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

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-Herzschrittmacher hat uns benachrichtigt, dass wir hier gleich gebraucht werden
GDD Forever!
GRESER&Lenz

Internet 4.0

Eine Welt ohne Datenschutzbeauftragte. Wollen wir das?

Gesundheitsvorsorge per Handy: Überlegene Technik setzt sich durch

Europäische Datenschutzgrundverordnung: Mit dem Datenschutz in Urlaub

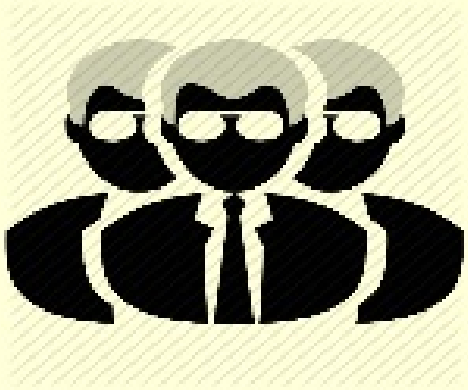
Types of Hackers.

White Hats

Black Hats

Grey Hats

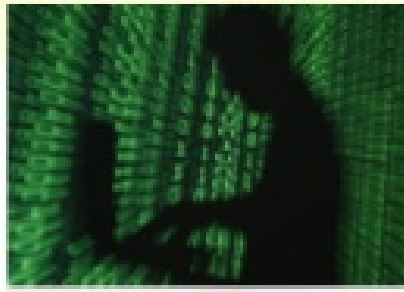
Srcript Kiddies



Spy Hackers

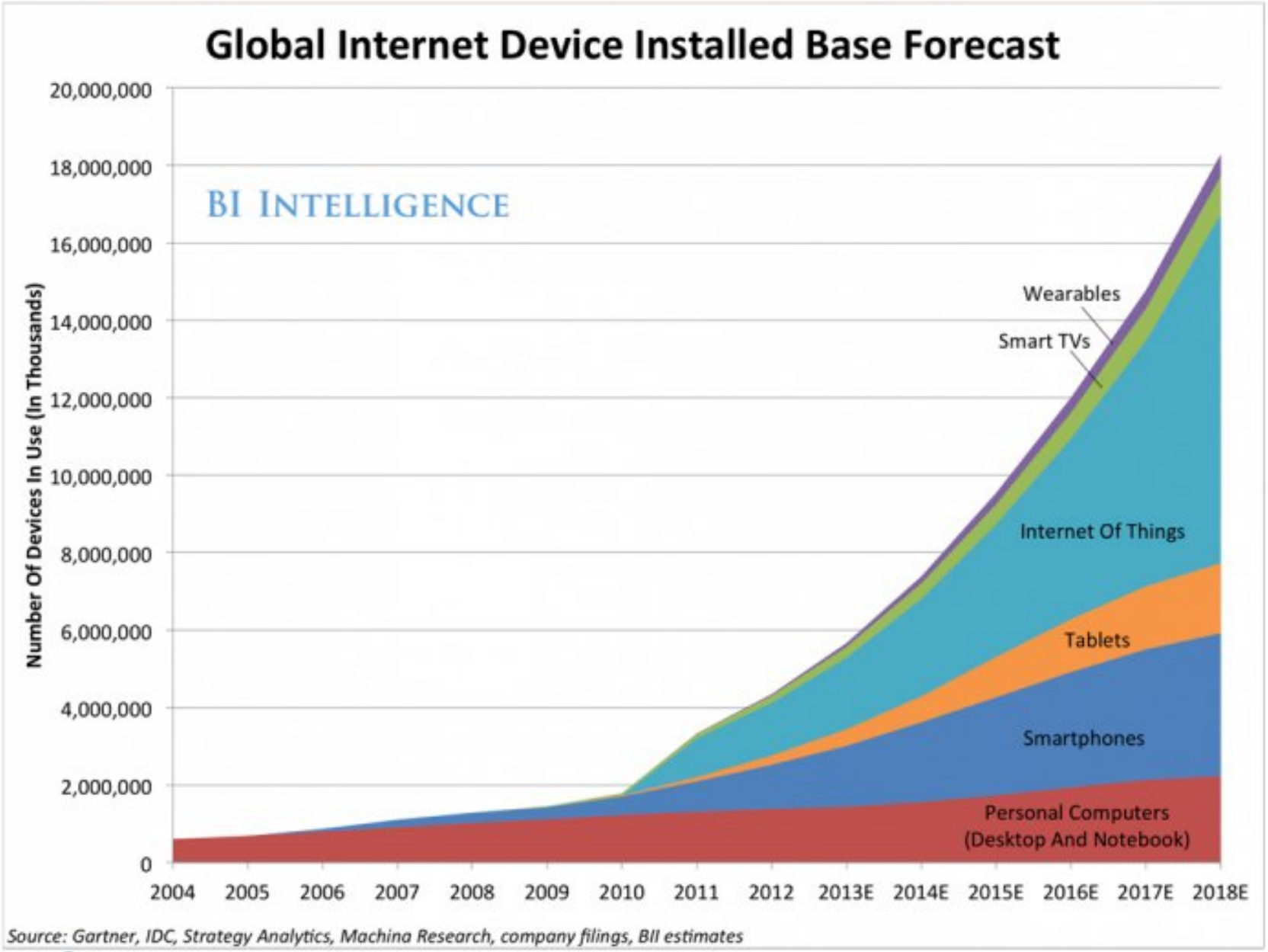
Suicide Hackers

Cyber Terrorist



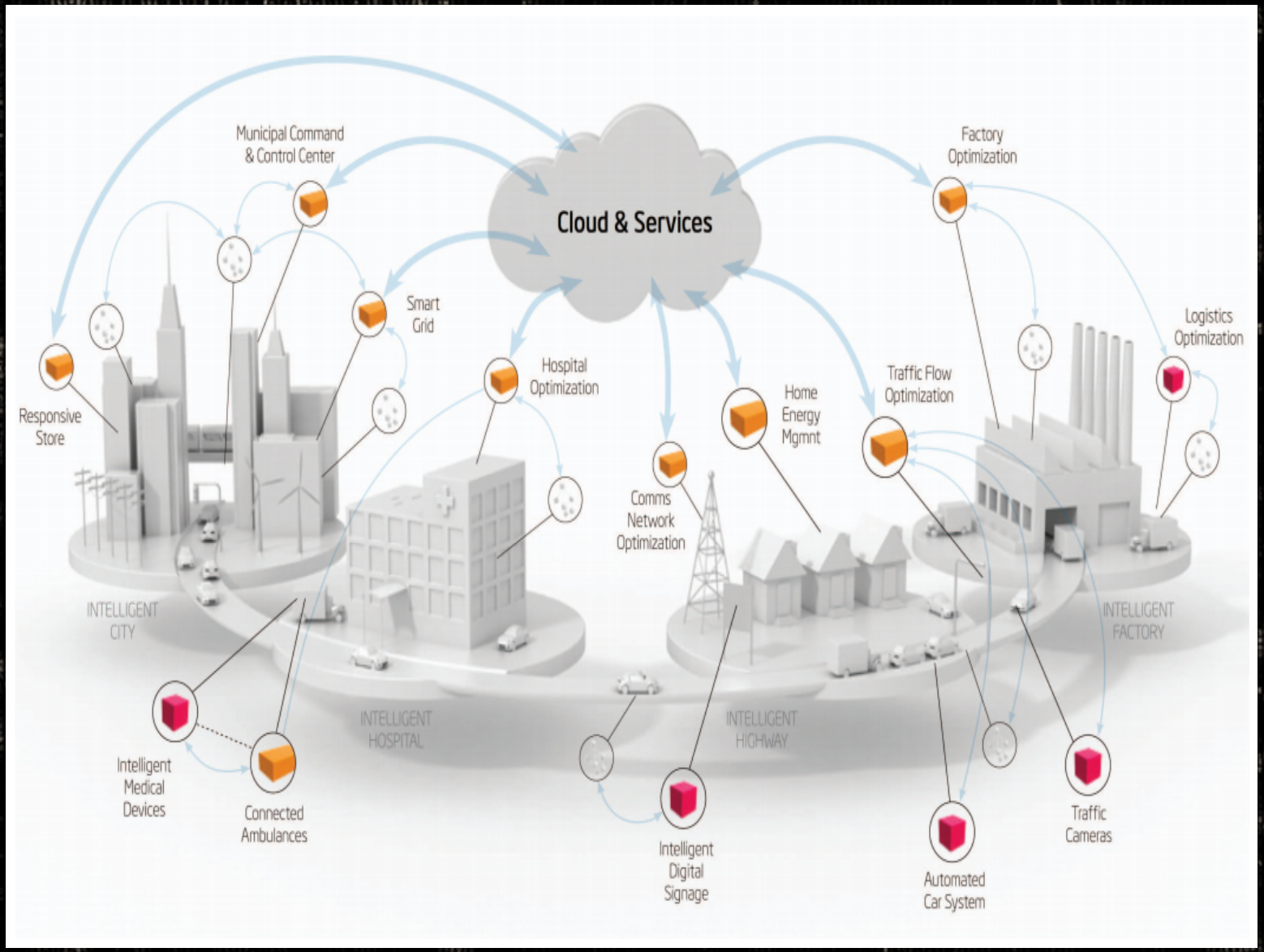
State Sponsored

Tech Chart of the Day



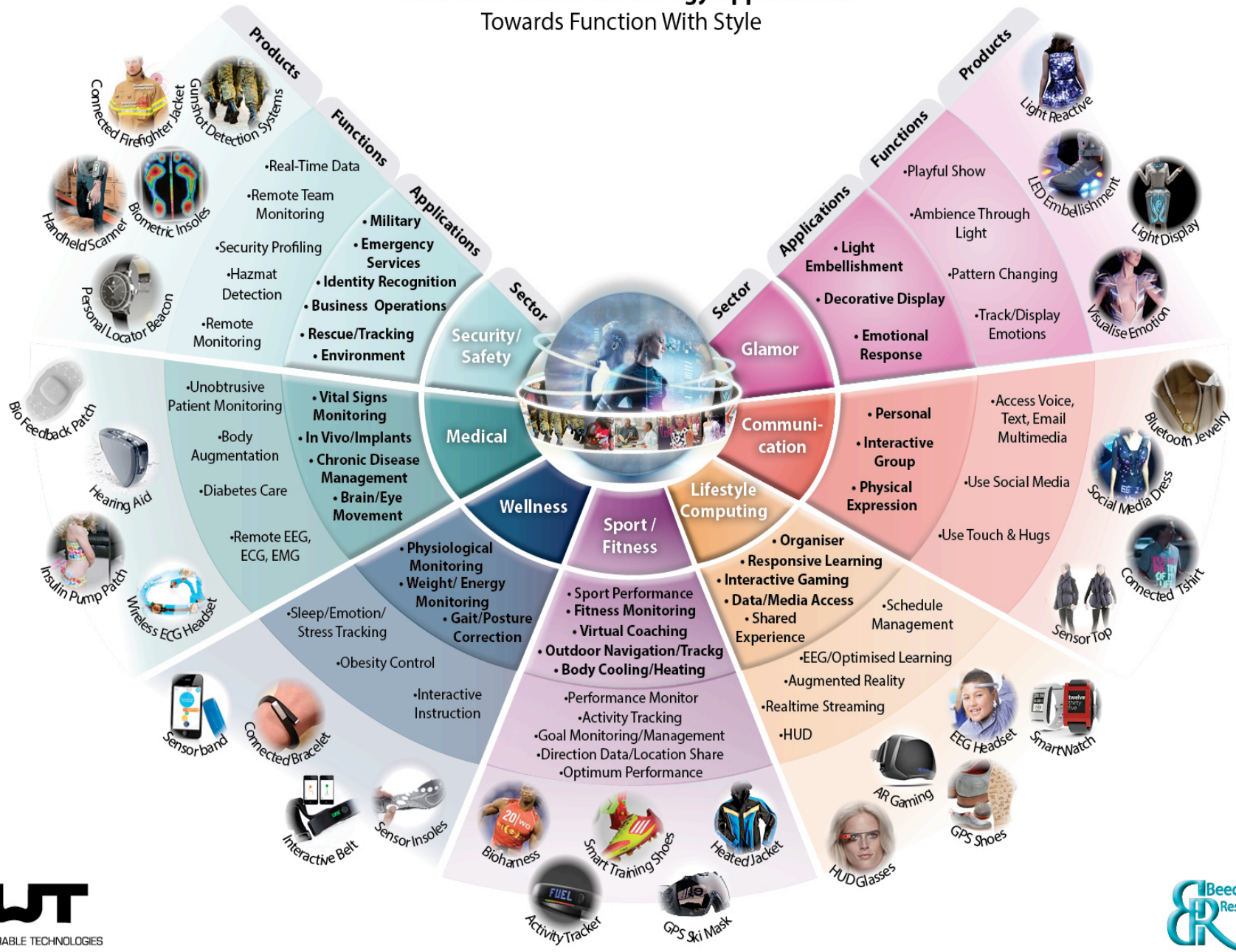
BUSINESS INSIDER

Internet der Dinge (Internet of Things)



World of Wearable Technology Applications:

Towards Function With Style

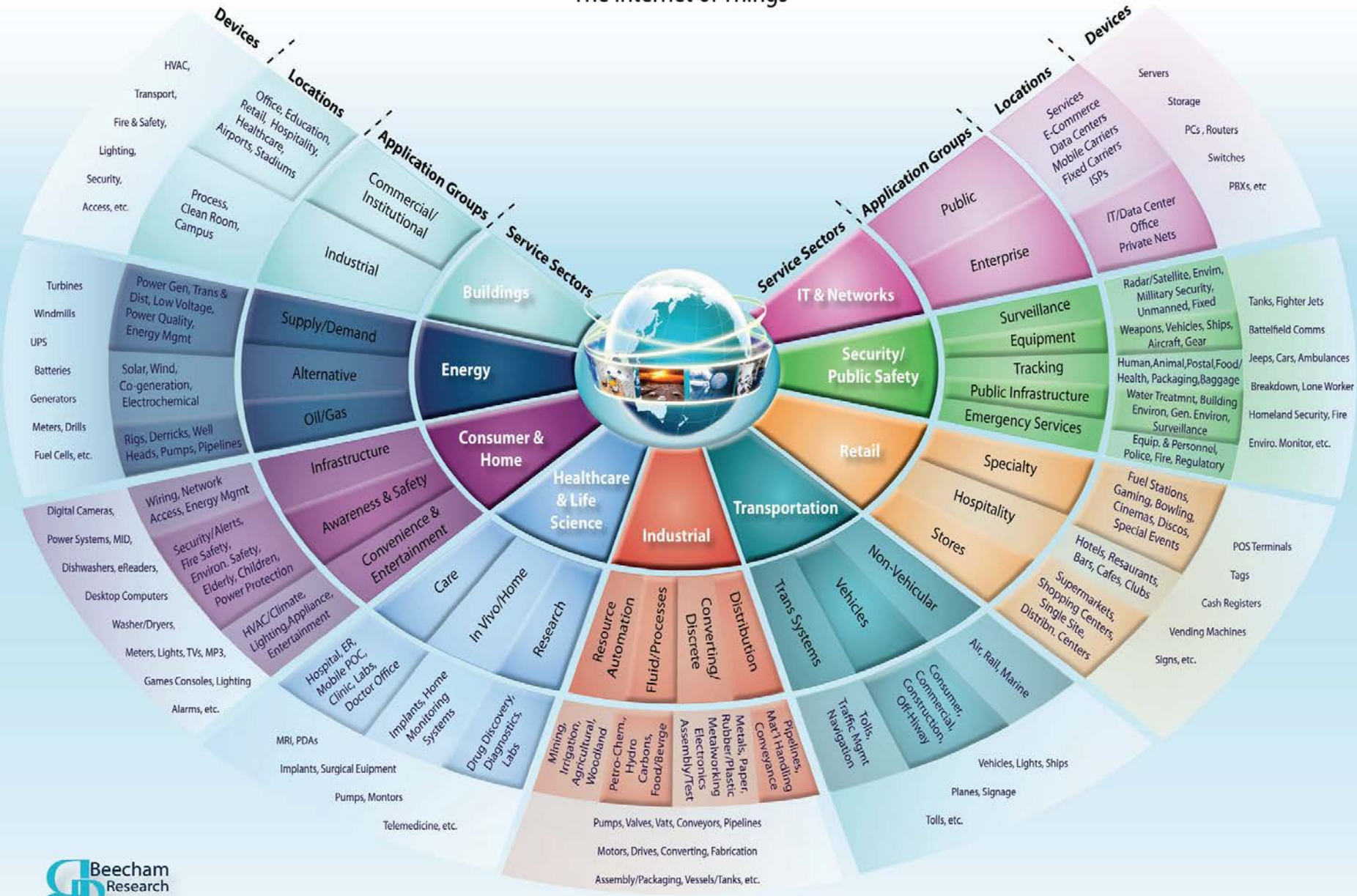


WEARABLE TECHNOLOGIES

Beecham Research

M2M World of Connected Services

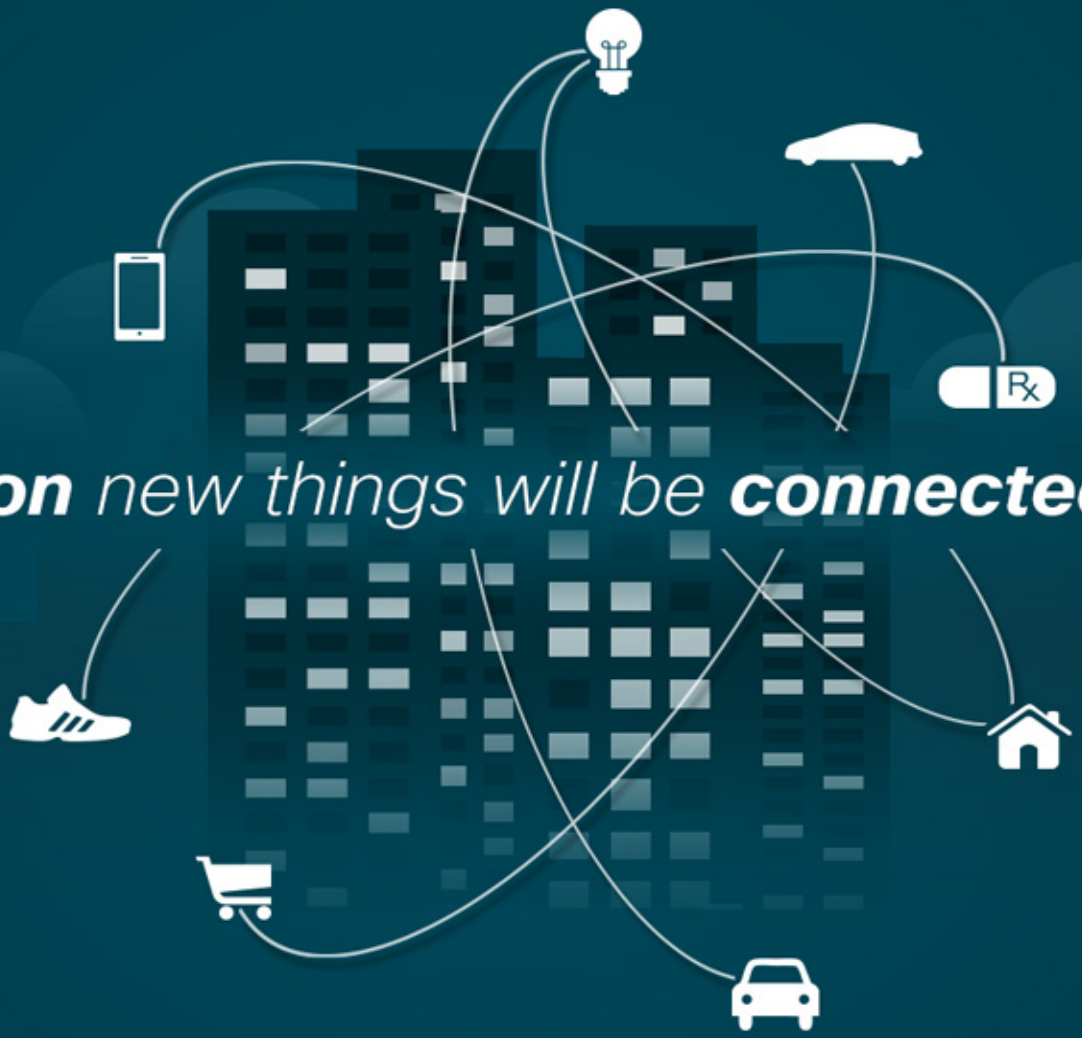
The Internet of Things



Beecham Research

THE INTERNET **OF EVERYTHING** IS HERE.

As the Internet evolves, so will we.



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

#IoE #TomorrowStartsHere

cisco

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.

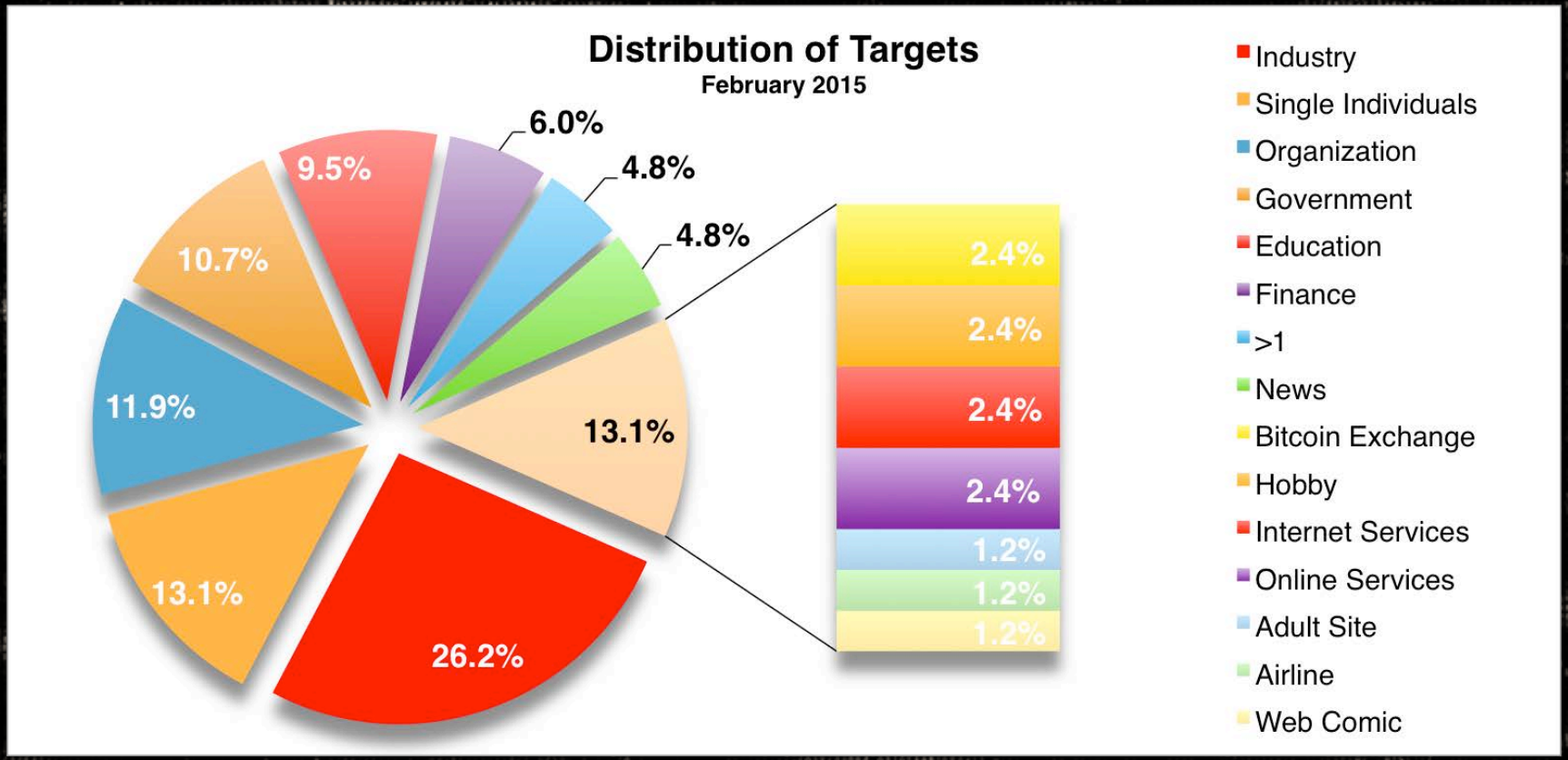
4 Grow Market
Move into new markets quickly by slicing and dicing your product by features, capacity, and more.

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		KLAS TELECOM	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	?	Mad Mimi	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 **36,000** 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	HeaveN		A hacker called HeaveN 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 **18 million** 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 **5,100** 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



SZ Kaspersky: Worauf es Hac ×

www.sueddeutsche.de/digital/sicherheitsexperte-kaspersky-darauf-haben-es-hacker-abgesehen-1.2331946

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.

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

Jenny Knackmuß[a,b], Thomas Möller[b], Wilfried Pommerien[a,c,d], and Reiner Creutzburg[a]

[a]Brandenburg University of Applied Sciences, Department of Informatics and Media
P.O.Box 2132, D-14737 Brandenburg, Germany

[b]Assecor GmbH, Storkower Str. 207, D-10369 Berlin, Germany

[c]Städtisches Klinikum Brandenburg GmbH, Zentrum für Innere Medizin II, Hochstr. 29,
D-14770 Brandenburg, Germany

[d]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

simatic - Shodan Search

https://www.shodan.io/search?query=simatic

Shodan Scanhub Developers View All...

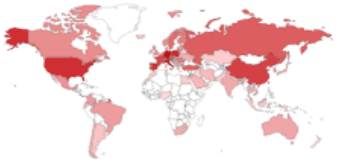
SHODAN simatic

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 ESMTP	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 18:41:26 GMT

Denmark, Vamdrup

Details

```
Siemens, SIMATIC, S7-200
```

87.181.15.189

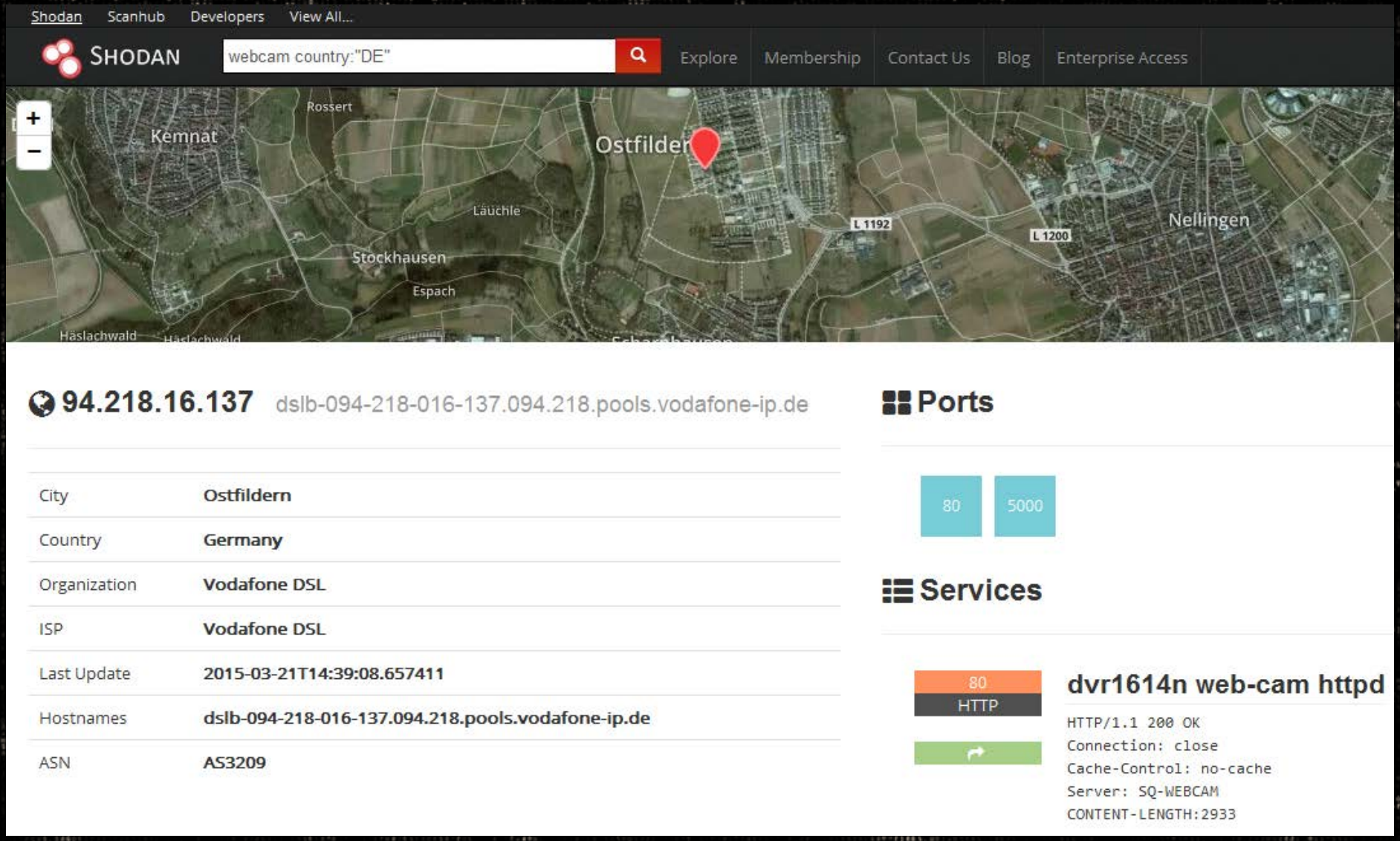
p57B50FBD.dip0.t-ipconnect.de

Deutsche Telekom AG

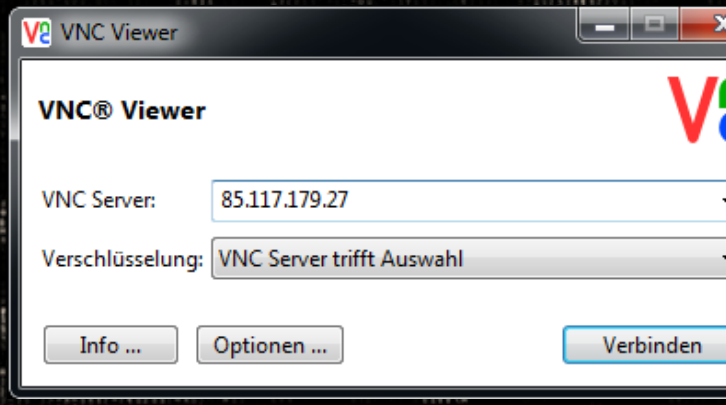
Added on 2015-03-17 18:36:35 GMT

Germany, Burgrieden

Details


Shodan
Scanhub
Developers
View All...
SHODAN
webcam country:"DE"
Explore
Membership
Contact Us
Blog
Enterprise Access
Rossert
Kemnat
Ostfildern
Läuchle
Stockhausen
Espach
L 1192
L 1200
Nellingen
Häslachwald
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
80
5000
Services
80
HTTP
dvr1614n web-cam httpd
HTTP/1.1 200 OK
Connection: close
Cache-Control: no-cache
Server: SQ-WEBCAM
CONTENT-LENGTH:2933

VNC Viewer

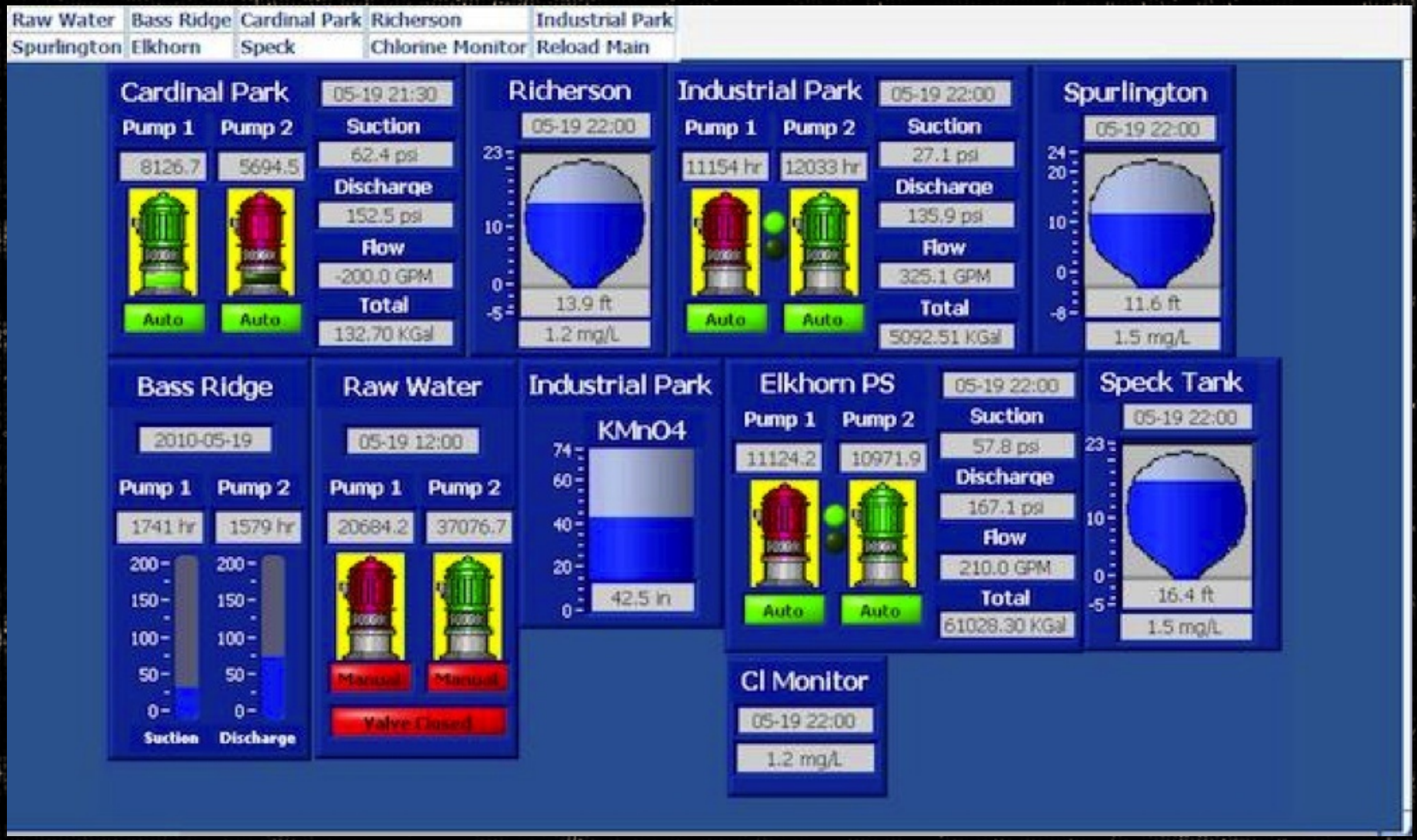


- Virtual Network Computing
- Remoteverbindungen
- plattformunabhängig
- basiert auf Remote Framebuffer Protocol (RFB)
  →Port 5900
- viele Industriesteuerungsanlagen
  ohne Authentifizierung über VNC erreichbar

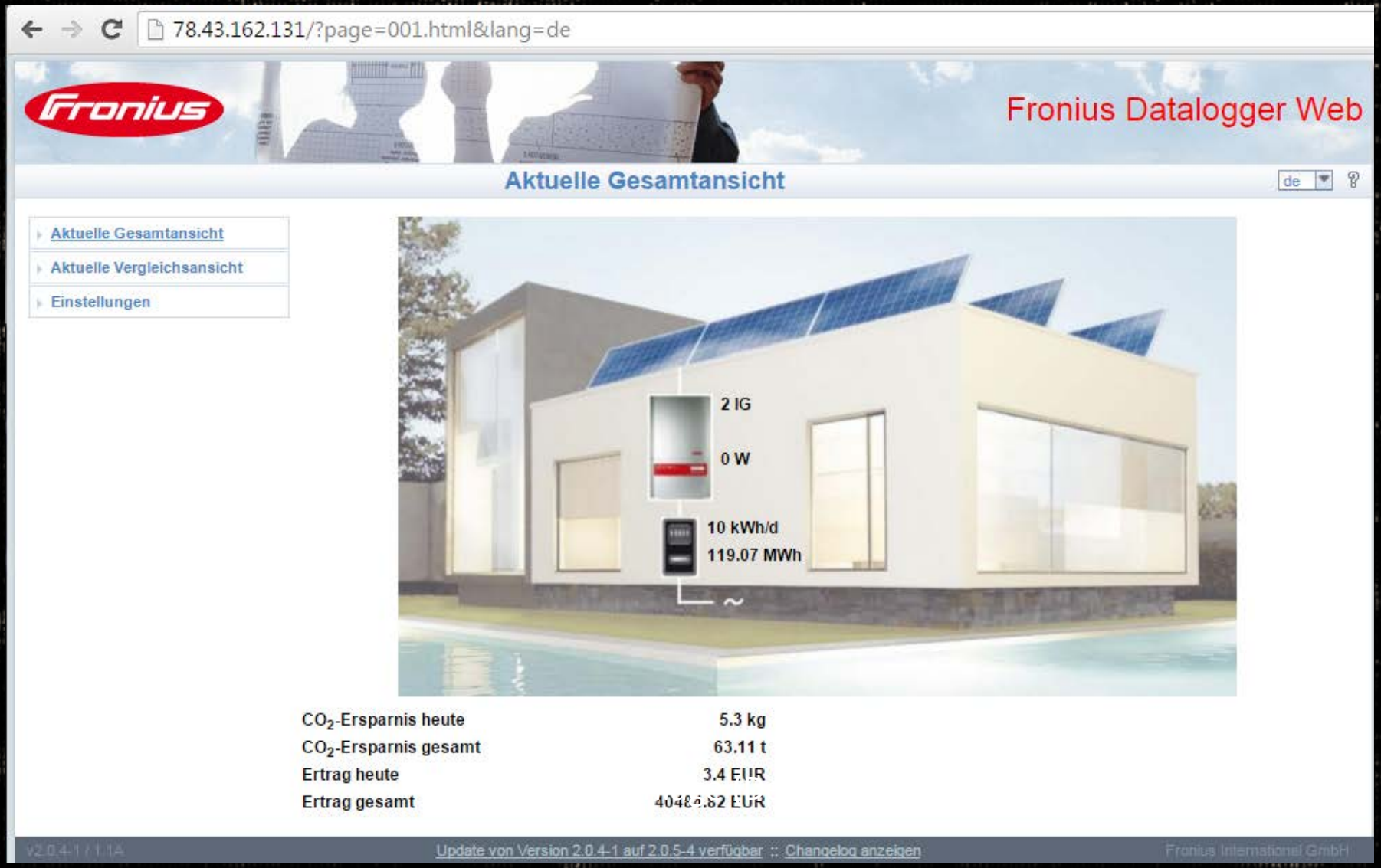
Das vernetzte Haus

https://www.symcon.de/ - Stand 07.01.2016

Kläranlage

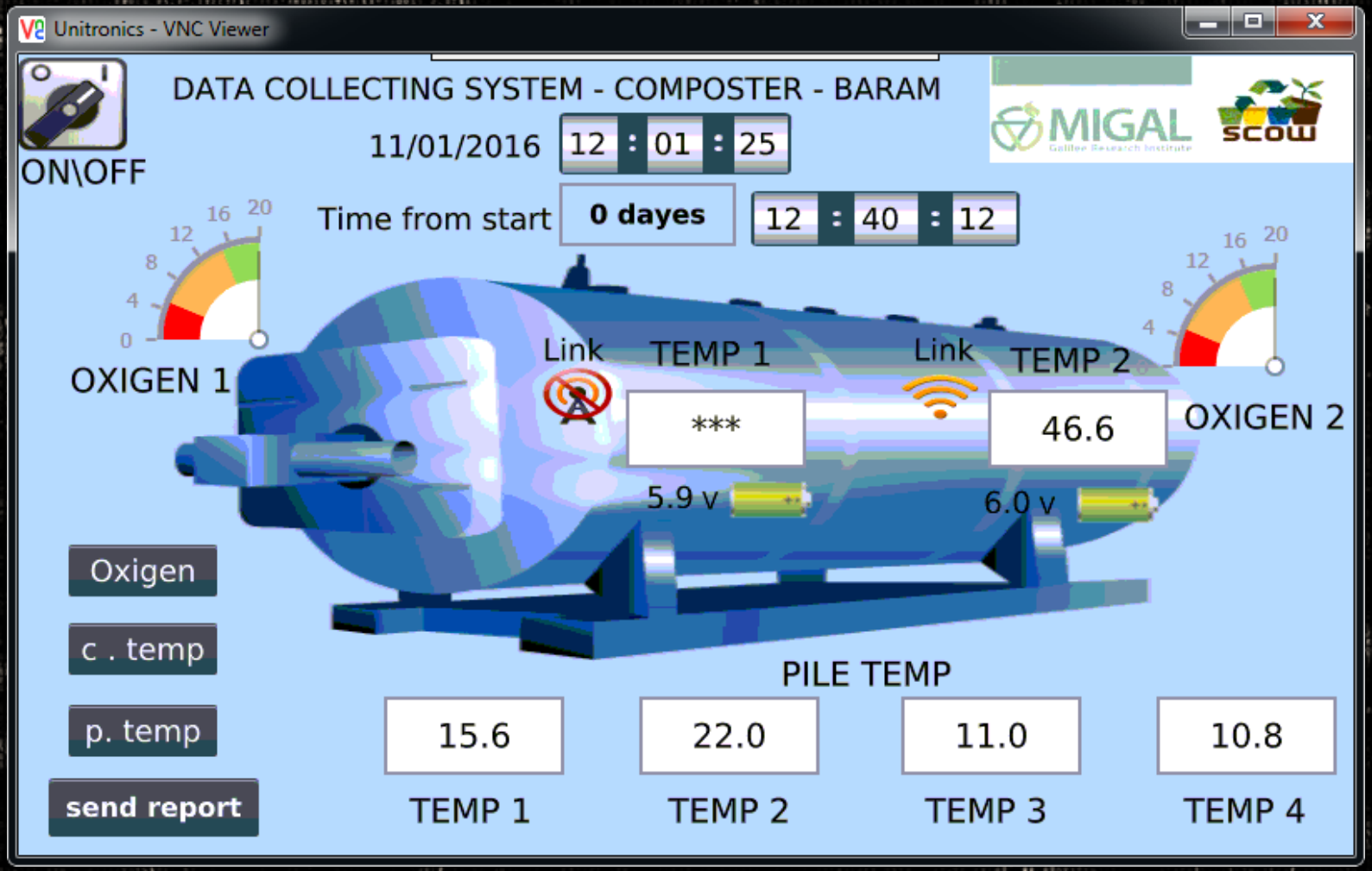

Raw Water
Bass Ridge
Cardinal Park
Richerson
Industrial Park
Spurlington
Elkhorn
Speck
Chlorine Monitor
Reload Main
Cardinal Park
05-19 21:30
Pump 1
Pump 2
8126.7
5694.5
Auto
Auto
Suction
62.4 psi
Discharge
152.5 psi
Flow
-200.0 GPM
Total
132.70 KGal
Richerson
05-19 22:00
23
10
0
-5
13.9 ft
1.2 mg/L
Industrial Park
05-19 22:00
Pump 1
Pump 2
11154 hr
12033 hr
Auto
Auto
Suction
27.1 psi
Discharge
135.9 psi
Flow
325.1 GPM
Total
5092.51 KGal
Spurlington
05-19 22:00
24
20
10
0
-8
11.6 ft
1.5 mg/L
Bass Ridge
2010-05-19
Pump 1
Pump 2
1741 hr
1579 hr
200
150
100
50
0
Suction
Discharge
Raw Water
05-19 12:00
Pump 1
Pump 2
20684.2
37076.7
Manual
Manual
Valve Closed
Industrial Park
KMnO4
74
60
40
20
0
42.5 in
Elkhorn PS
05-19 22:00
Pump 1
Pump 2
11124.2
10971.9
Auto
Auto
Suction
57.8 psi
Discharge
167.1 psi
Flow
210.0 GPM
Total
61028.30 KGal
Speck Tank
05-19 22:00
23
10
0
-5
16.4 ft
1.5 mg/L
Cl Monitor
05-19 22:00
1.2 mg/L

Solaranlage



Gefunden Dezember 2015 via Twitter (Gruppe:scadastrangelove)

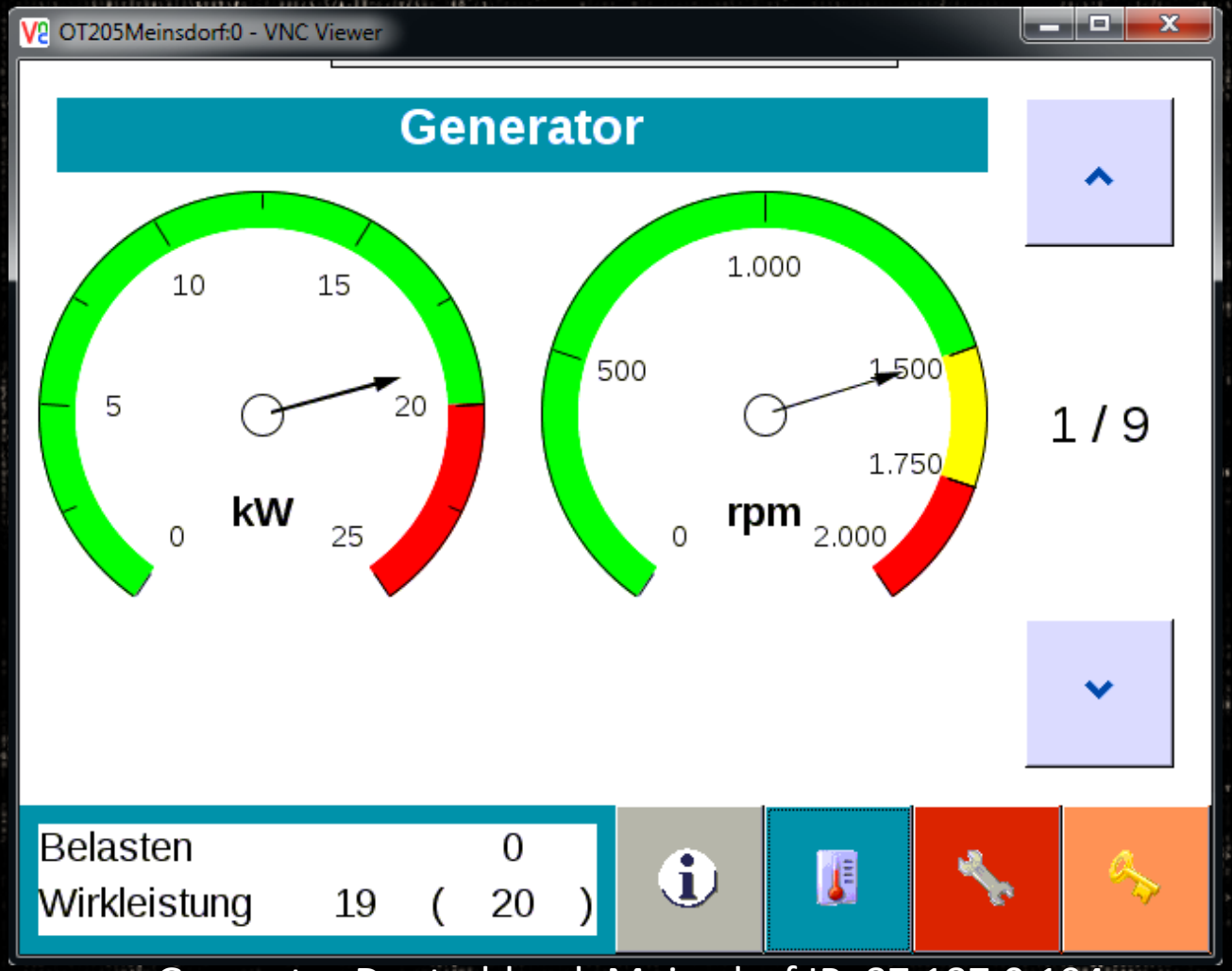
Kompostierer (Israel)



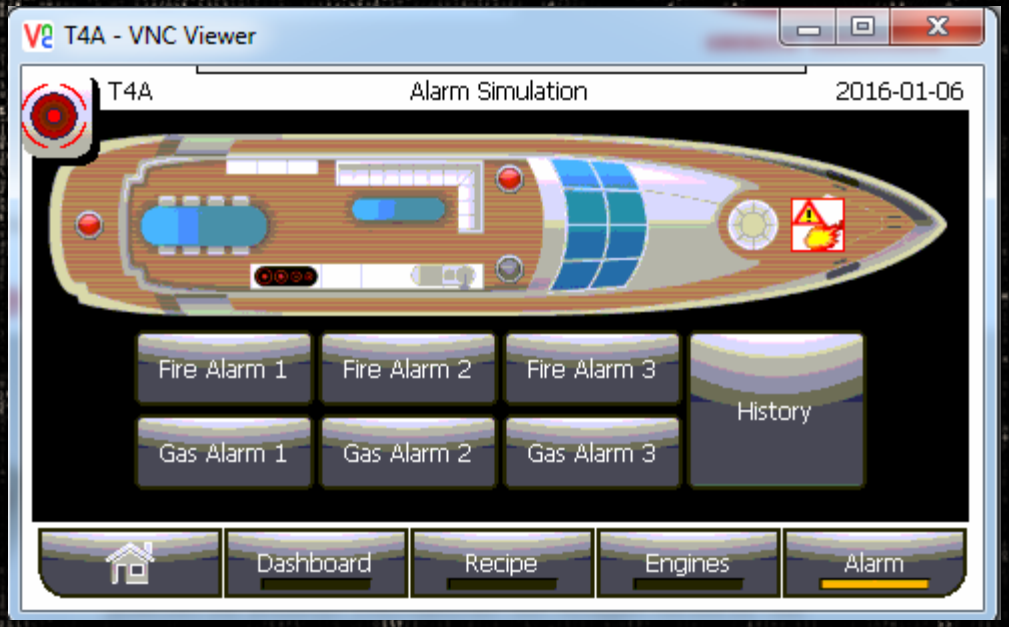
Gefunden über SHODAN-Webseite (Jan 2016)

Krematorium

Stromgenerator



Generator Deutschland, Meinsdorf IP: 87.187.0.194

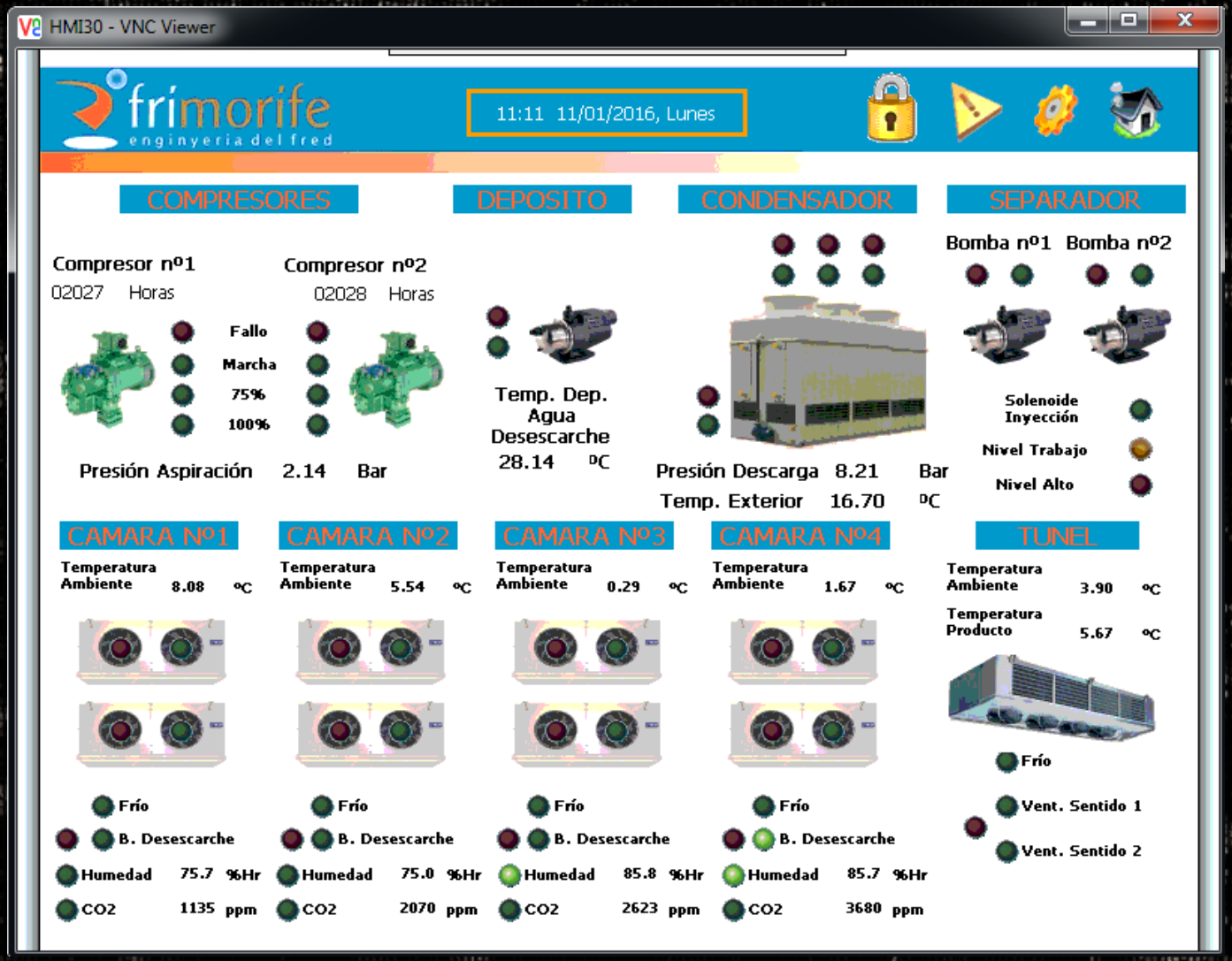


Getwittert Dezember 2015 von Gruppe @medseclinkedin

Wasser-Tanks(USA)

Gefunden über SHODAN-Webseite (Dez 2015)

Kompressoren (Spanien)



Gefunden über SHODAN-Webseite (Dez 2015)

4. SCADA - Industriesteuerungen

- SCADA - Supervisory Control and Data Acquisition

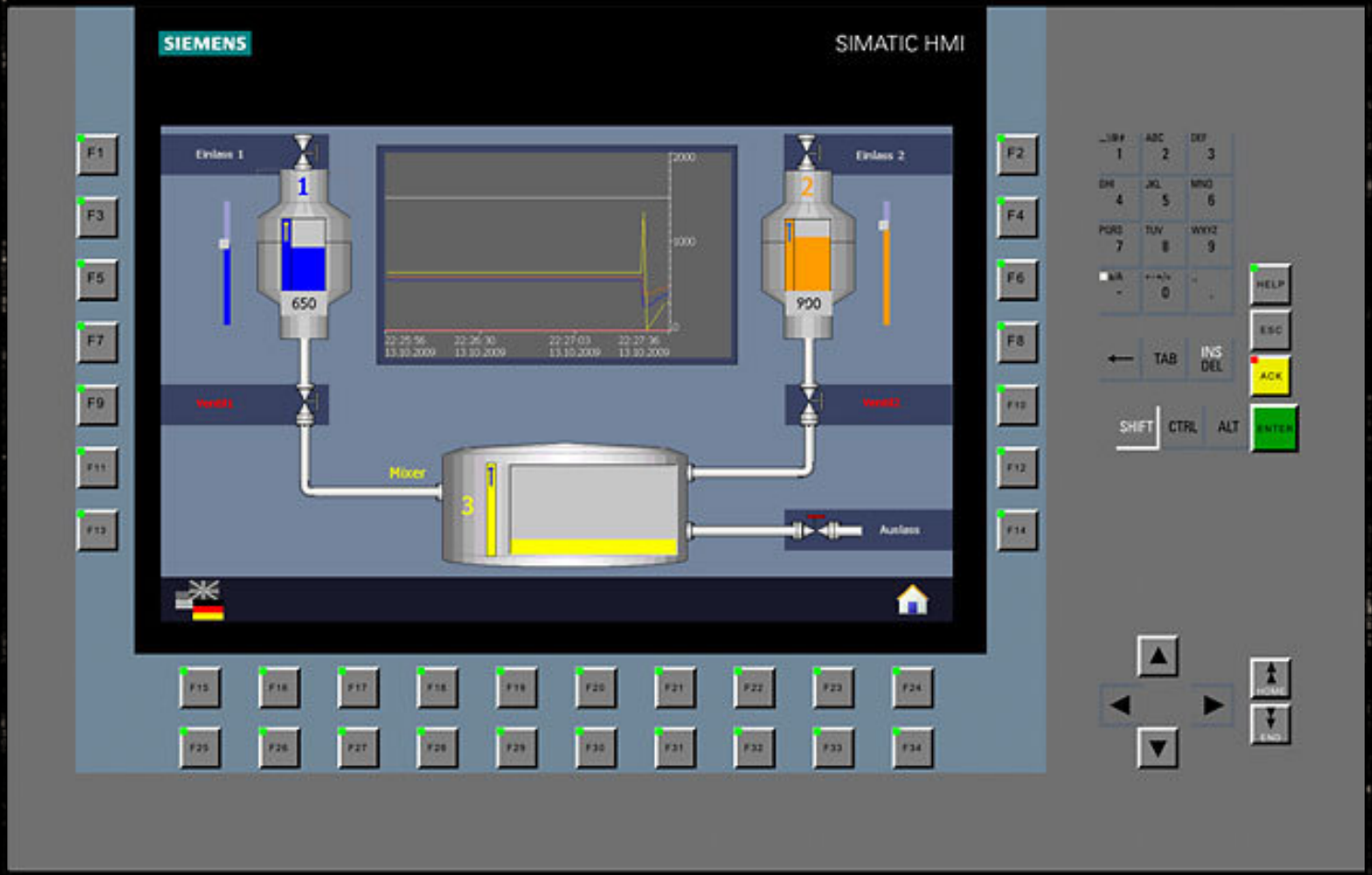
- SCADA → verwendet bei vielen kritischen Infrastrukturen zum Monitoring und zur Kontrolle von Industriesteuerungen

Industrial Control Systems (ICS)

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

SCADAhacker

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 dont always require authentication - it isnt part of the protocol!

Modbus

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

dnp

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

TRIDIUM

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

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

GE Industrial Solutions

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

HART IP

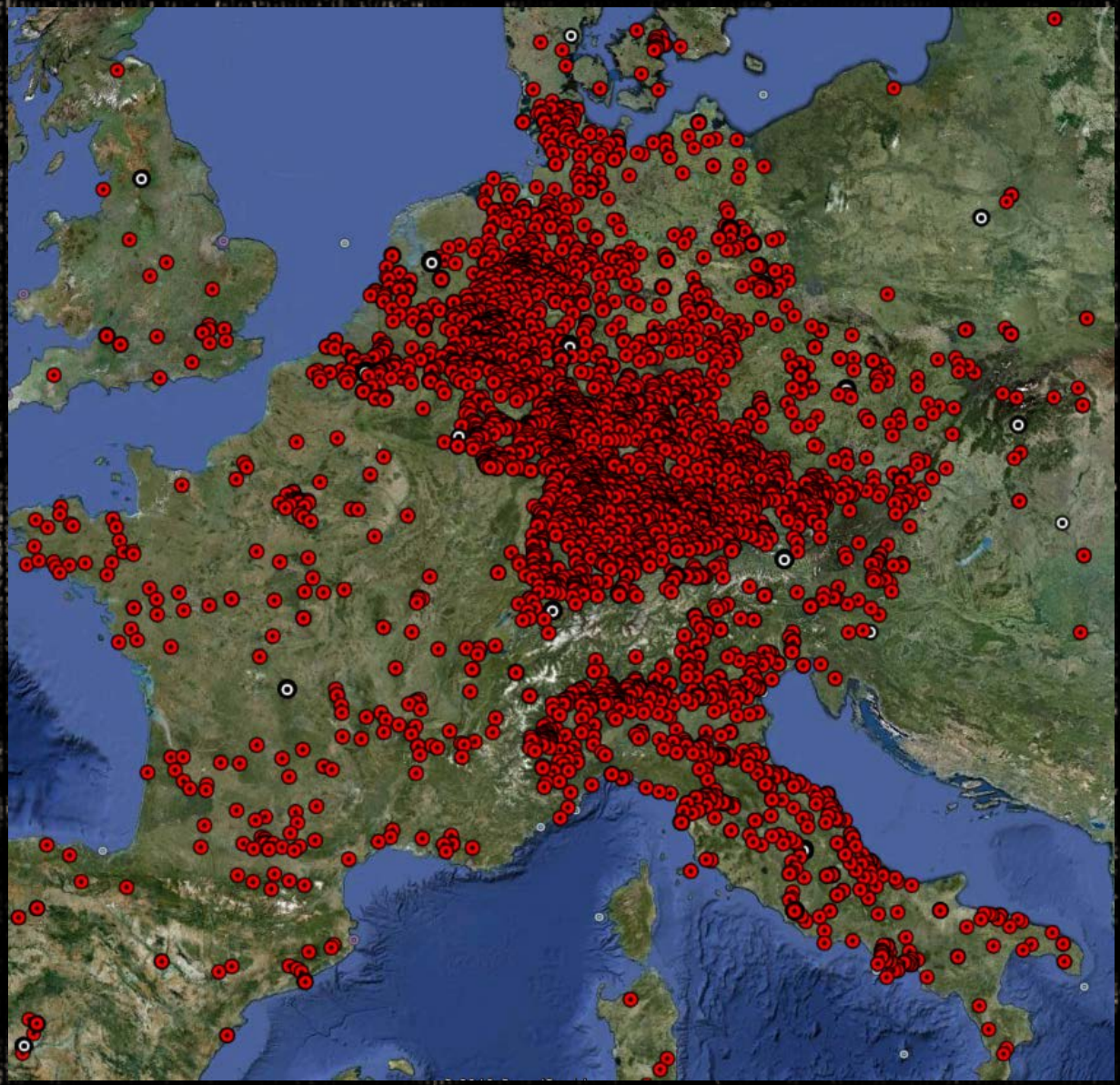
The HART Communications Protocol (Highway Addressable Remote Transducer Protocol) is an early implementation of Fieldbus, a digital industrial automation protocol. Its most notable advantage is that it can communicate over legacy wiring.

PHOENIX CONTACT

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