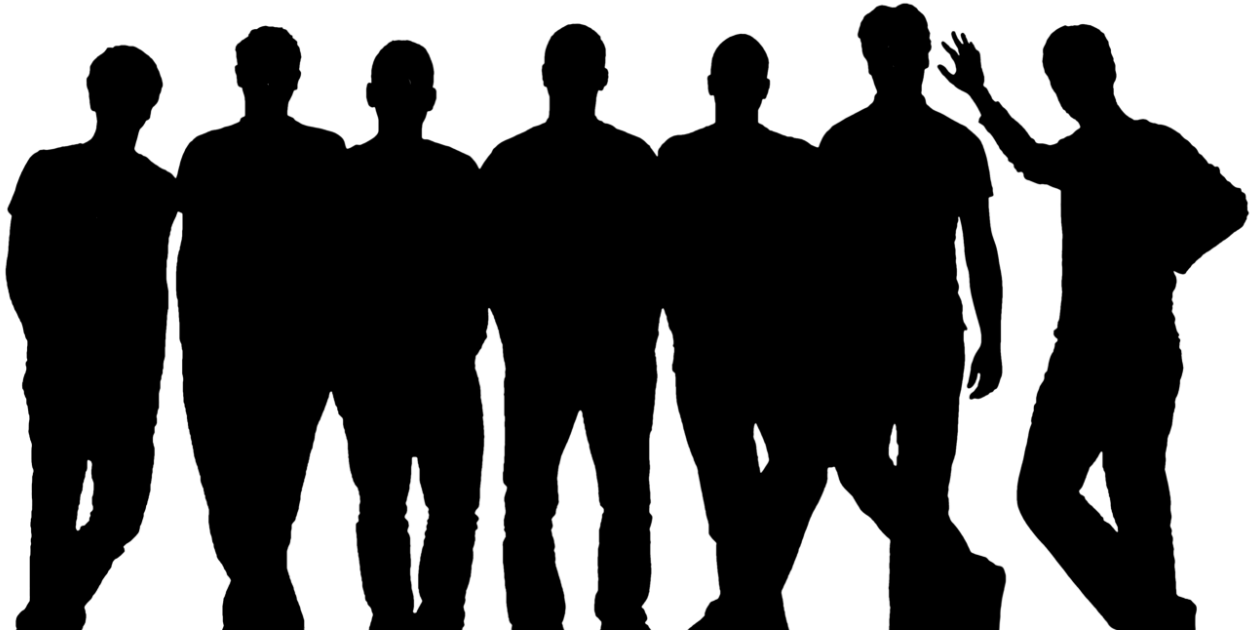
Verwundbarkeit Vernetzter Industriesteuerungen
- Lagebild, Angriffe, Schutzmaßnahmen -

Jan-Ole Malchow, Johannes Klick, Prof. Volker Roth

AG Sichere Identität
Fachbereich Mathematik und Informatik
Freie Universität Berlin

SCADACS



Volker Roth
Daniel Marzin
Stephan Lau

Jan-Ole Malchow
Sascha Zinke
Stephan Arndt

Johannes Klick
Mateusz Khalil
Robert Kovacs

http://www.scadacs.org

SCADACS

Problemstellung

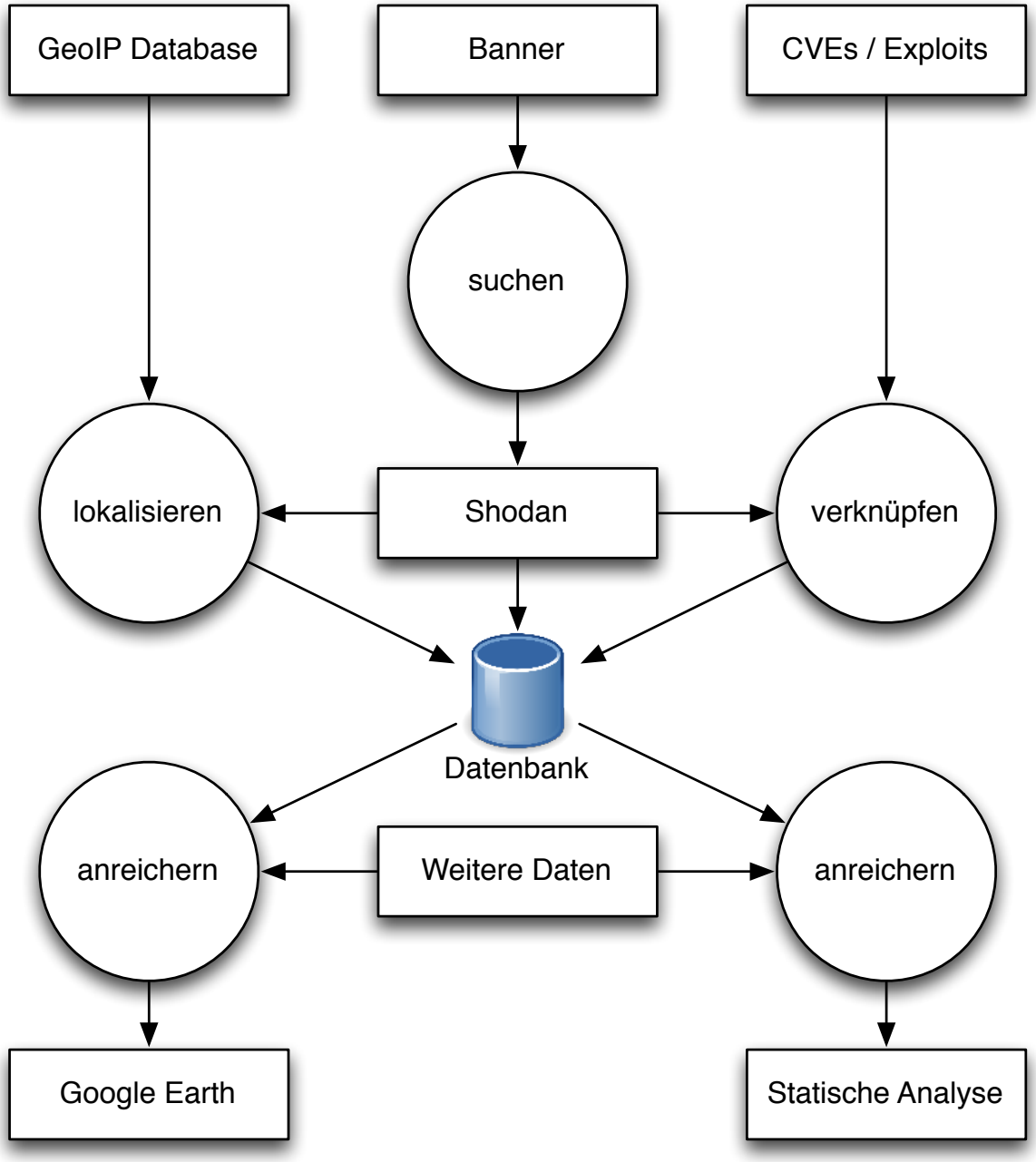
Steuerungen sind schlecht Geschützt gegen Angreifer

- fehlende Authentifizierung
- keine Verschlüsselung
- direkt mit dem Internet verbunden

Fragestellung

- Wie sind die Steuerungen geografisch verteilt?
- Um welche Arten von Steuerungen handelt es sich?
- Handelt es sich um ein flächendeckendes Problem?
- Gibt es bestehende CVEs / Exploits zu den Geräten?

Methodik - Prozessübersicht



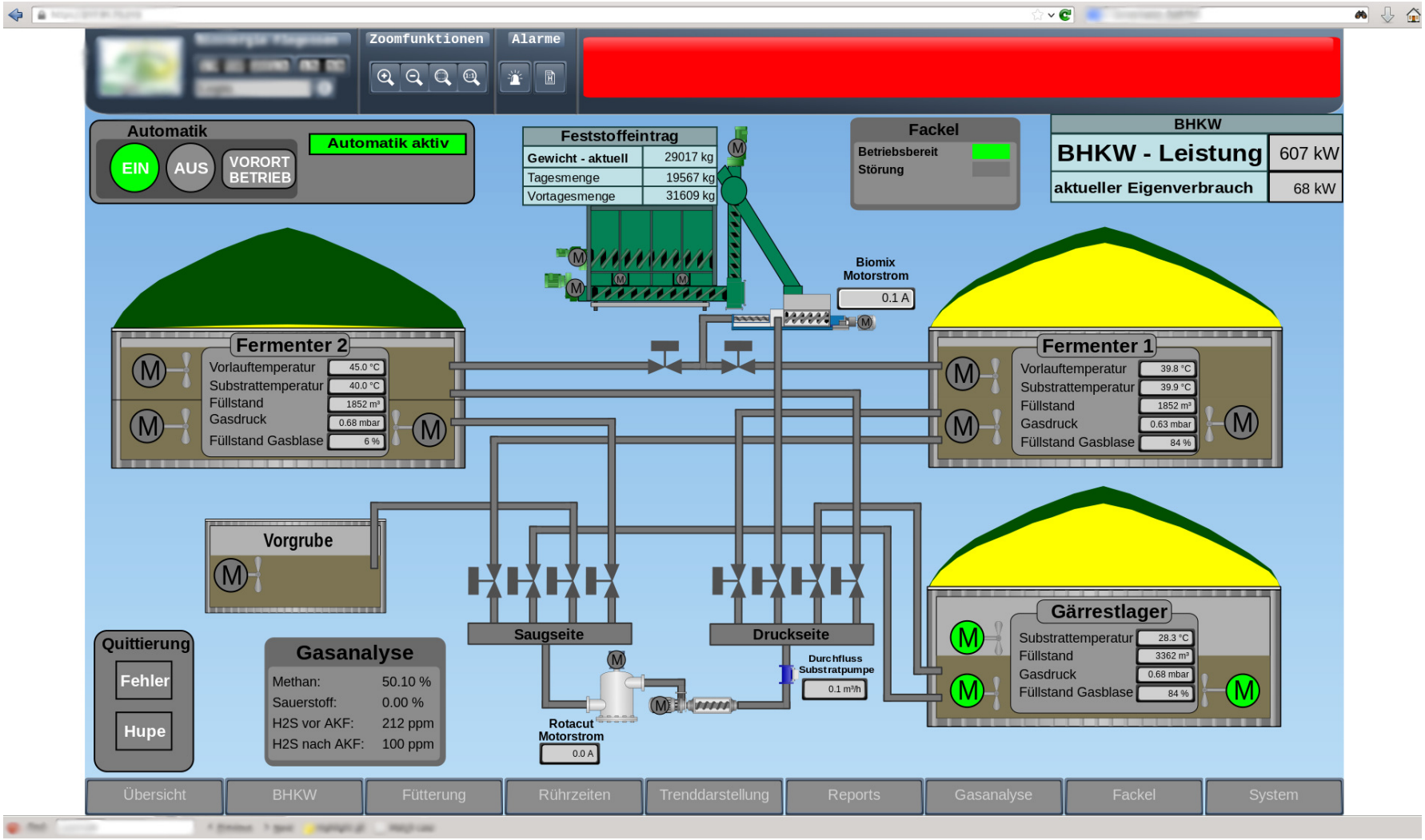
Methodik - SHODAN Funktionsweise

SHODAN ist eine spezielle Suchmaschiene

- sucht im Internet nach Diensten wie SNMP, HTTP(S), Telnet etc.
- verbindet sich mit diesen Diensten und speichert bzw. fragt Identifikationsinformationen ab
- Suche anhand sogenannter “Banner”
- findet Geräte im Internet, die WEB-Suchmachien wie Google nicht finden

Klassifizierung von Anlagen

SCADA Systeme



SCADACS

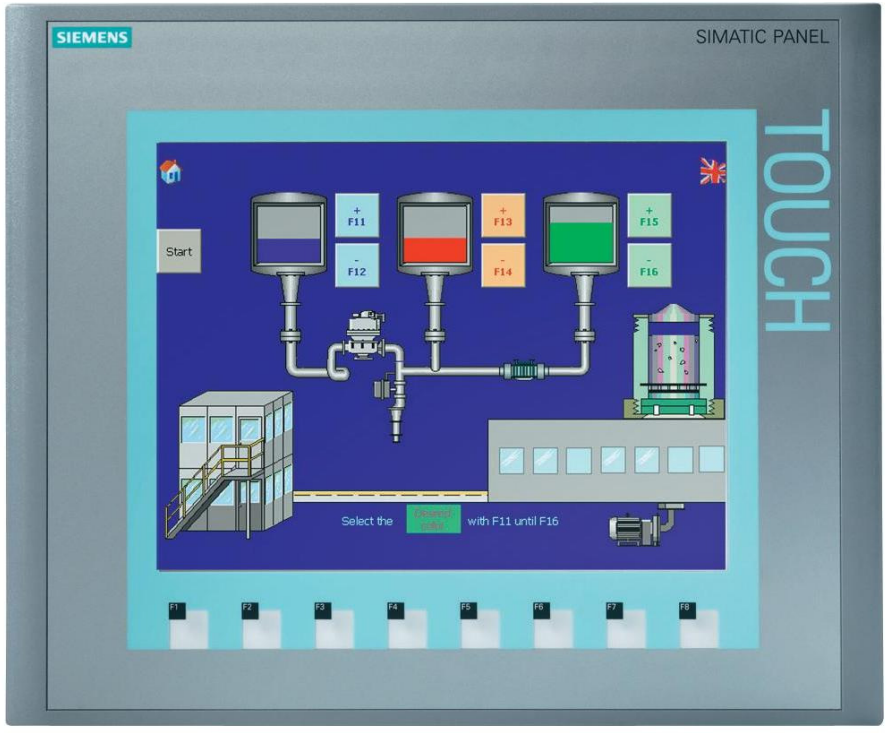
PLC - Programmable Logic Controller

SCADACS

PLC Network Devices (PLCND)

SCADACS

HMI - Human Machine Interfaces



SCADACS

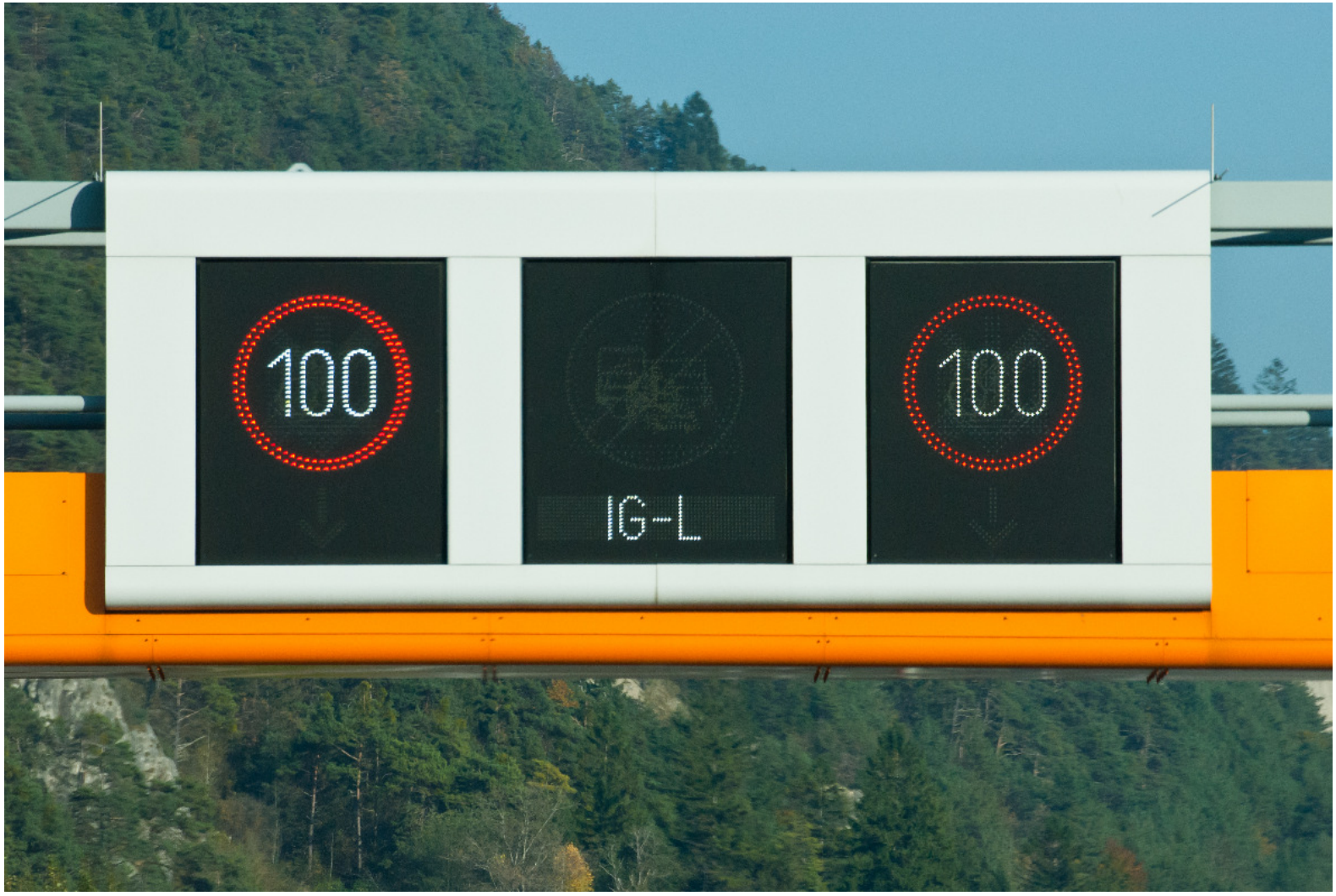
BMS - Building Management Systems

SCADACS

PDU - Power Distribution Units

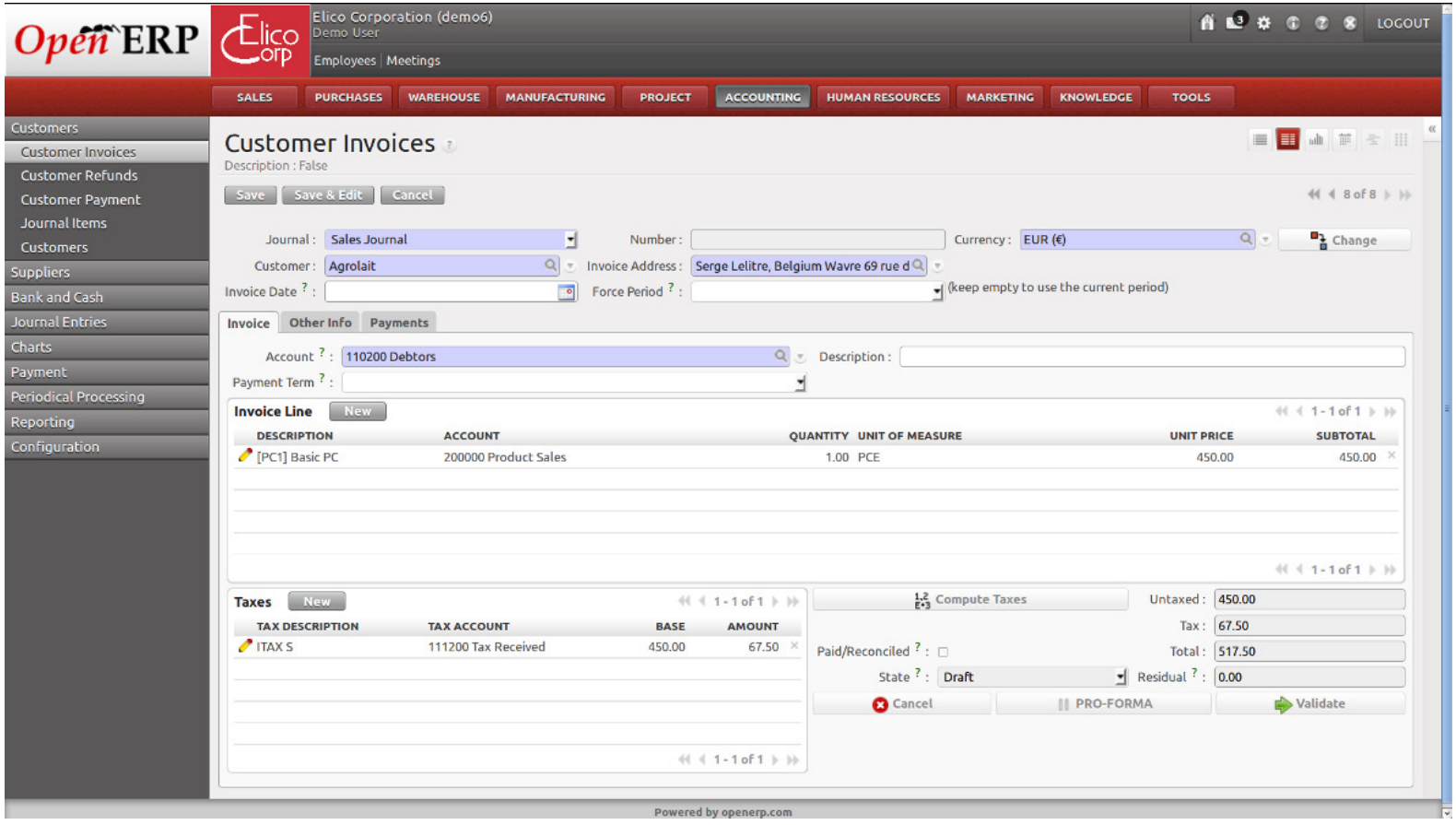
SCADACS

TM - Traffic Management Devices



SCADACS

ERP - Enterprise Rescource Planning Systems



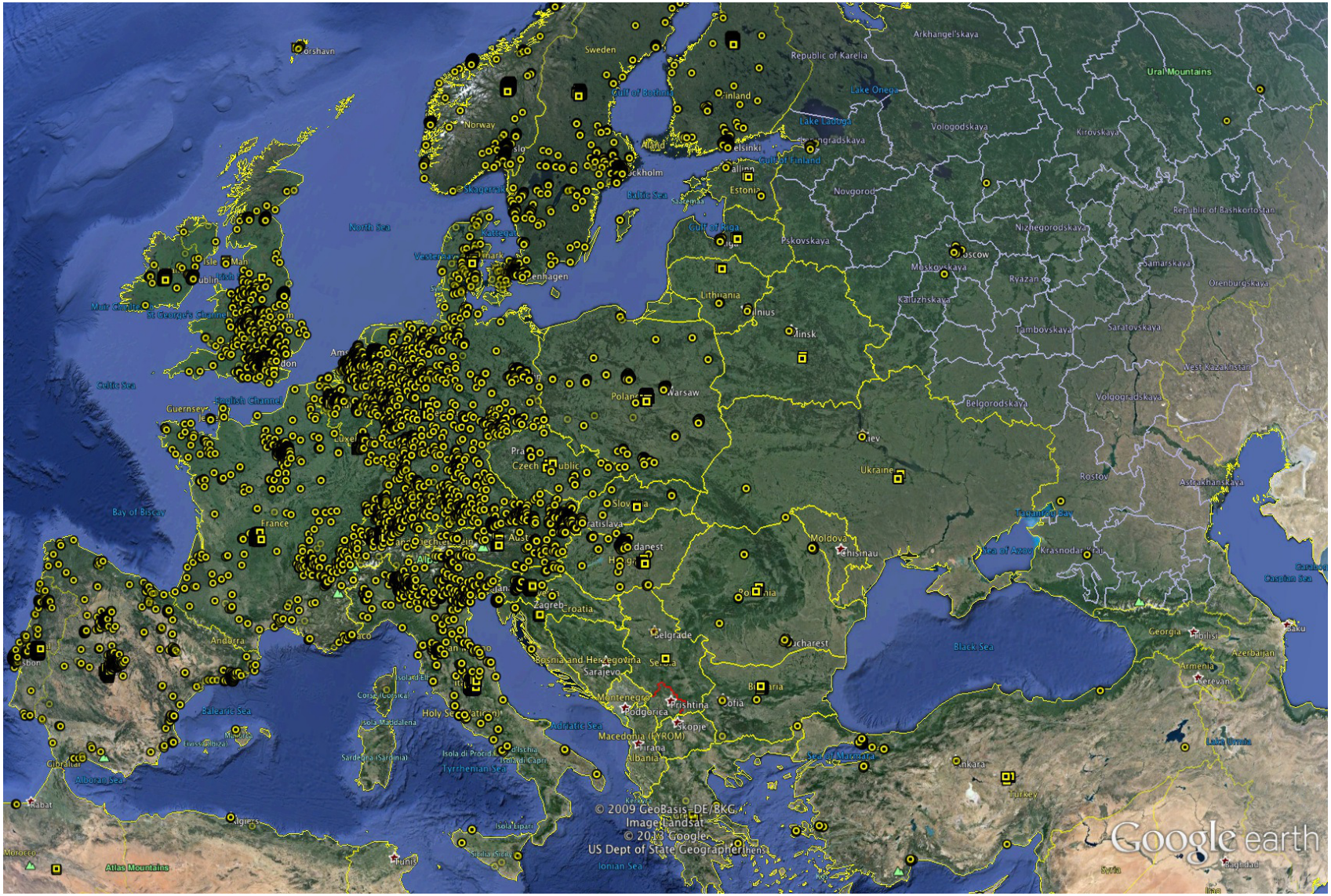
SCADACS

UPS - Uninterruptible Power Supplys

SCADACS

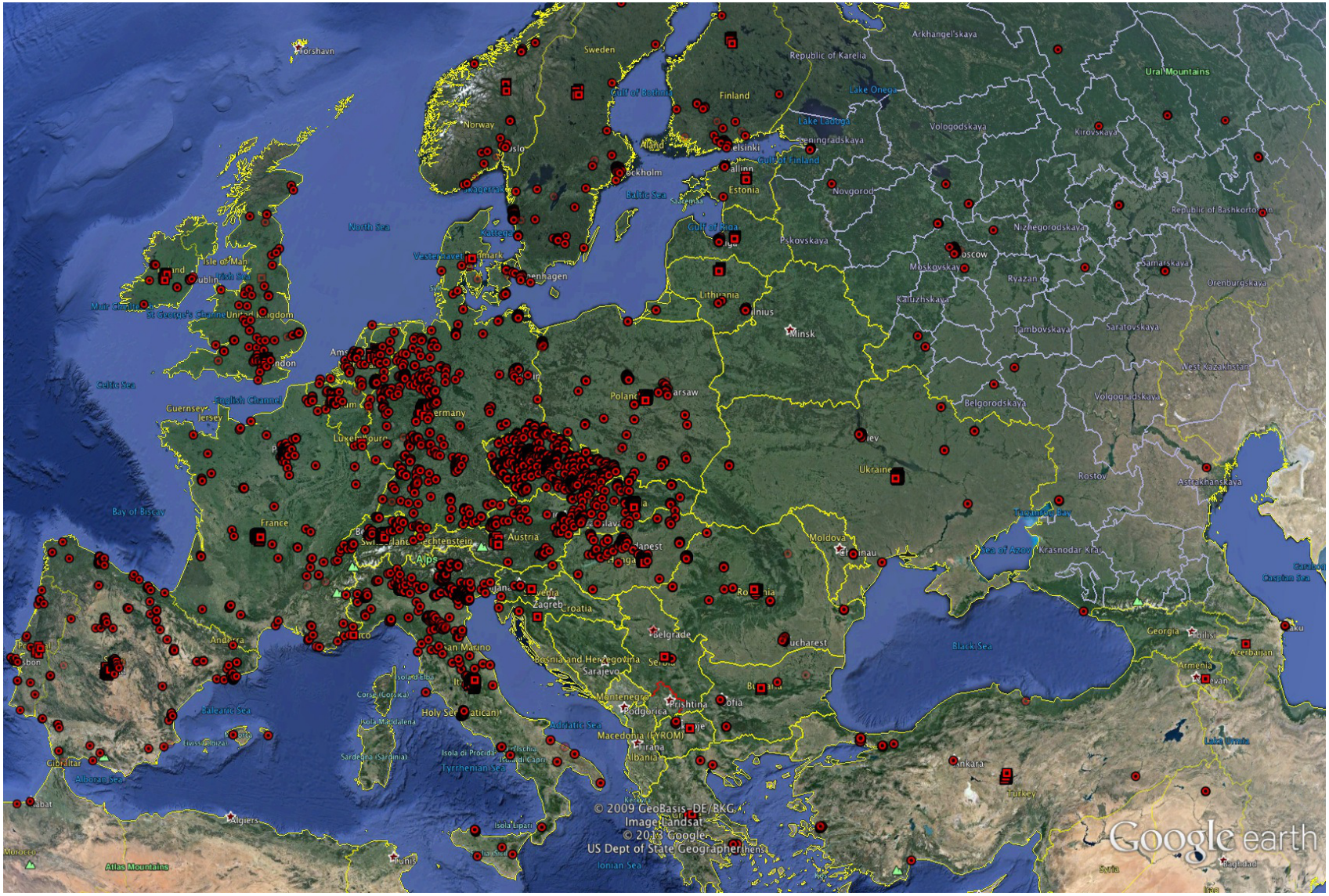
Ergebnisse

IRAM - Deutschland - BMS



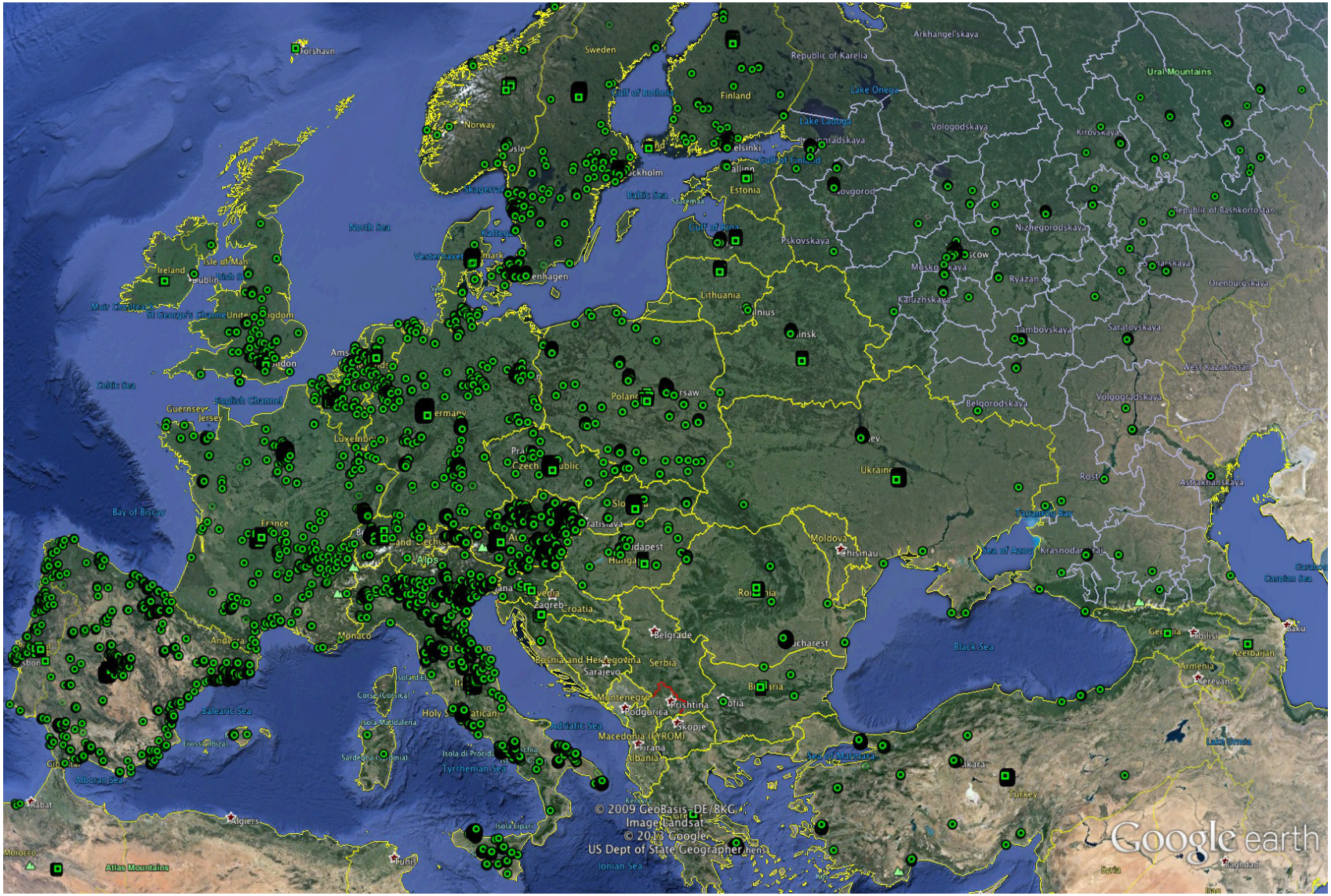
SCADACS

IRAM - Deutschland - PLC



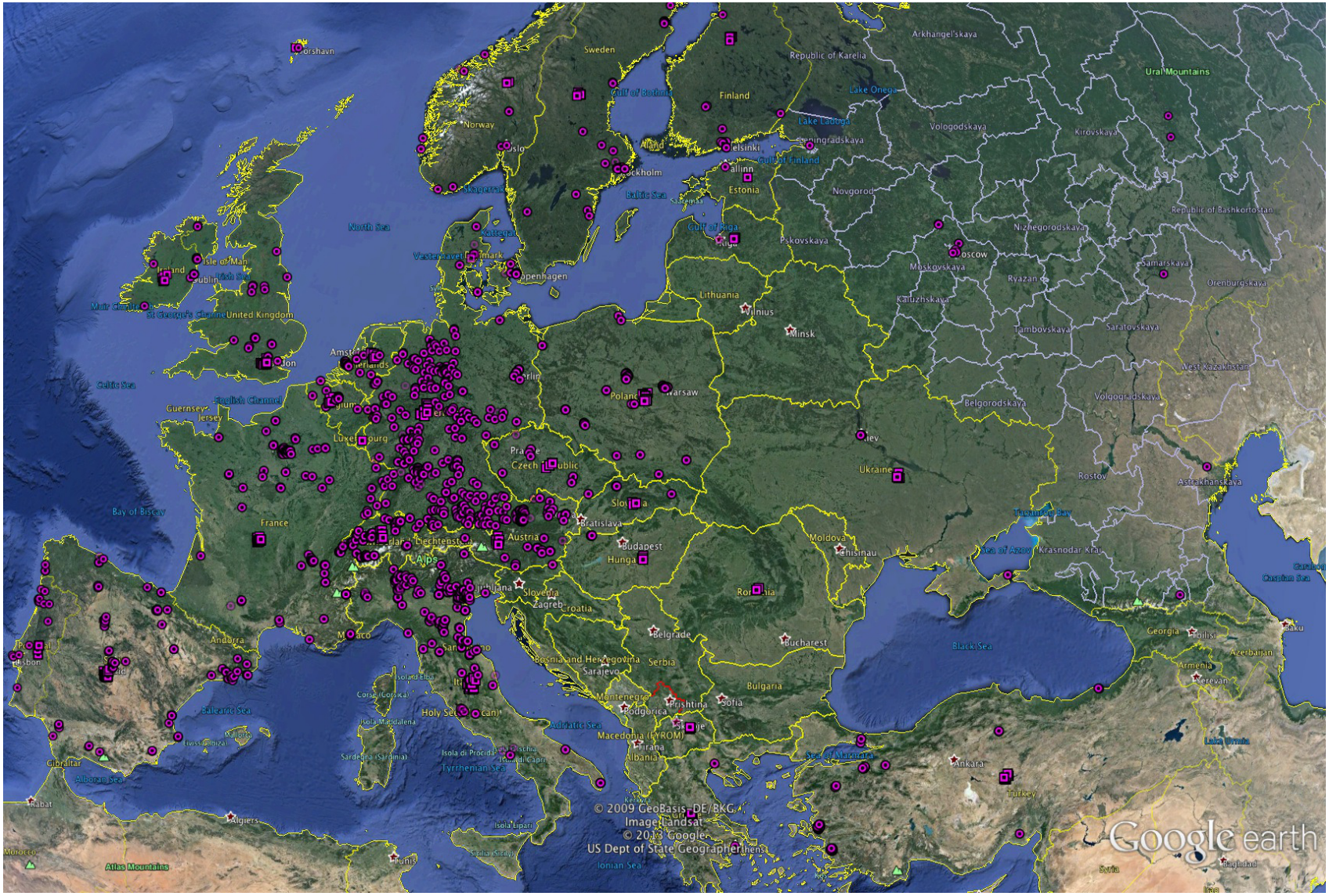
SCADACS

IRAM - Deutschland - PLCND



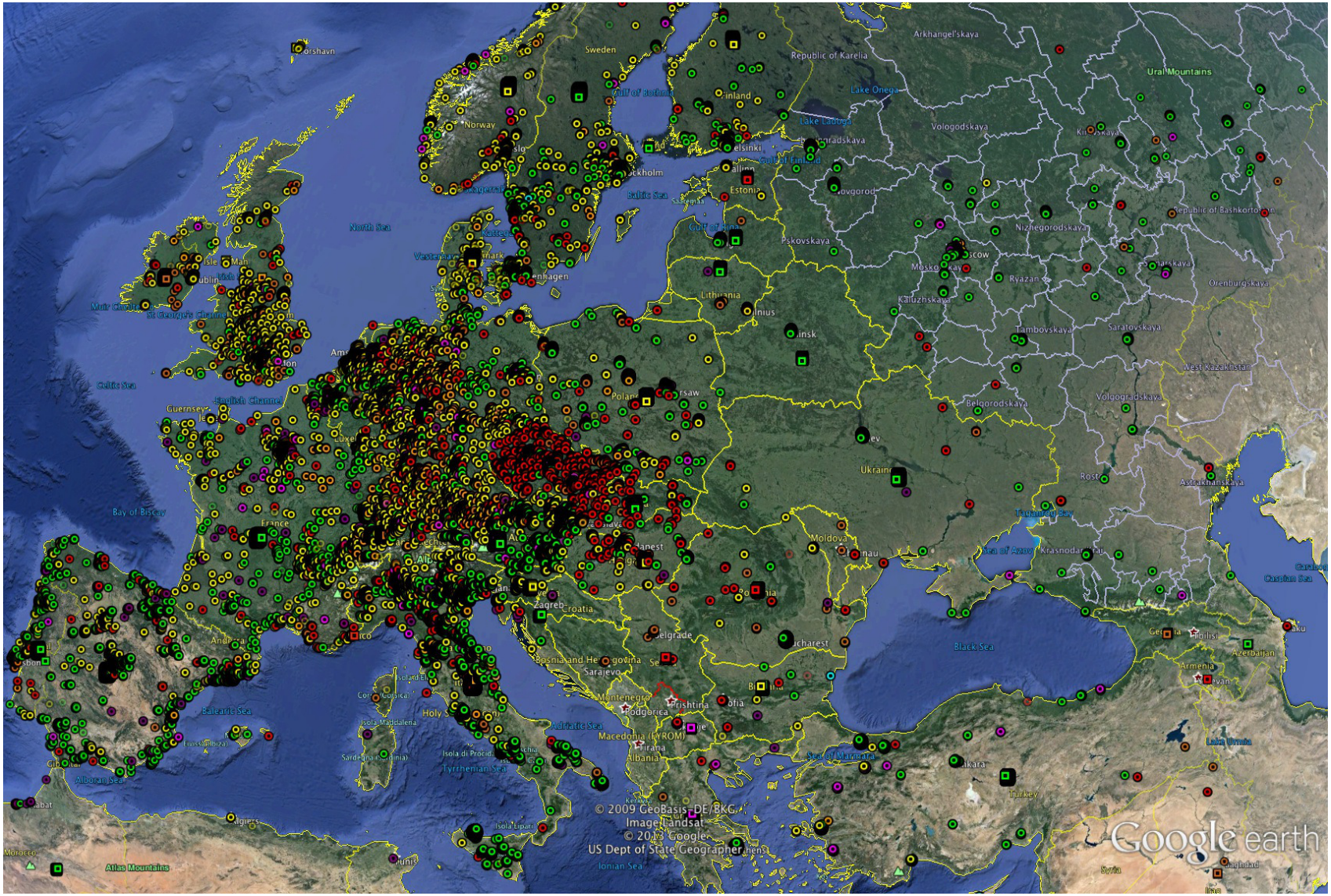
SCADACS

IRAM - Deutschland - SCADA



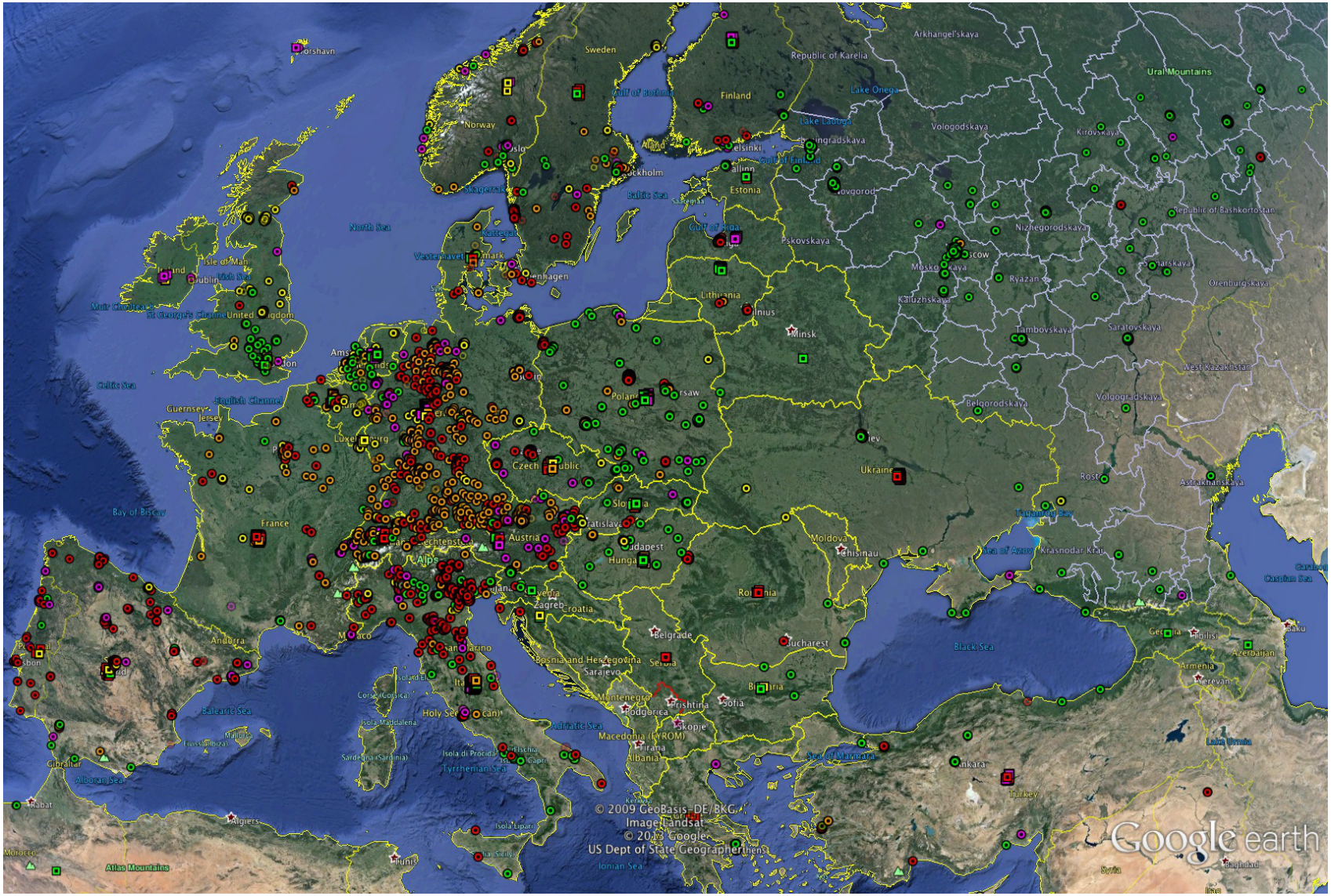
SCADACS

IRAM - Europa



SCADACS

IRAM - Europa (verwundbar)



SCADACS

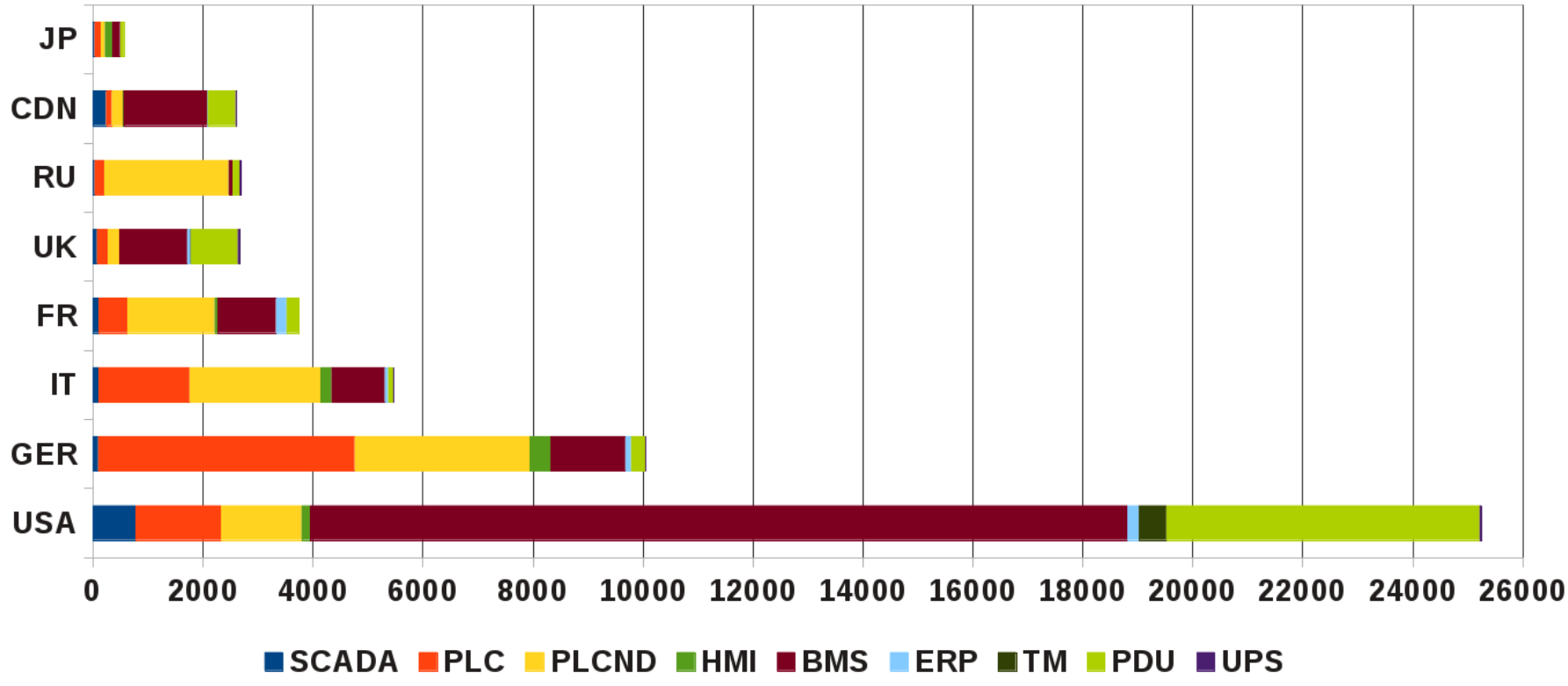
Auswertung

Kennzahlen

Tabelle : Anzahl der Geräte pro Kategorie, sowie den Anteil der Geräte mit bekannten Verwundbarkeiten und verfügbaren Exploits

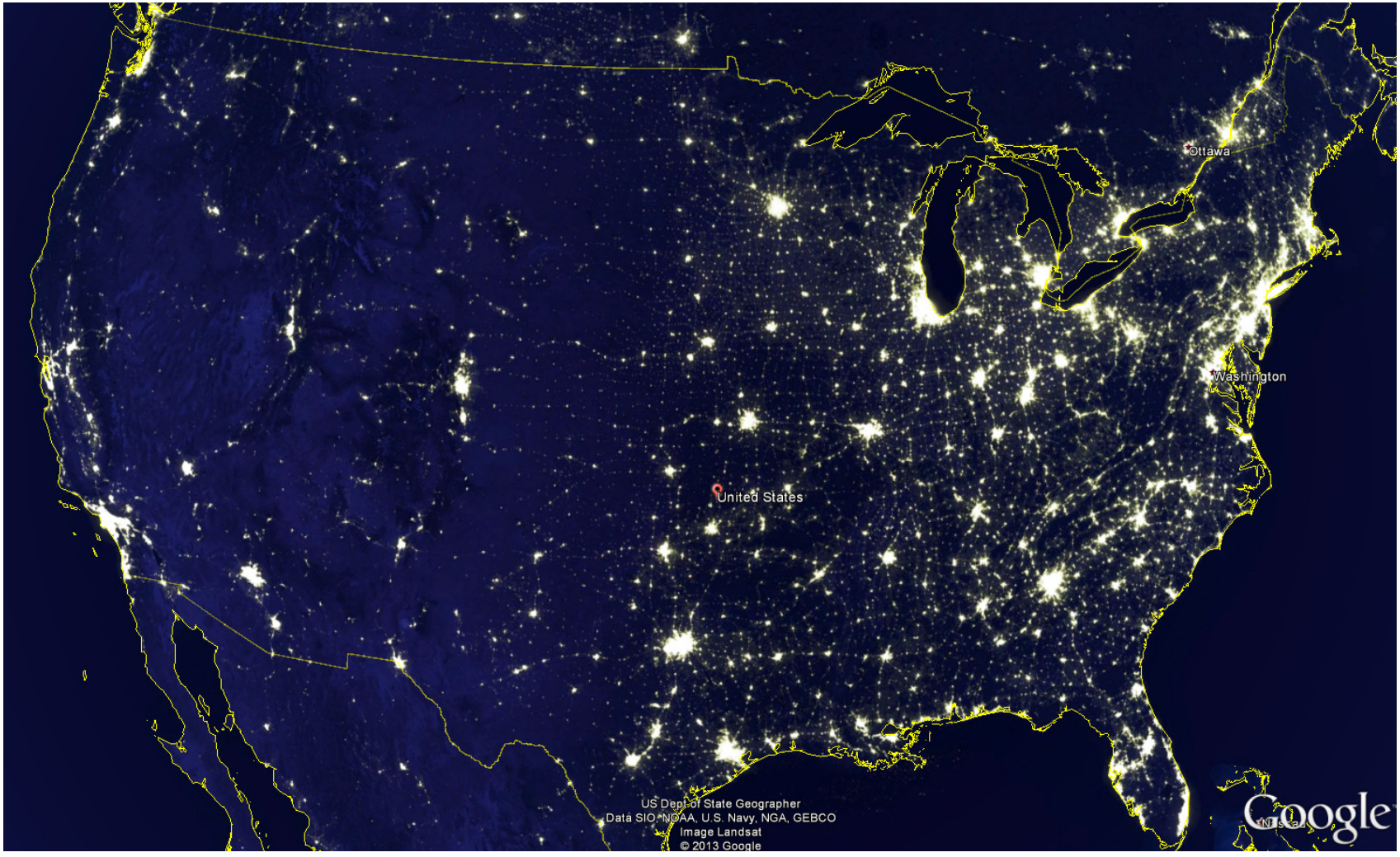
Kategorien	**Geräte**	**CVEs/Exploits**
BMS	31.411	9%
PLCND	23.873	14%
PDU	10.381	0%
PLC	7.254	26%
SCADA	2.254	28%
HMI	1.741	41%
ERP	1.400	0%
TM	788	0%
UPS	167	0%

Kennzahlen



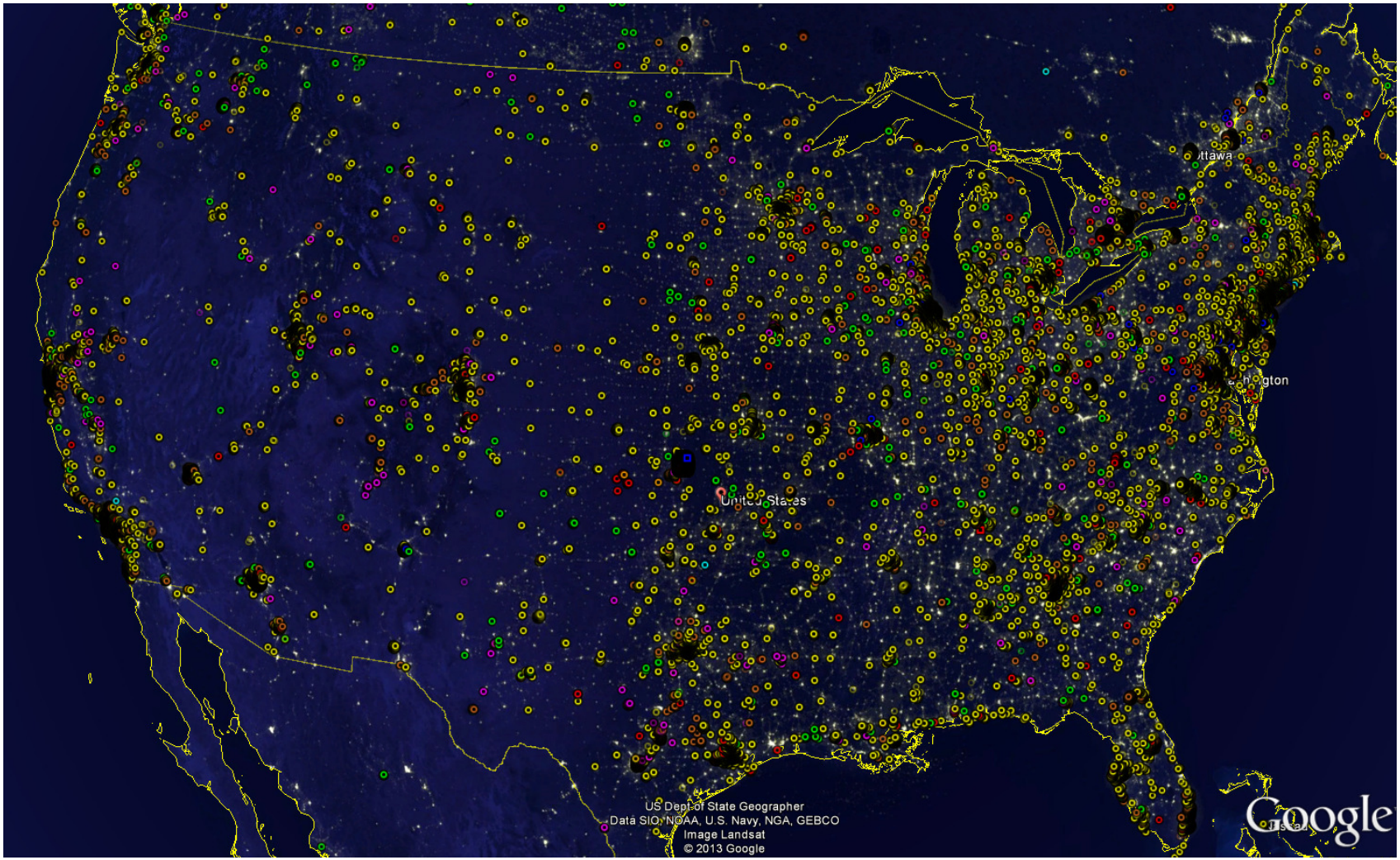
SCADACS

IRAM - USA Nachtaufnahme ohne Steuerungen



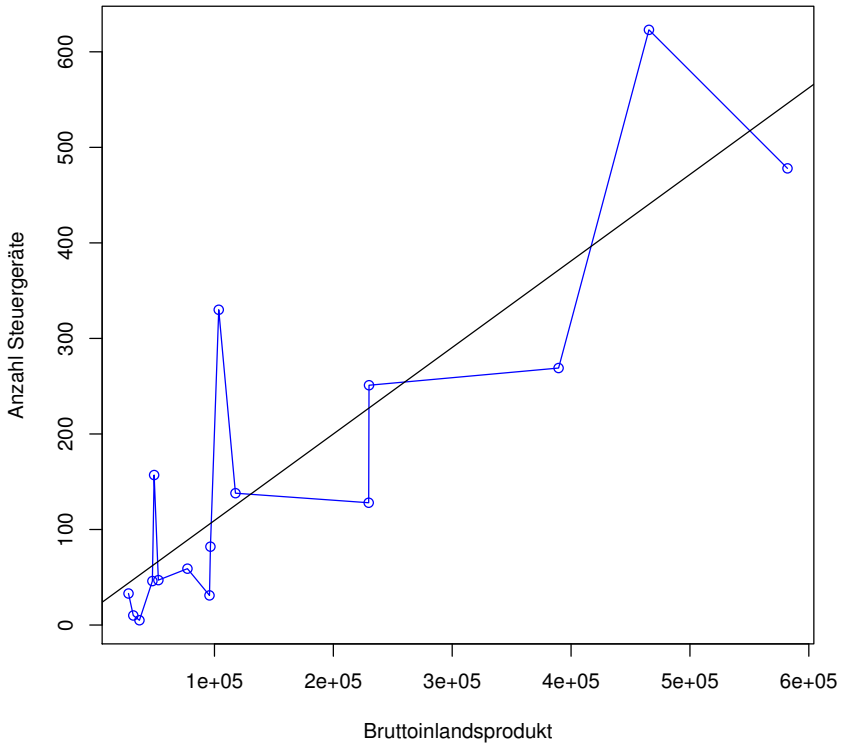
SCADACS

IRAM - USA Nachtaufnahme mit Steuerungen

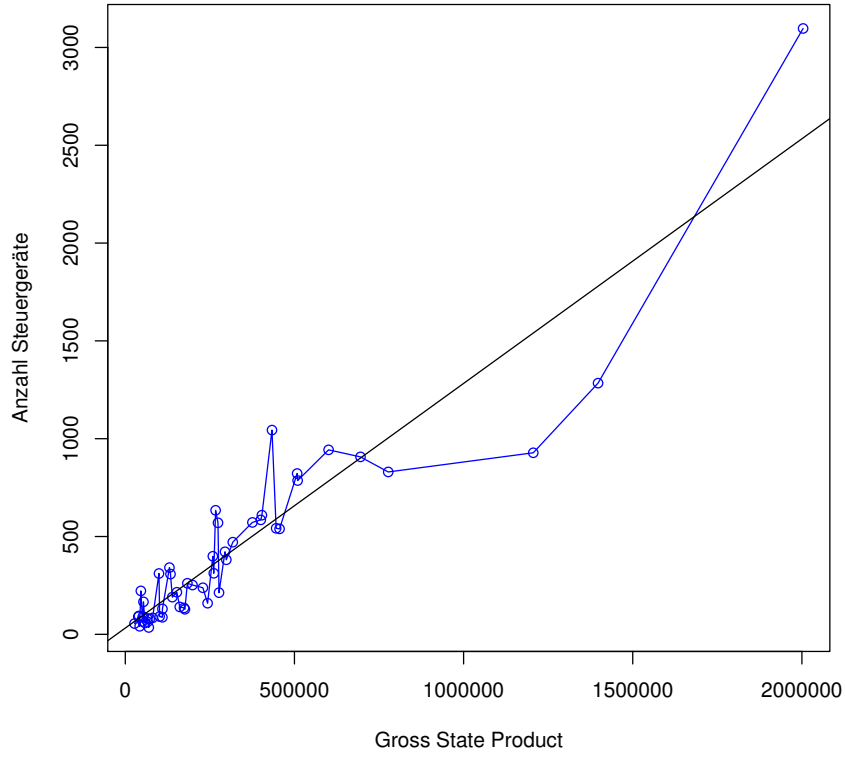


SCADACS

Korrelation zur Wirtschaftsleistung



(a) Deutschland (Jahr 2012)



(b) USA (Jahr 2012)

SCADACS

Frage

Sind industrielle Kontrollsysteme im Fokus von Angreifern?

Antwort

Kaspersky hat eine Angriffskampagne untersucht und die Ergebnisse zur Verfügung gestellt.

Die Folgenden Abbildungen und Informationen basieren auf dem Bericht Energetic Bear - Crouching Yeti des Kaspersky Lab Global Research and Analysis Teams.

Wer oder was ist Dragonfly?

Dragonfly ist eine Hackergruppe mit wahrscheinlich osteuropäischen Ursprung. Sie scheint sich in letzter Zeit auf das produzierende Industriegewerbe zu konzentrieren.

Verwendete Angriffsvektoren

Dragonfly nutze hauptsächlich folgende Anrgiffsmethoden:

- Spear-Phishing E-Mails mit preparierten PDF-Dokumenten die eine Sicherheitslücke in Adobe Flash ausnutzten (CVE-2011- 0611)
- Preparierte Installer mit Trojanern
- Waterhole Attacks unter der Verwendung von vielen verschiedenen bekannten Schwachstellen

SCADACS

Angriffmethode 1: Preparierte Softwareinstaller

Es wurden gezielt die Webserver von Firmen kompromitiert, welche PLC bezogendes Equipment verkaufen. Folgende Firmen waren betroffen:

- eWON (industrielle VPN Router, Protokollwandler, etc.)
- MB-Connect (industrielle VPN und Backup-Lösungen)

Die Installer beinhalteten eine bösartige DLL (HAVEX Trojaner).

eWON

Press/News - Events - Partner area - Careers - Contact | Global website

eWON MACHINES CAN TALK

Products | Solutions | Applications | PLC connectivity | Support | Distributors | About us

Search

Industrial VPN router for PLC remote access and troubleshooting

Save time and money by installing an eWON Cosy on your remote machines.

Explore eWON

Home / Support / Software download

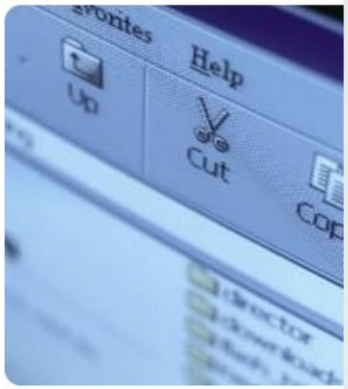
- Support
- Firmware releases
- Software download
- viewON 2 registration

Print

Software download

Download the newest version here

Description	File	Revision
eBuddy Free eWON add-on tool to easily • set up eWON IP address • upload eWON firmware upgrades • backup/restore data and configurations Requirements: • Windows 2000, XP, Vista or 7 - 64 bits	ebuddysetup.exe	release note
eCatcher Easy, secure, Internet remote access with Talk2M. For Free+ and Pro services	ecatchersetup.exe	release note



Contact us

Where to buy
Find a distributor

Support
Wiki

Related Links

ACS

MB-Connect

Tuesday, 12 August 2014

Press Releases | Imprint | GTC | Sitemap | Datenschutz

Ideas and solutions for remote maintenance.

mbNET mbCONNECT24 mymbCONNECT24

MB CONNECT LINE
remote maintenance solutions

HOMEPAGE APPLICATIONS SOLUTIONS PRODUCTS SUPPORT NEWS CONTACT search...

Homepage | **Products**

PRODUCTS

- mbNET
- mbSPIDER
- mbSECBOX
- mbNET.mini
- mbCONNECT24
- mymbCONNECT24
- mymbCONNECT24.hosted
- mbPOINT

With the products of MB CONNECT LINE GmbH we offer for systems of more than 90 of the most reputable manufacturers automation solutions for remote support. These range from serial via MPI bus connections to professional.

The mbNET industrial routers are an important part of our program and allow eg UMTS or WLAN location-independent use as a nahzu at remote facilities to produce energy through renewable resources.

The house mbCONNECT24 very own Internet portal provides a central web portal for remote maintenance via Internet and is administrated by the in-house server-purpose portal mymbCONNECT24 complete itself.

Our latest product - the mbSPIDER - is a programmable data modem with alarm function and web visualization. It is used to record consumption data and the monitoring of plants and objects. To the mbSPIDER allows meter readings, measurement values, record analog values and logic states continuously.

With our products we offer innovative ideas and solutions for secure remote administration.

mbNET.
Remote units for industrial maintenance via the internet

mbSPIDER
The individual programmable data modem.

mbSECBOX
PLC-backup and virus detection for S7-300/400 PLC with mbSECBOX*

mbNET.mini
The compact solution for data connection - Small but powerful

ACS

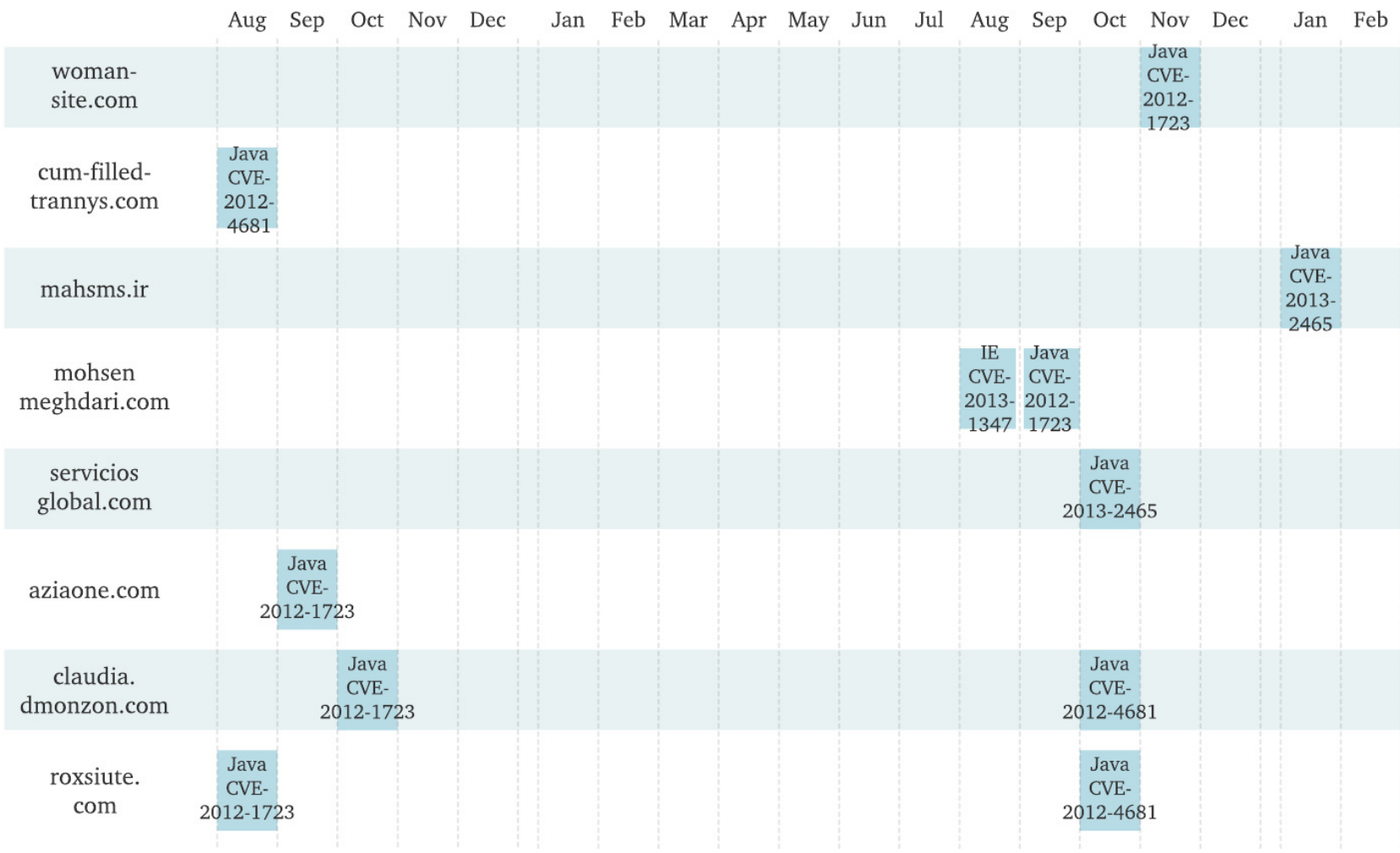
Bösartige JAR/HTML Dateien - Waterholing

Die Angreifer infizierten Websites, sodass die Nutzer zu Websites umgeleitet worden sind, die bösartige JAR bzw. HTML-Files beinhalteten.

Folgende Schwachstellen wurden u.a. ausgenutzt:

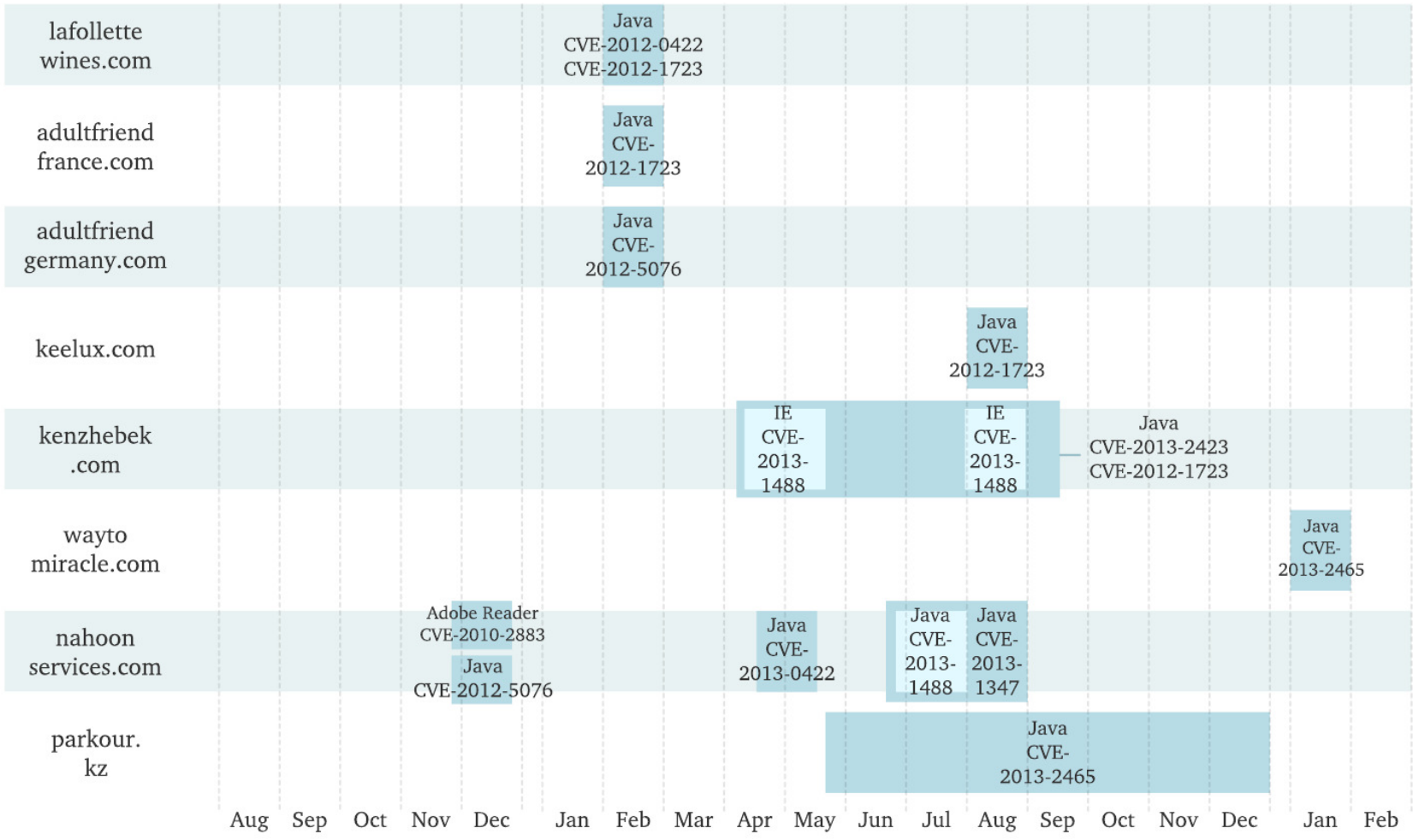
- CVE-2013-1347 IE 8
- CVE-2013-2465 Java 6 / 7
- CVE-2012-1723 Java 6 / 7

Infizierte Websites



SCADACS

Infizierte Websites



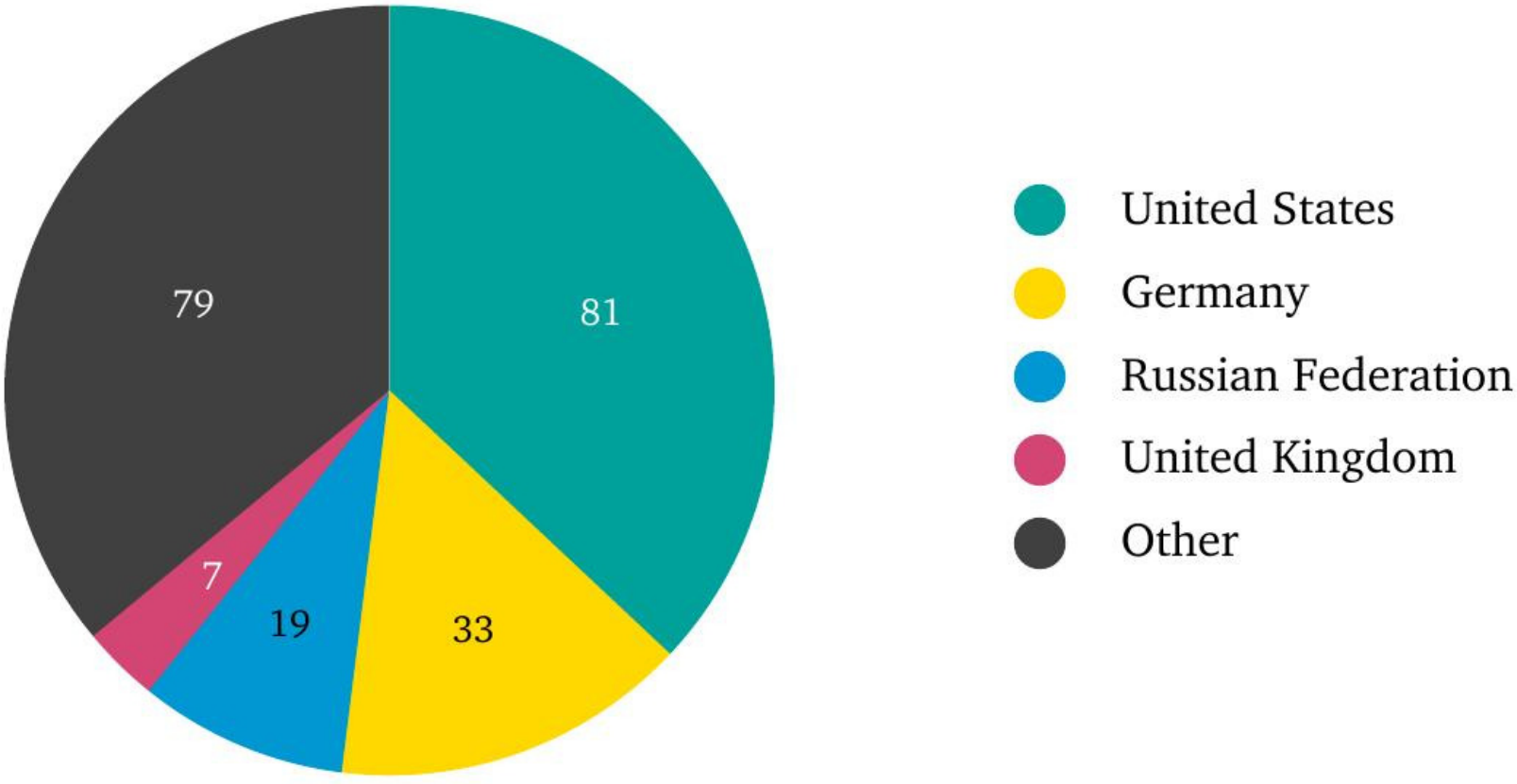
SCADACS

Havex Trojaner

Eigenschaten

- C&C-Kommandostruktur (via HTTP Commands)
- Dynamische aus dem Internet ladbare Module
- Die Module sind bei der Übertragung verschlüsselt

C&C Server Verteilung



SCADACS

Besondere Module

- System-Info-Module
  - OS Version
  - Username
  - Current IP
  - List of drives
  - Default Browser
  - Running Processes
  - Proxy Settings
  - User Agent
  - Email Name
  - BIOS version and date

SCADACS

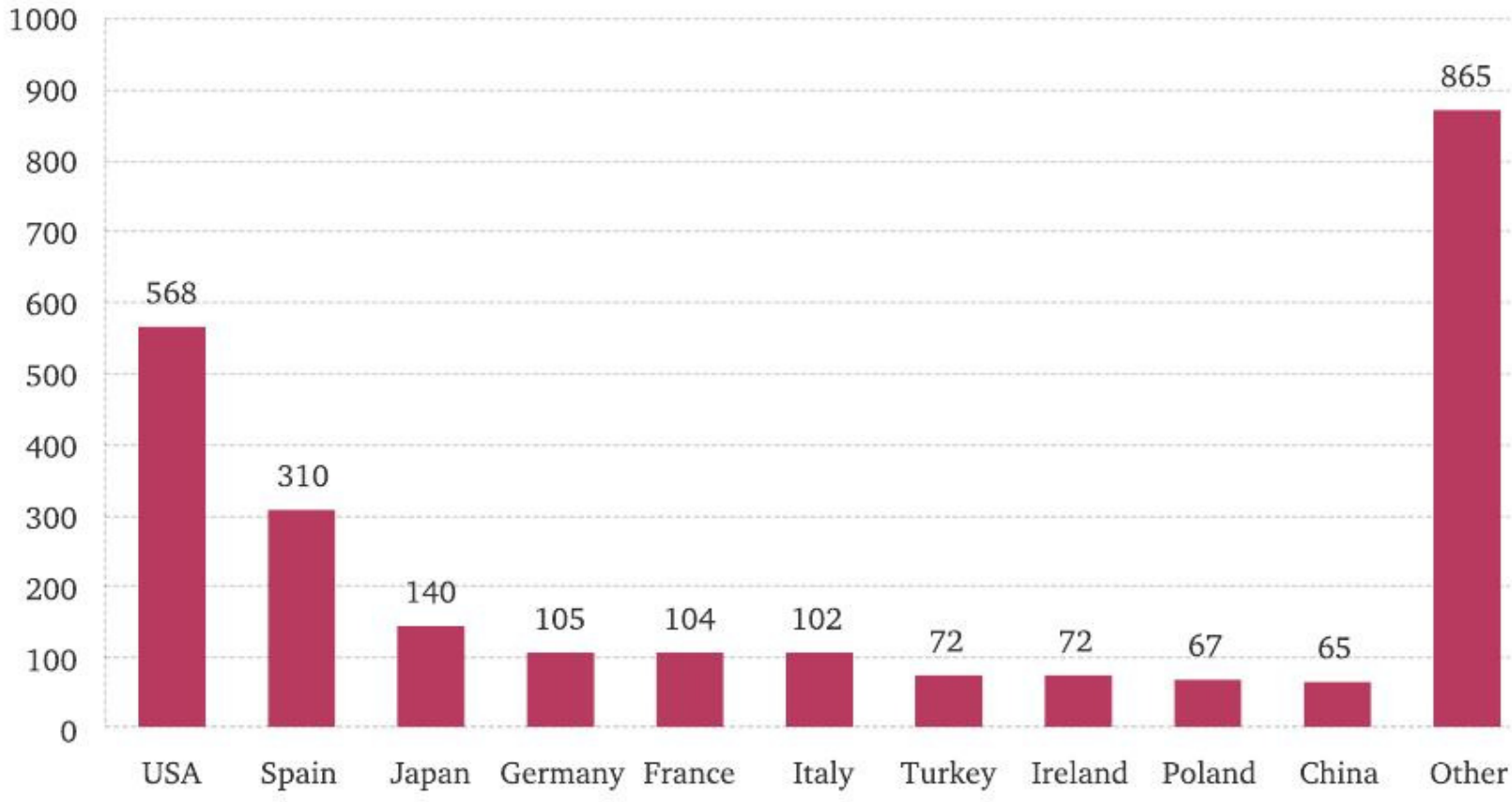
Besondere Module

- Kontaktdaten-Dieb
- Browser-Password-Decrypter
- OPC Scanner
- Netzwerk-Scanner
  - Port: 502 (Modbus)
  - Port: 102 (Siemens S7Comm)
  - Port: 11234 (Measuresoft ScadaPro)
  - Port: 12401 (7-Technologies IGSS SCADA)
  - Port: 44818 (Rslinx)

Betroffene Industrien

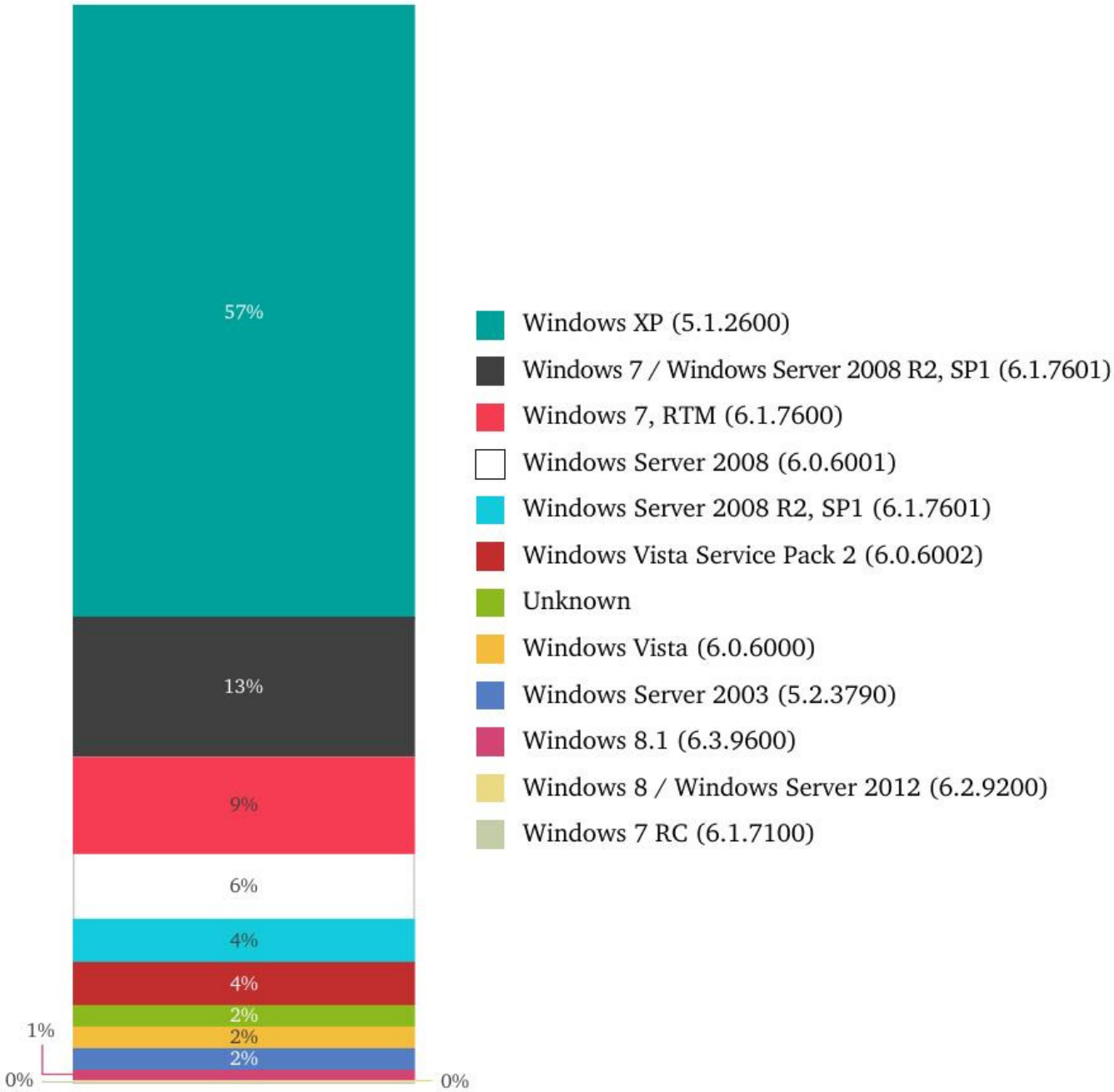
Sector	Number of victim organizations
Educational	32
Research	14
Mechanical Engineering	10
Information Technology	10
Construction	9
Government	8
Health	5
Network Infrastructure	3
Pharmaceutical	2
Electrical Engineering	2
Packaging	2
Financial	2
Energy	2
Cleaning	1

Fälle sortiert nach Ländern



SCADACS

Fälle sortiert nach OS



Zusammenfassung

- Eine große Menge von Steuerungseinheiten befinden sich direkt im Internet
- Viele Steuerungen sind gefährdet und ungeschützt
- Besonders in wirtschaftlich starken Regionen sind viele Geräte zu finden
- Es handelt sich um ein internationales und fächendeckendes Problem
- Angreifer suchen mit Schadsoftware gezielt nach Kontrollsystemen
- Es besteht Handlungsbedarf

SCADACS

Vielen Dank für Ihre Aufmerksamkeit

Anmerkung:

Die FU Berlin sucht Partner aus dem produzierenden Gewerbe für gemeinsame Forschungsprojekte im Bereich SCADA / ICS Sicherheit. Bei Interesse können Sie uns gerne ansprechen oder eine e-Mail schreiben.

Kontakt:

johannes.klick@fu-berlin.de jan-ole.malchow@fu-berlin.de volker.roth@fu-berlin.de

SCADACS

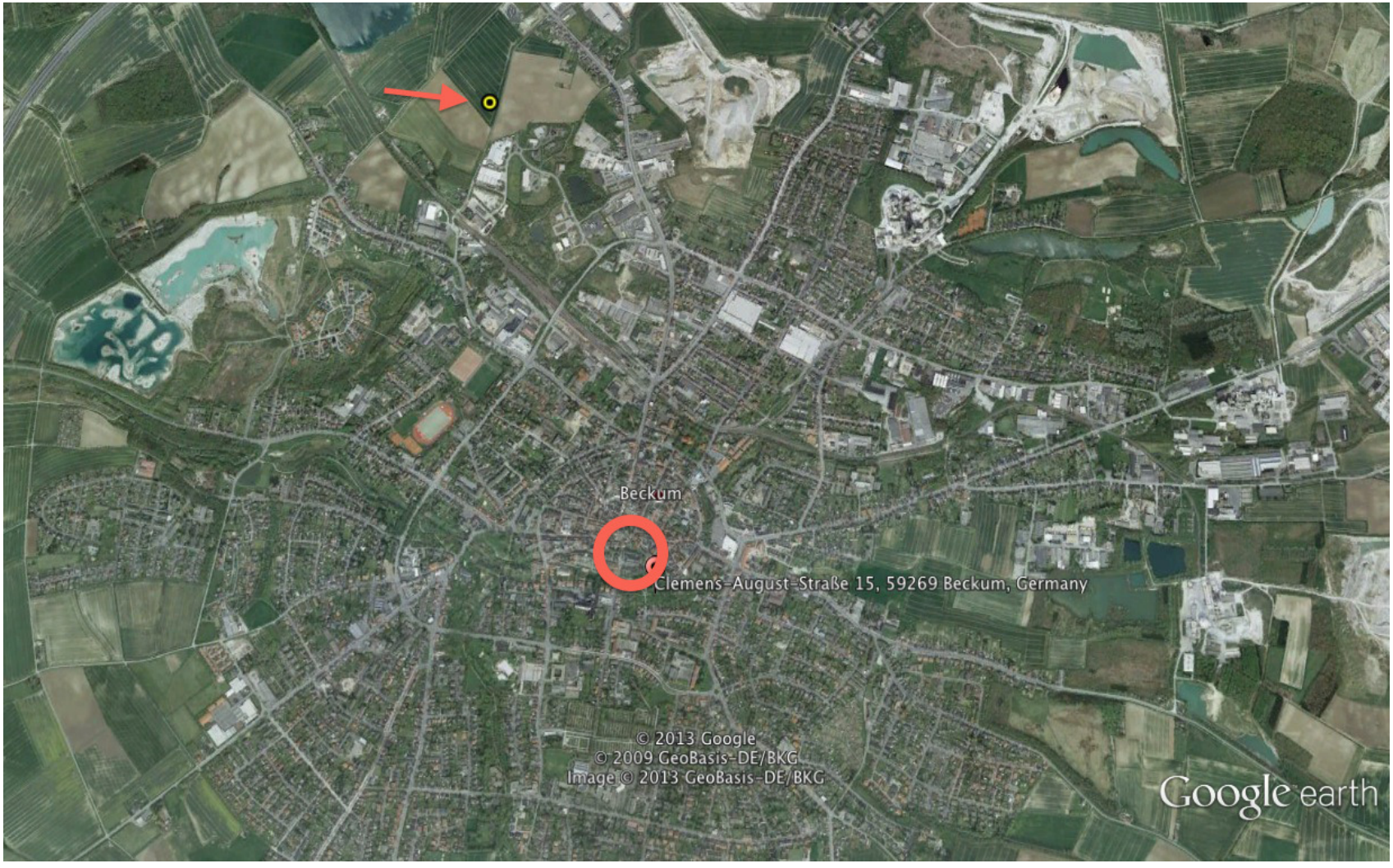
IRAM - Demonstration (Video)

Video

IRAM - Asien

SCADACS

IRAM - Asien



SCADACS