Cache-Control: no-cache  
Server: SQ-WEBCAM  
CONTENT-LENGTH: 2933

# VNC Viewer

- Virtual Network Computing
- Remoteverbindungen
- plattformunabhängig
- basiert auf Remote Framebuffer Protocol (RFB)  
→ Port 5900
- viele Industriesteuerungsanlagen  
ohne Authentifizierung über VNC erreichbar



# Das vernetzte Haus

IP-Symcon: Ihre Lösung für ein smartes Zuhause



# Kläranlage



# Solaranlage

78.43.162.131/?page=001.html&lang=de

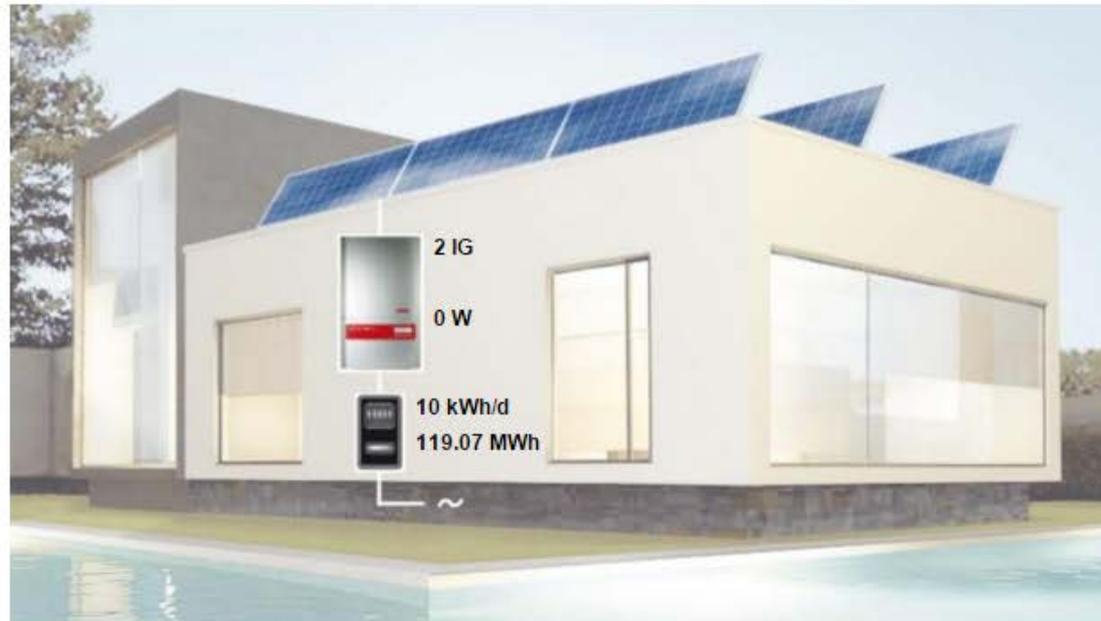


Fronius Datalogger Web

Aktuelle Gesamtansicht

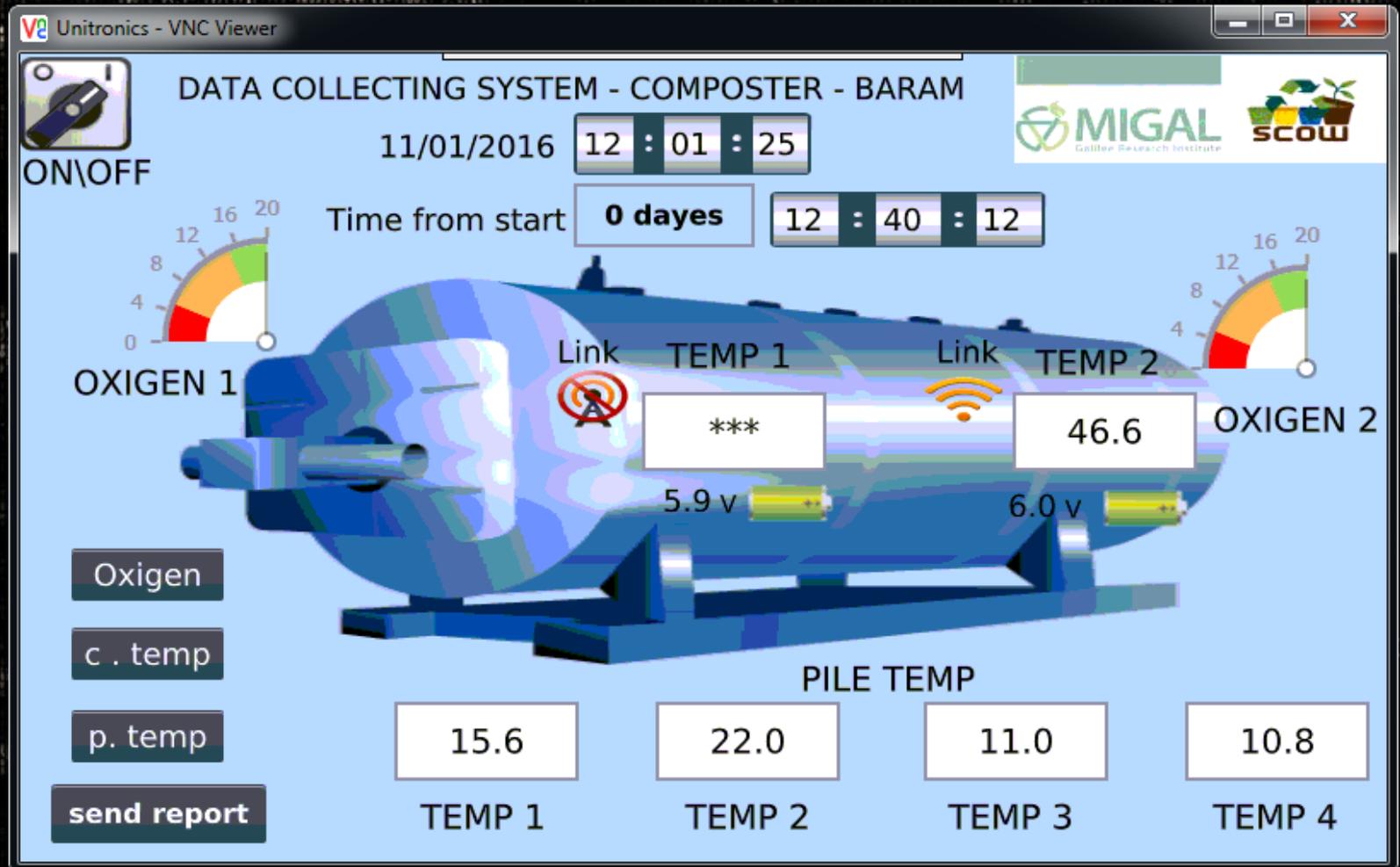
de ?

- Aktuelle Gesamtansicht
- Aktuelle Vergleichsansicht
- Einstellungen



CO <sub>2</sub> -Ersparnis heute	5.3 kg
CO <sub>2</sub> -Ersparnis gesamt	63.11 t
Ertrag heute	3.4 EUR
Ertrag gesamt	4048.82 EUR

# Kompostierer (Israel)



Gefunden über SHODAN-Webseite (Jan 2016)

# Krematorium

Disconnect Options Clipboard Send Ctrl-Alt-Del Refresh

OPERATOR ID  COOLDOWN 9 MINUTES

CASE ID

**OVERRIDES**

Master Timer

Afterburner

C. Burner #1

Throat Air

Hearth Air

Pollution Ctrl

**CASE INFO**

Size:

Container:

Gender:

Case # of Day:

DEFAULTS

Infant

PRESET 2

PRESET 3

ELAPSED TIME 1 : 52

22 % OXYGEN

A/B T/A H/A CB1

752 Deg

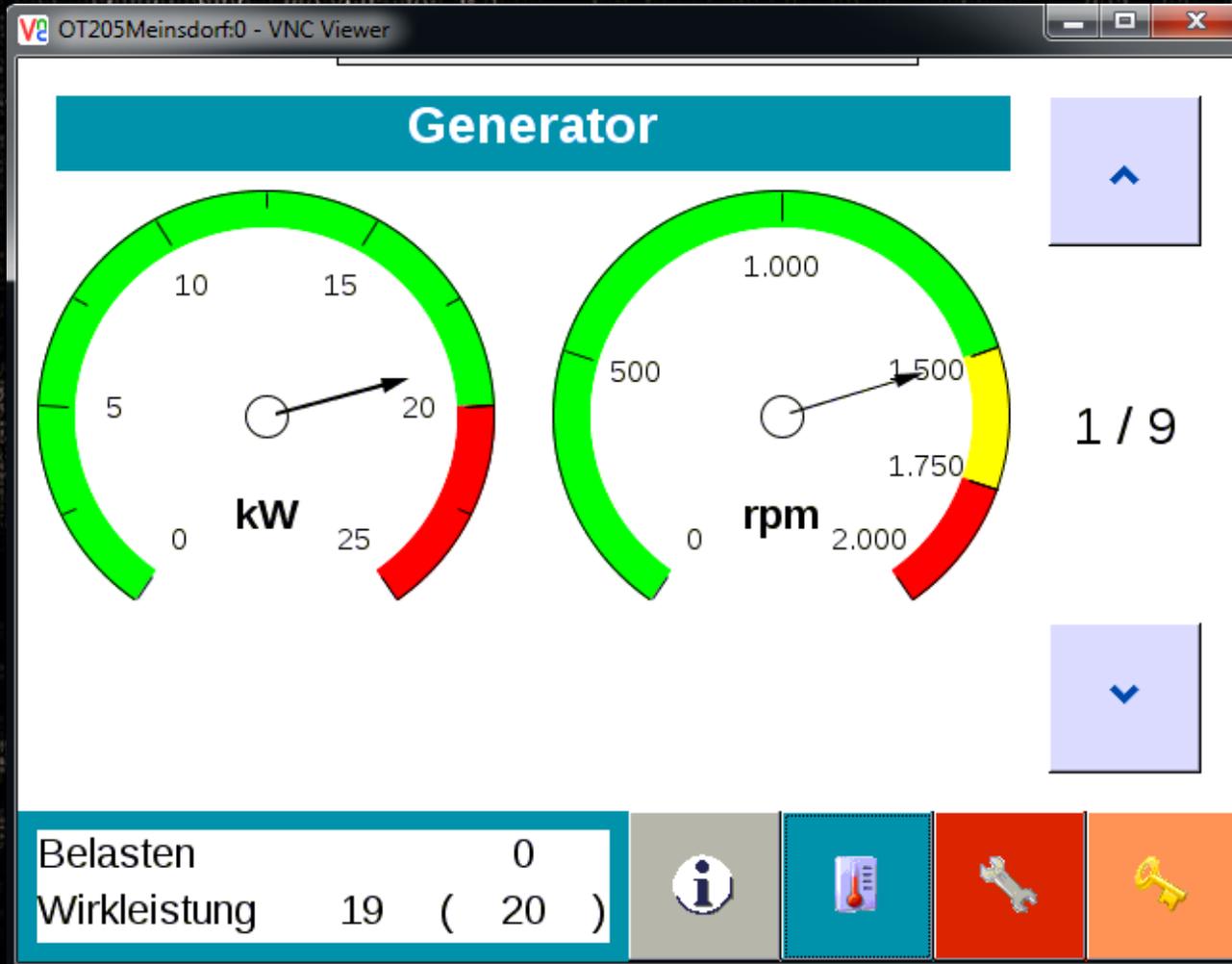
Datalog Enabled

ABORT CYCLE START EXIT

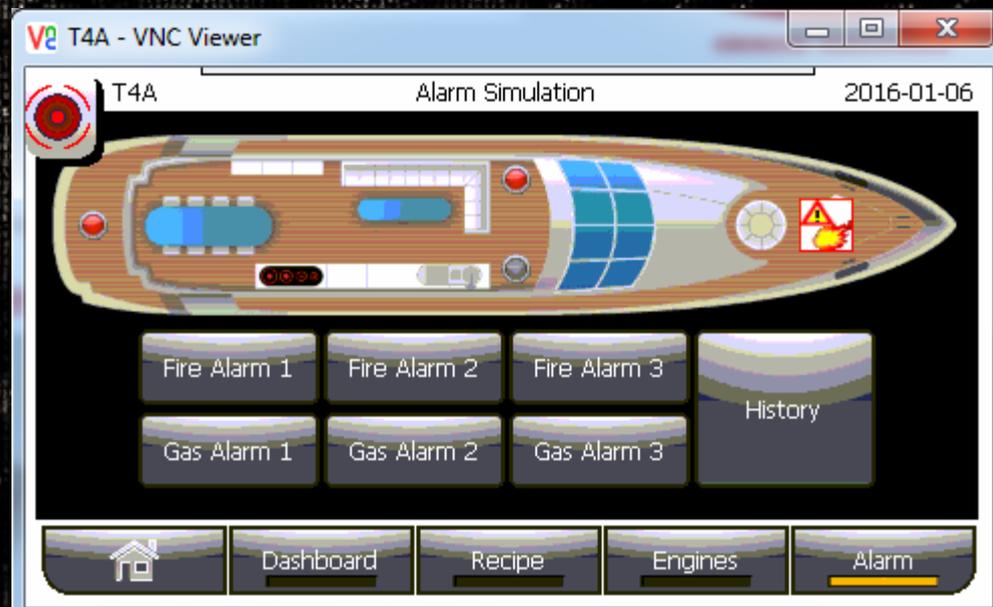
6/6/2012 10:28:47 PM

The image shows a control interface for a crematorium. At the top, there are menu options: Disconnect, Options, Clipboard, Send Ctrl-Alt-Del, and Refresh. Below this, the OPERATOR ID is 'sh' and the COOLDOWN time is 9 MINUTES. The CASE ID field is empty. On the left, there are two main sections: 'OVERRIDES' and 'CASE INFO'. The 'OVERRIDES' section includes Master Timer (1 : 00), Afterburner (OFF), C. Burner #1 (00 : 30), Throat Air (01 : 00), Hearth Air (00 : 15), and Pollution Ctrl (ON). The 'CASE INFO' section includes Size, Container, Gender, and Case # of Day, each with a dropdown menu. Below these are buttons for DEFAULTS, Infant, PRESET 2, and PRESET 3. The main area on the right features a 3D cutaway diagram of the furnace. It shows three burners (A/B, T/A, H/A) and a container (CB1) with a temperature of 752 Deg. The oxygen level is 22%. The elapsed time is 1 : 52. A 'Datalog Enabled' indicator is present. At the bottom, there are buttons for ABORT, CYCLE START, and EXIT. The date and time 6/6/2012 10:28:47 PM are displayed at the bottom left.

# Stromgenerator



Generator Deutschland, Meinsdorf IP: 87.187.0.194



# Wasser-Tanks(USA)

QTERM-A12 - VNC Viewer

Back

## Tanks

LOGOUT

	Top Level	Water Thickness		Temperature	
TANK 1	18.0	14.5	in	28.0	degF
TANK 2	44.5	34.5	in	34.0	degF
TANK 3	95.5	24.5	in	38.0	degF
TANK 4	47.5	12.5	in	39.0	degF
TANK 5	120.0	63.5	in	43.0	degF
TANK 6	9.0	6.0	in	12.0	degF
TANK 7	16.0	13.0	in	24.0	degF
TANK 8	16.5	7.0	in	26.0	degF

Overview Selection

BMS Selection

Coriolis Selection

Tanks

Site

Wireless

Alarm Level 100.0

ESD Level 226.0

Gefunden über SHODAN-Webseite (Dez 2015)

# Kompressoren (Spanien)



Gefunden über SHODAN-Webseite (Dez 2015)

# 4. SCADA - Industriesteuerungen

- SCADA - Supervisory Control and Data Acquisition
- SCADA → verwendet bei vielen kritischen Infrastrukturen zum Monitoring und zur Kontrolle von Industriesteuerungen

# Industrial Control Systems (ICS)

- Beispiele von ICS:
  - Steuerung der Klimaanlage in einem Bürogebäude
  - Steuerung der Turbinen in einem Kraftwerk
  - Beleuchtung in einem Theater, Kino
  - Industrieroboter
  - .....

# SCADAhacker

Think like a **hacker**...  
to secure industrial control systems.

SCADA**hacker**.com



Home

Training

Resources

Tools

Library

Dashboard

Newsletter

Blog

About

Contact

... but also how these systems are configured  
and operated for use within  
critical infrastructure

## IF YOU HAVE BEEN WAITING FOR THE 10-DAY INTENSE COURSE, A NEW TRAINING OPPORTUNITY IS NOW AVAILABLE

The interest in the intense, immersion 10-day program on ICS implementation and security has been overwhelming. This course is not currently scheduled for public offerings. However ... SCADA**hacker** has joined forces with leading system integrator Lin & Associates of Phoenix, Arizona to offer a unique opportunity to learn the basics of ICS configuration and operation, in a public 3-day workshop scheduled for March 3-5 (optional 1-day ICS workshops available on March 6). These 4-days provide both lecture and hands-on modules, and provide an opportunity for attendees to get "up close and personal" with the systems really used to control critical infrastructure. No virtual PLCs, Raspberry Pi, or "toy" SCADA equipment - real ICS equipment used at the heart of the industrial automation and control industry.

After enjoying a weekend in beautiful Phoenix where you can visit landmarks like the Grand Canyon, Petrified National Park, Sedona, Flagstaff and others, the 5-day advanced "Understanding, Assessing and Securing Industrial Control Systems" course will be offered March 9-13.

The need for this type of opportunity within the ICS security sector is critical in understanding the real-world aspects of securing operational systems. To facilitate involvement, students that register for BOTH the 3-day workshop and the 5-day security course will receive a SPECIAL DISCOUNT equal to the registration fee for the 3-day workshop. In other words, the 3-day workshop is FREE when attending both. As a SPECIAL BONUS, anyone who registers for either the DCS Configuration or HMI Scripting workshop will receive a \$50 Amazon Gift Card for each optional session. No where else can you receive 9-days of training from leading industry experts for the price of \$4,550 !!!

Login

Register

Site Search

### ICS Training

Understanding, Assessing  
and Securing ICS -  
Advanced 5-day Course  
[Course Details](#)

**2 WEEKS OF TRAINING  
FOR THE PRICE OF 1 !!!**

**March 3-6, 2015**  
ICS Configuration &  
Operation Workshop  
Embassy Suites  
Phoenix, Arizona  
[Register Now](#)

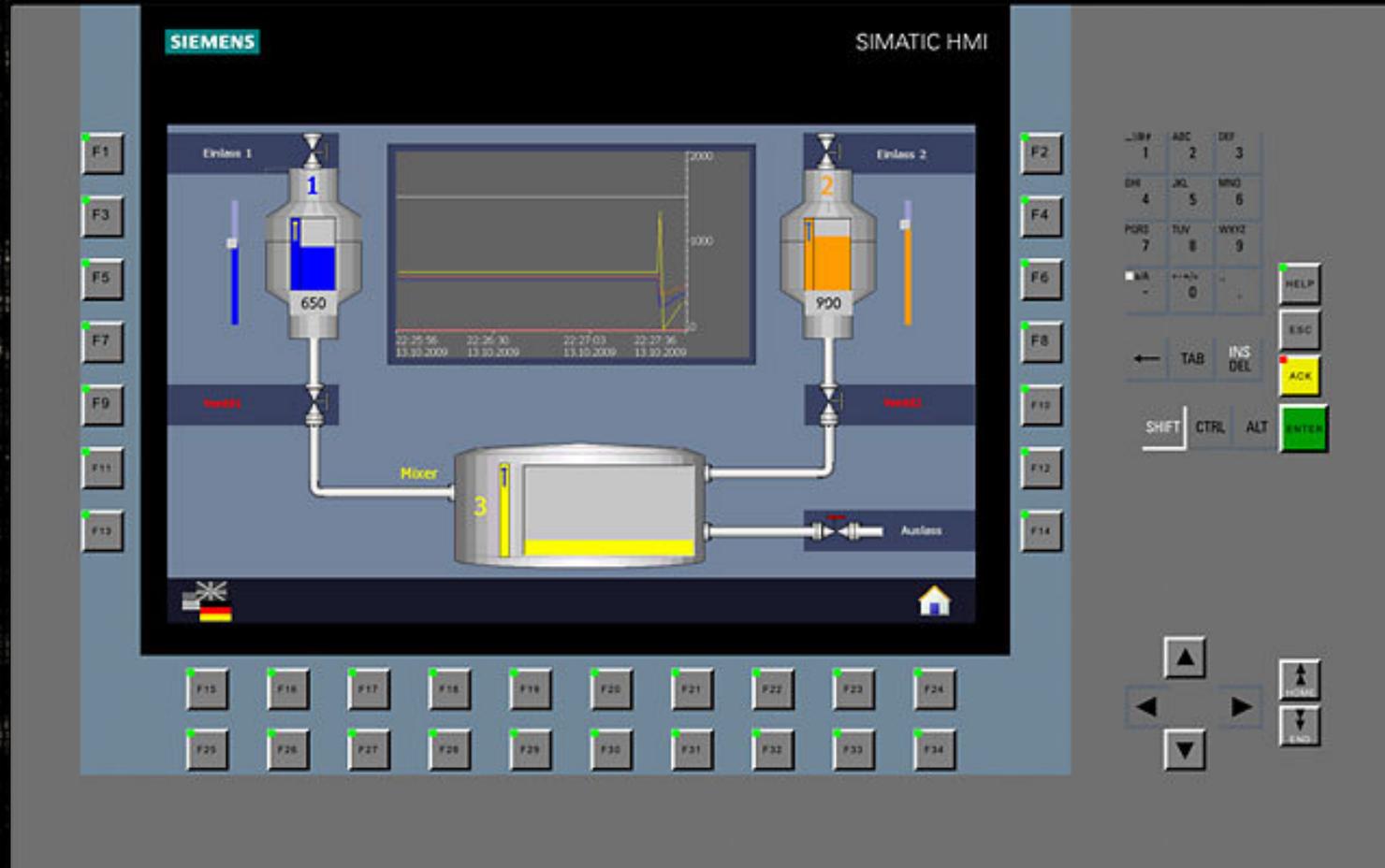
**March 9-13, 2015**  
ICS Cyber Security Training  
Lin & Associates  
Phoenix, Arizona  
[Register Now](#)

**May 18-22, 2015**  
ICS Cyber Security Training  
Lambeau Field VIP Suites  
Green Bay, WI  
[Register Now](#)

**New Release**

**Now Available !!!**

# Industrial Control Systems (ICS)



Fernsteuerungs-App von Siemens [Bildquelle: ct-Online-Artikel 5/2013]

# Shodan - Industrial Control Systems

## Protocols

The following protocols are some of the languages that the industrial control systems use to communicate across the Internet. Many of them were developed before the Internet became widely used, which is why Internet-accessible ICS devices don't always require authentication - it isn't part of the protocol!



Modbus is a popular protocol for industrial control systems (ICS). It provides easy, raw access to the control system without requiring any authentication.

[Explore Modbus](#)

### SIEMENS

S7 (S7 Communication) is a Siemens proprietary protocol that runs between programmable logic controllers (PLCs) of the Siemens S7 family.

[Explore Siemens S7](#)



DNP3 (Distributed Network Protocol) is a set of communications protocols used between components in process automation systems. Its main use is in utilities such as electric and water companies.

[Explore DNP3](#)



The Fox protocol, developed as part of the Niagara framework from Tridium, is most commonly seen in building automation systems (offices, libraries, Universities, etc.)

[Explore Niagara Fox](#)



BACnet is a communications protocol for building automation and control networks. It was designed to allow communication of building automation and control systems for applications such as heating, air-conditioning, lighting, and fire detection systems.

[Explore BACnet](#)

### EtherNet/IP

EtherNet/IP was introduced in 2001 and is an industrial Ethernet network solution available for manufacturing automation.

[Explore EtherNet/IP](#)



Service Request Transport Protocol (GE-SRTP) protocol is developed by GE Intelligent Platforms (earlier GE Fanuc) for transfer of data from PLCs.

[Explore GE-SRTP](#)



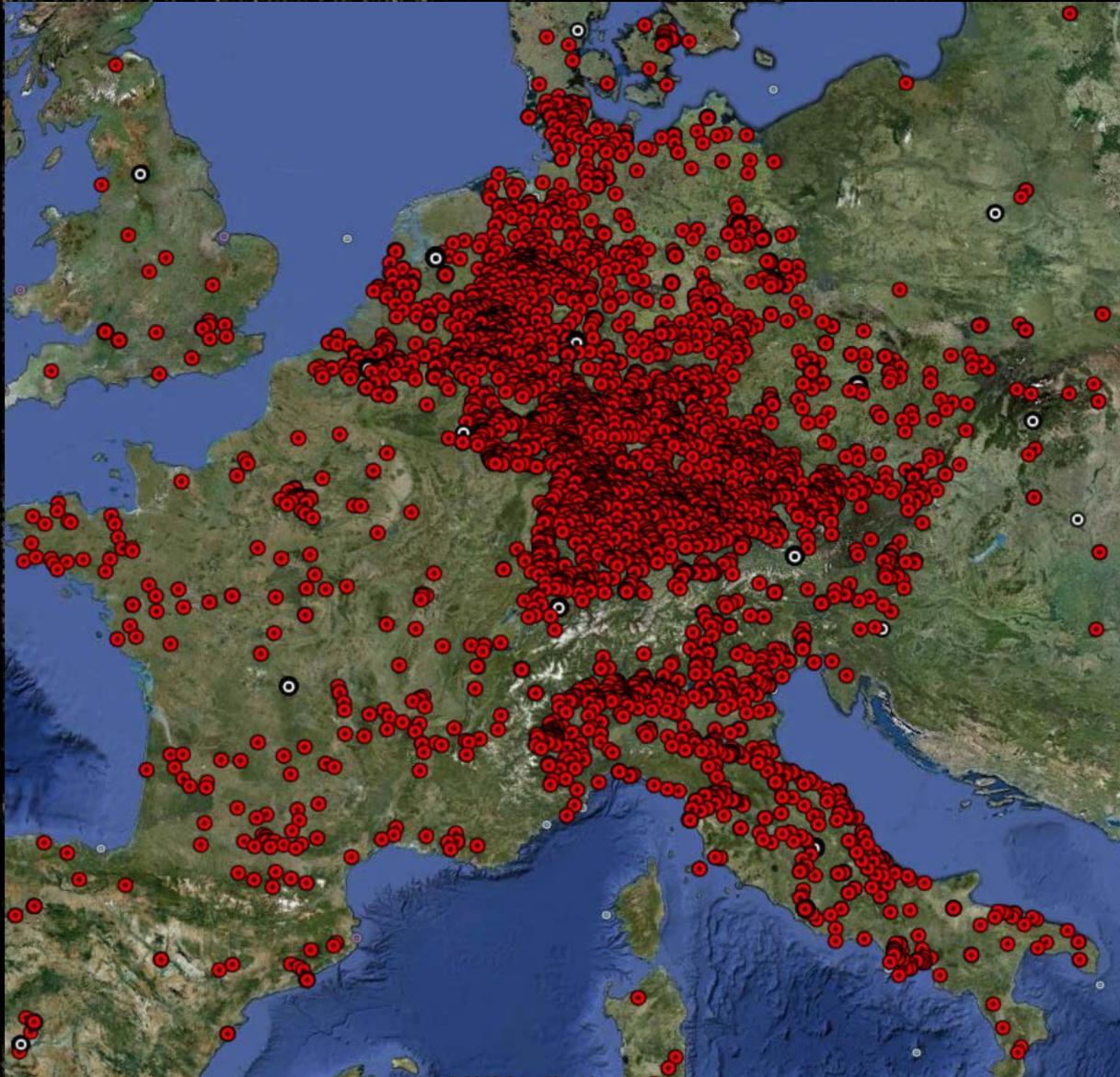
The HART Communications Protocol (Highway Addressable Remote Transducer Protocol) is an early implementation of Fieldbus, a digital industrial automation protocol. Its most notable advantage is that it can communicate over legacy wiring.



PCWorx is a protocol and program by Phoenix Contact used by a wide range of industries.

[Explore PCWorx](#)

# Industrial Risk Assessment Map (IRAM)



# Kritische Infrastruktur

- Energieversorger
- Wasserversorger
- Atomkraftwerke
- Krankenhäuser
- Banken
- Verkehrssteuerung
- Provider (ISP)
- Chemiewerke
- .....

# Maßnahmen

- Projekte, Services
- Sicherheitsüberprüfungen, Audits
- Security Check,
- Vulnerabilitätstests,
- Penetrationstests,
- Computerforensische Untersuchungen

# IT-Sicherheitsgesetz – Erfahrungen, Konsequenzen

- Guter Schritt in die richtige Richtung!
- Kritische Infrastrukturen MÜSSEN regelmäßig geprüft und zertifiziert werden
- Branchenspezifische Lösungen sind nötig

• **ABER**

# Konsequenzen - I

Wie brauchen viel mehr

- Geld,
- Planstellen
- Manpower
- Ausbildung,
- Qualifizierung, Weiterbildung

um unsere kritischen Infrastrukturen zu schützen.

(gilt für alle Bundesbehörden, Landesbehörden,  
Verwaltungen, Unternehmen,...)

# Konsequenzen - II

Klare Richtlinien,  
Arbeitsanweisungen,  
Branchenspezifische Zertifizierungen,  
Regelung des Umganges mit Sicherheitstools,  
Anonymisierung der Meldungen,

Was passiert nach der Meldung???

Cybersecurity-Versicherung abschließen! (z.B. HisQox)

# Kontakt



Email: [creutzburg@th-brandenburg.de](mailto:creutzburg@th-brandenburg.de)