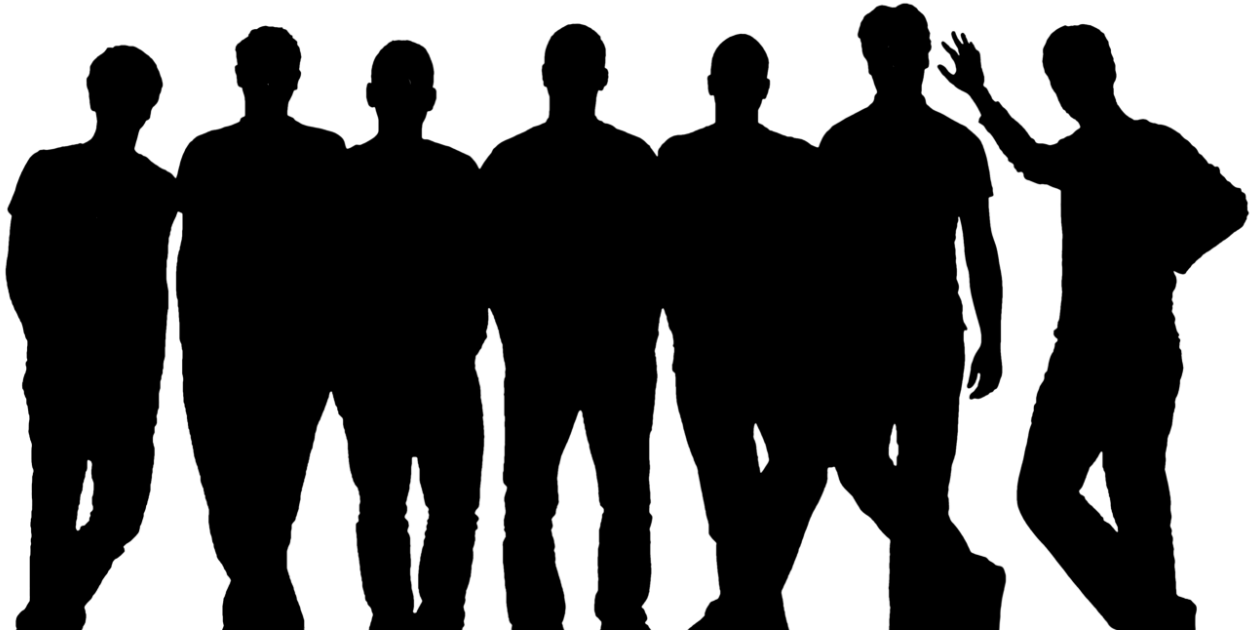
Erreichbarkeit von digitalen Steuergeräten
Ein Lagebild

Jan-Ole Malchow, Johannes Klick

AG Sichere Identität
Fachbereich Mathematik und Informatik
Freie Universität Berlin

SCADACS



Volker Roth
Daniel Marzin
Robert Fehrmann

Jan-Ole Malchow
Sascha Zinke
Philipp Lämmel

Johannes Klick
Mateusz Khalil
Robert Kovacs

http://www.scadacs.org

SCADACS

Problemstellung

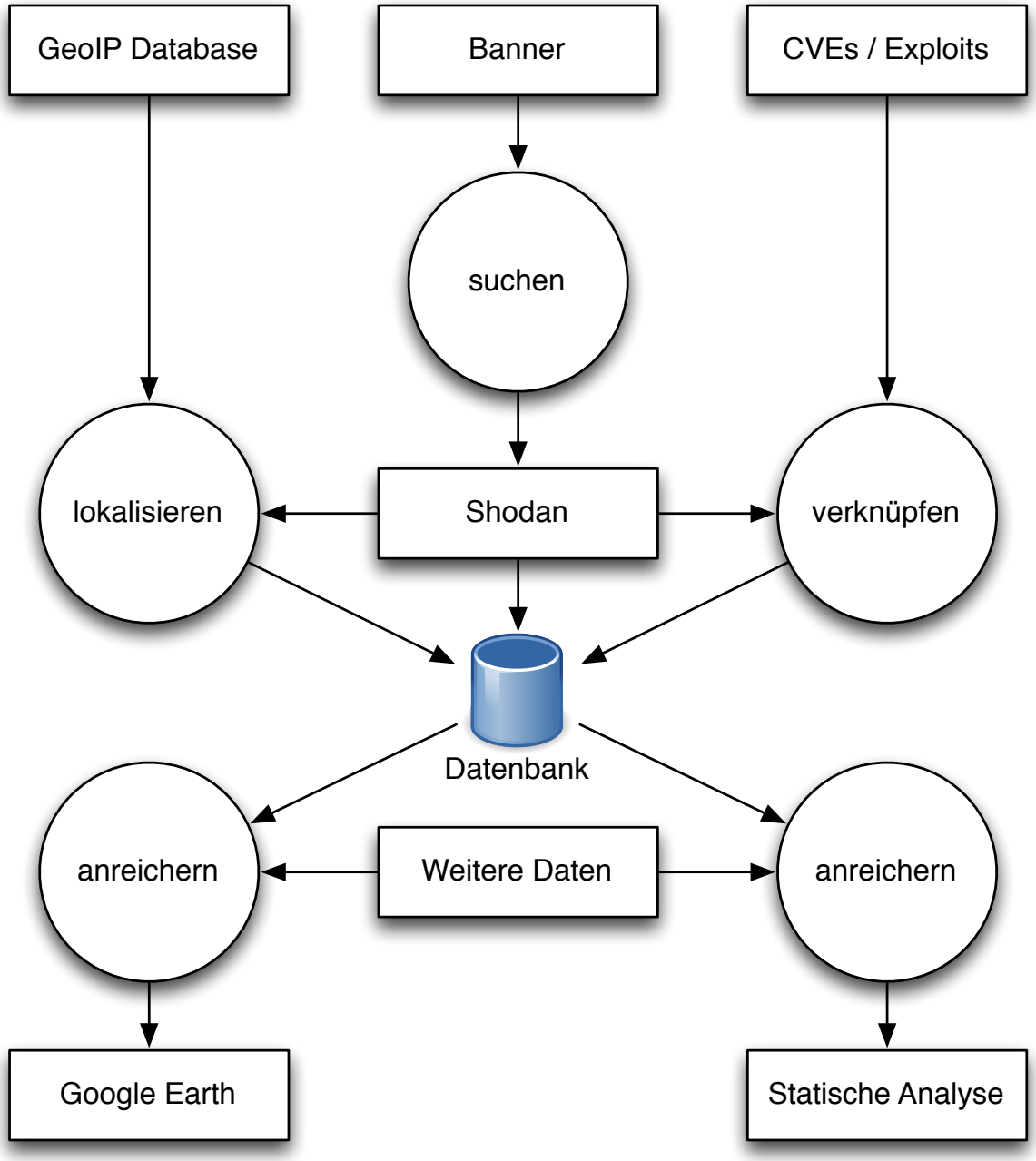
Steuerungen sind schlecht Geschützt gegen Angreifer

- 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



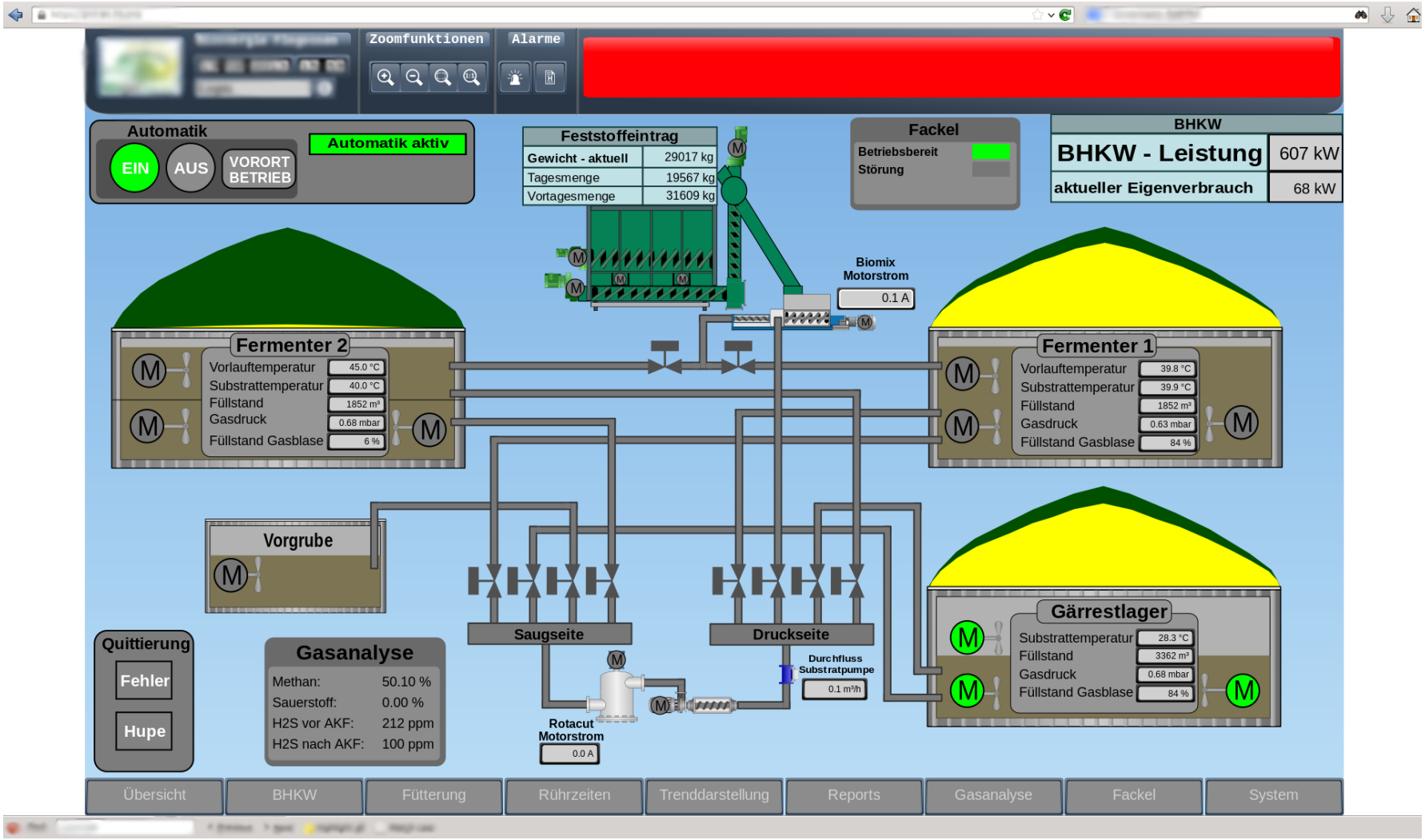
Methodik - SHODAN Funktionsweise

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

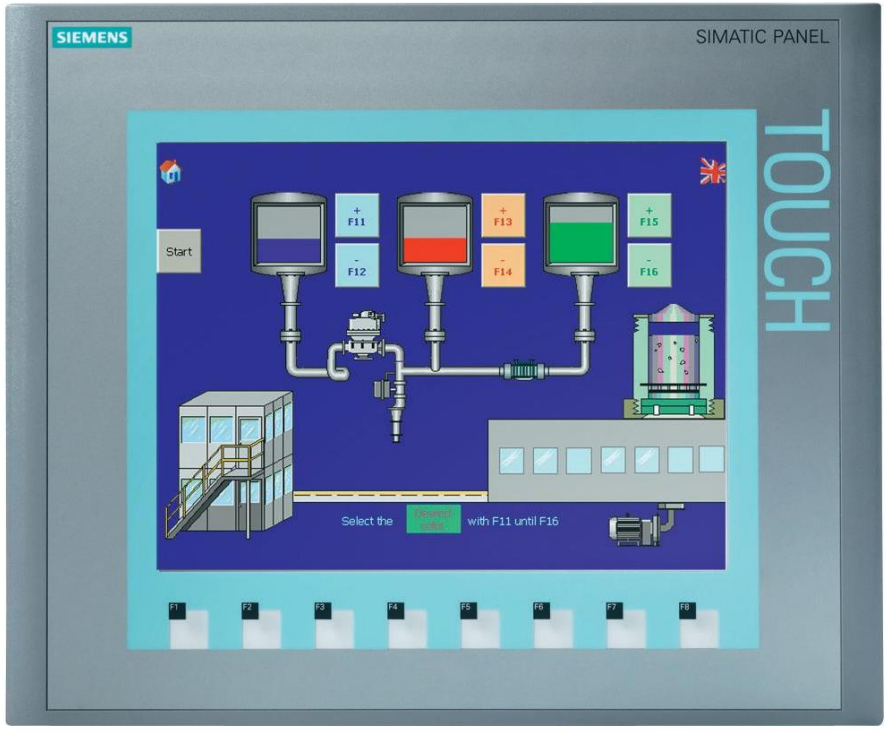
PLC - Programmable Logic Controller

SCADACS

PLC Network Devices (PLCND)

SCADACS

HMI - Human Machine Interfaces



SCADACS

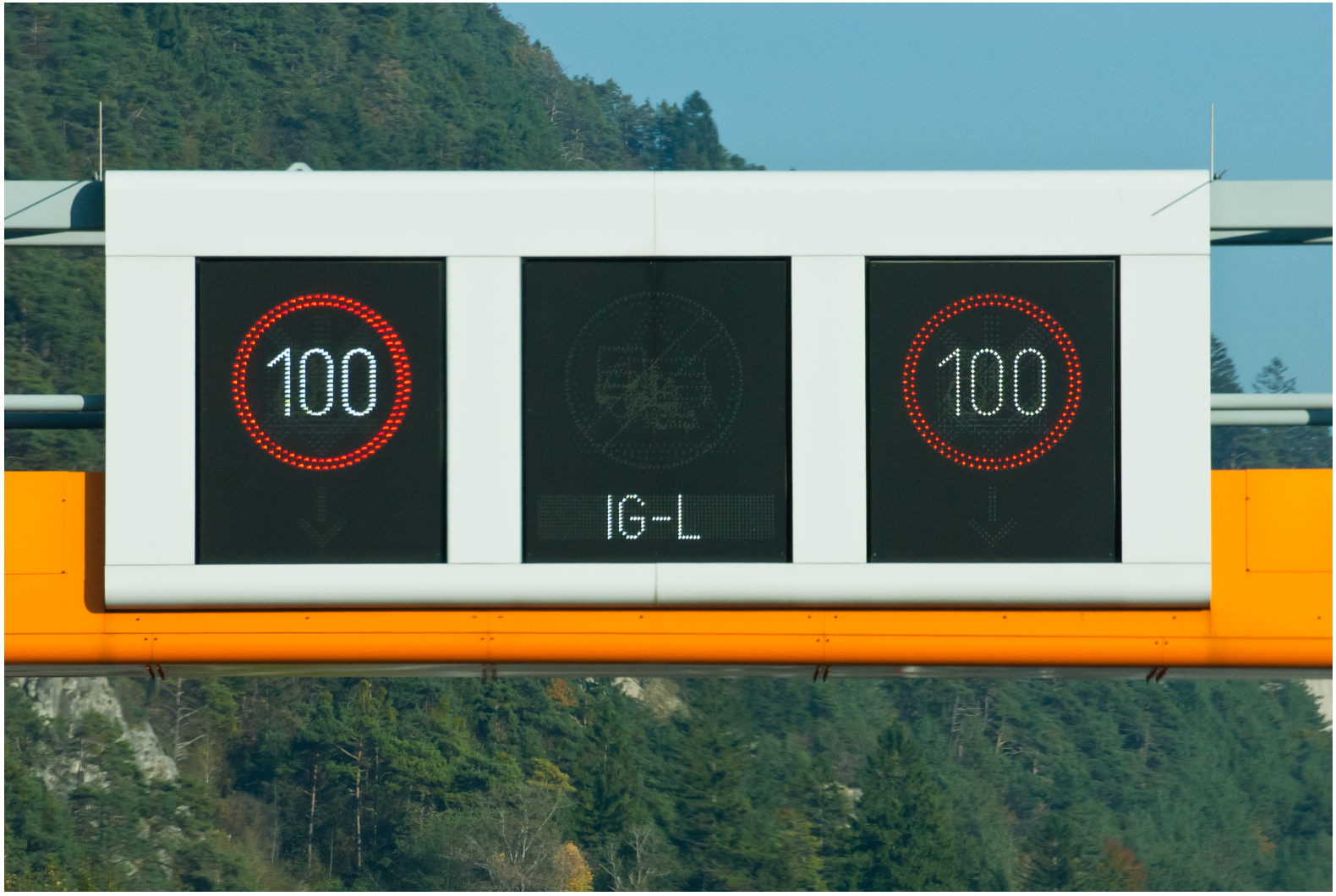
BMS - Building Management Systems

SCADACS

PDU - Power Distribution Units

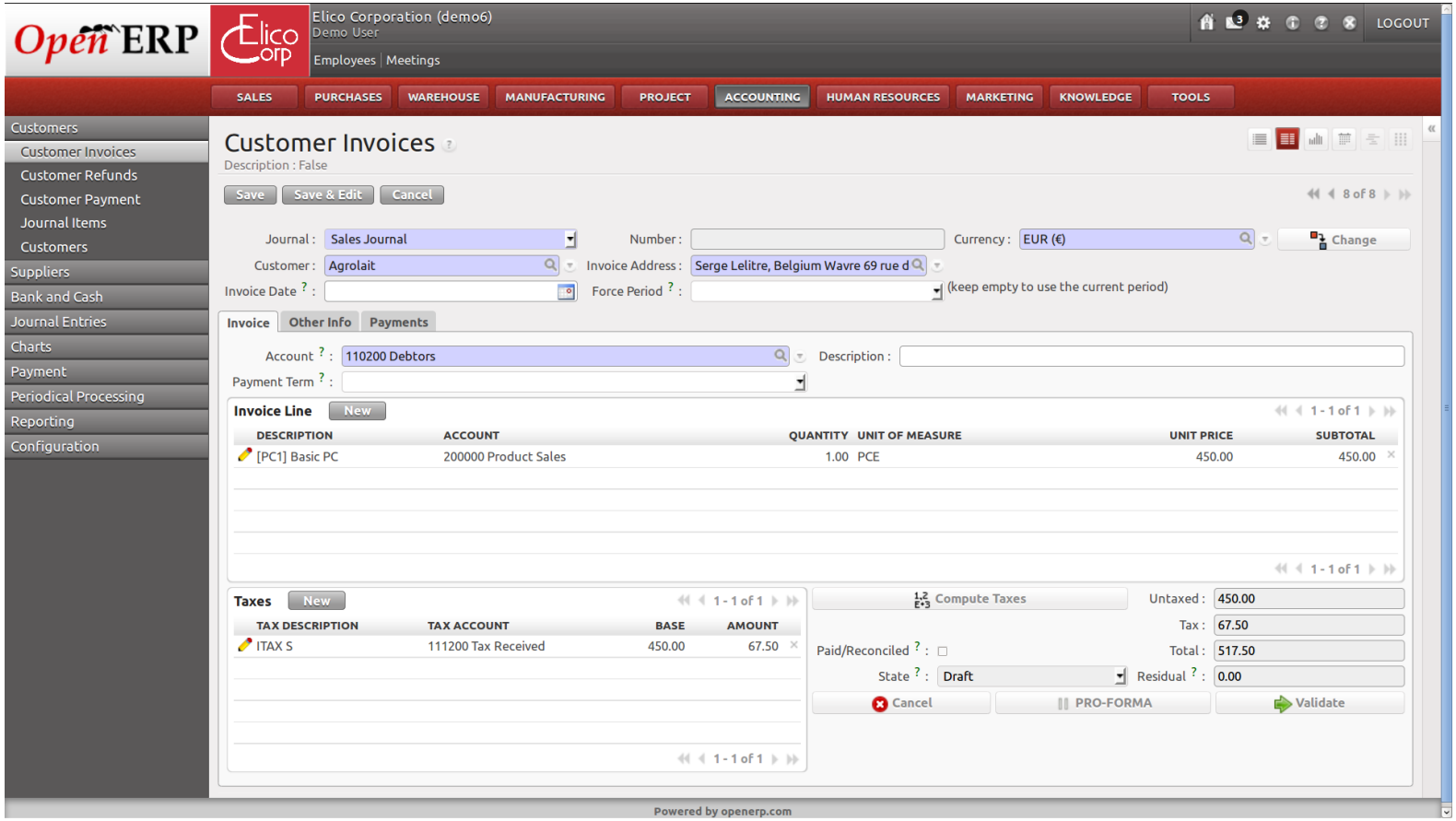
SCADACS

TM - Traffic Management Devices



SCADACS

ERP - Enterprise Rescource Planning Systems



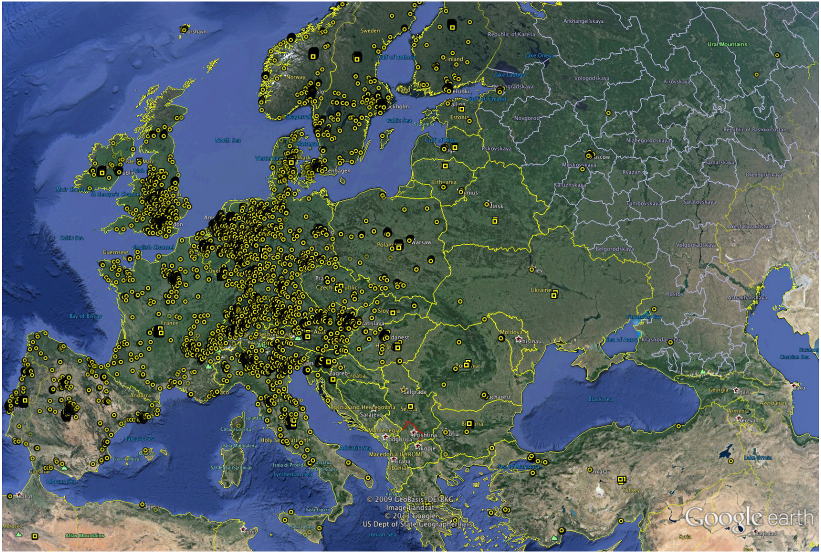
SCADACS

UPS - Uninterruptible Power Supplys

SCADACS

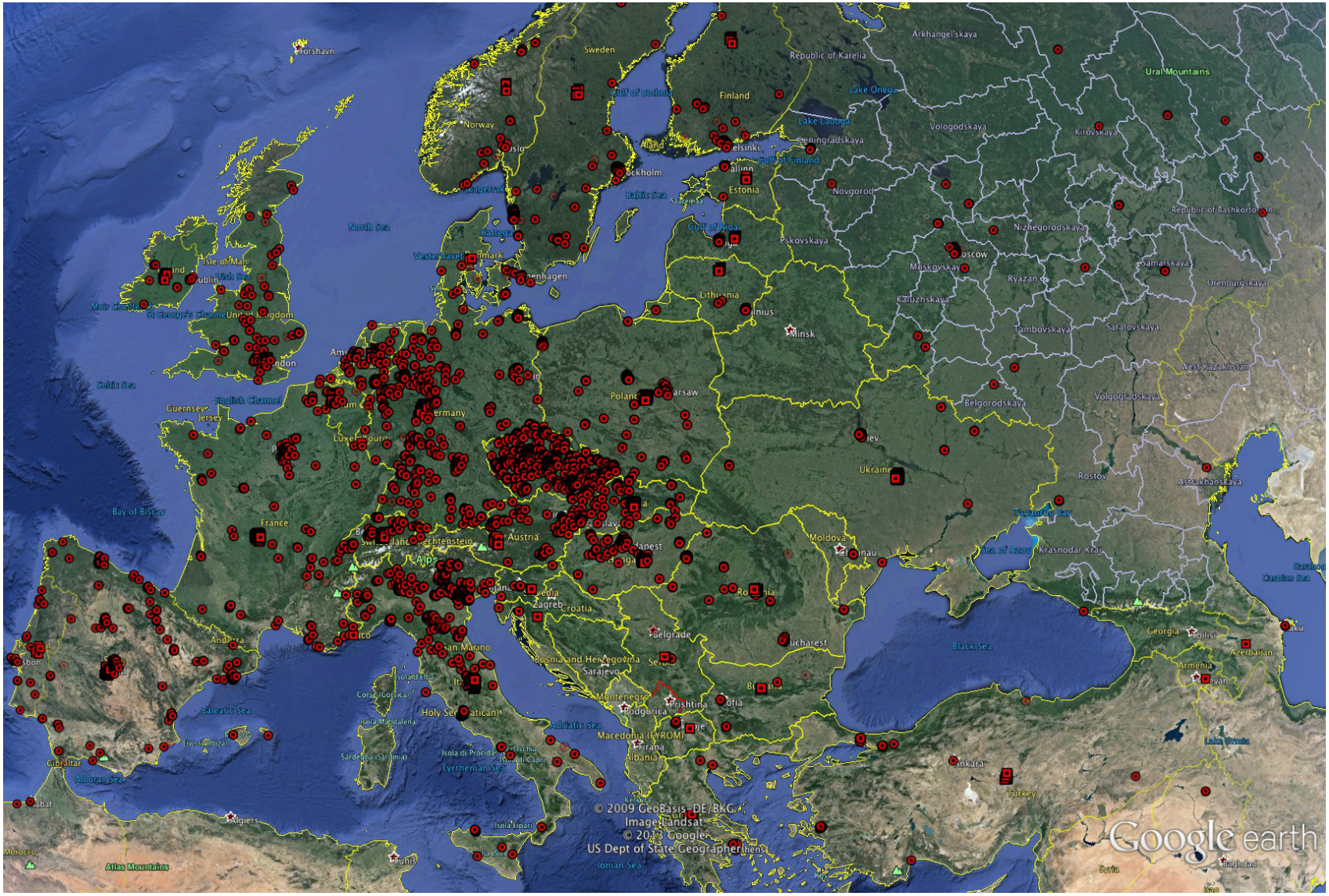
Ergebnisse

IRAM - Deutschland - BMS



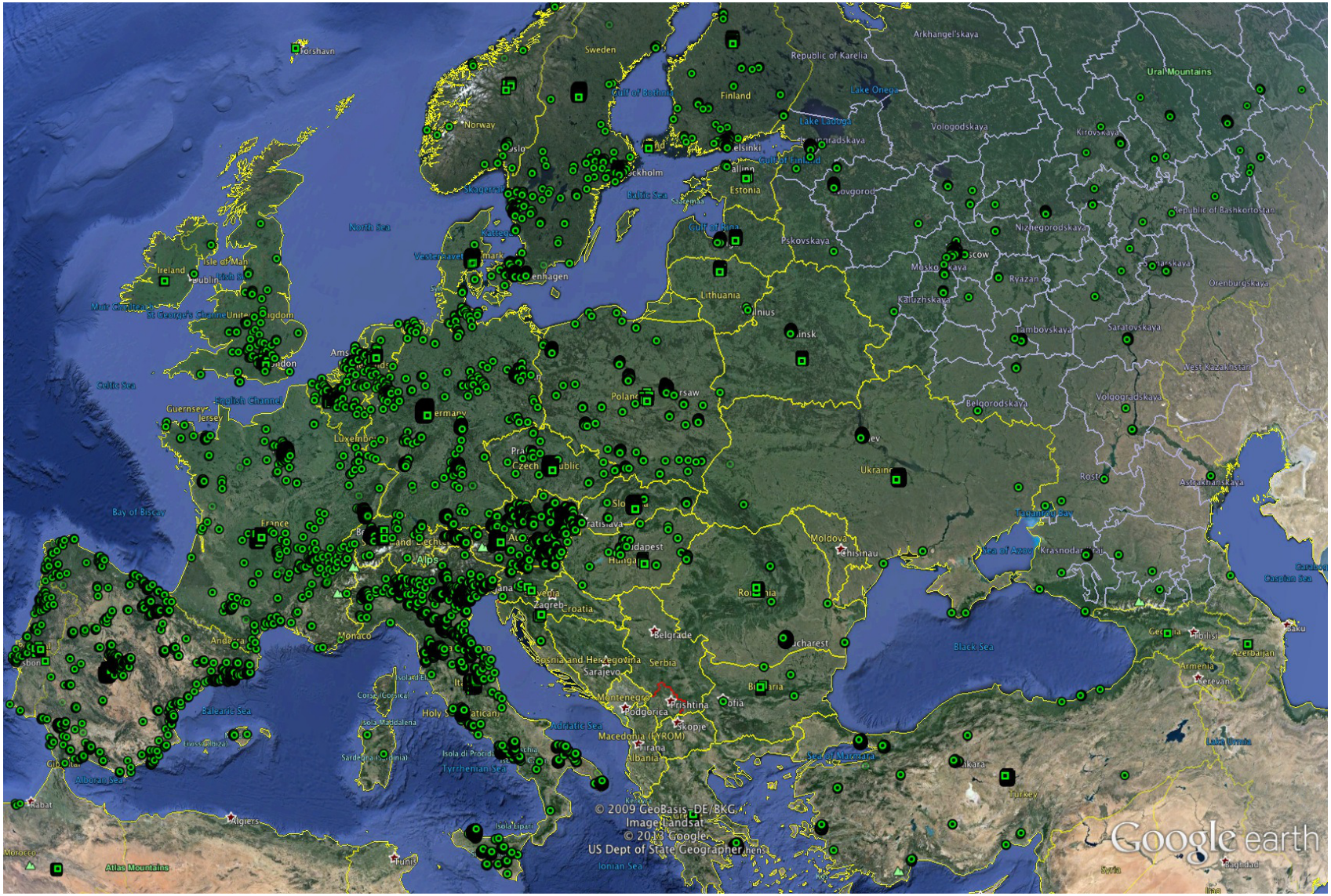
SCADACS

IRAM - Deutschland - PLC



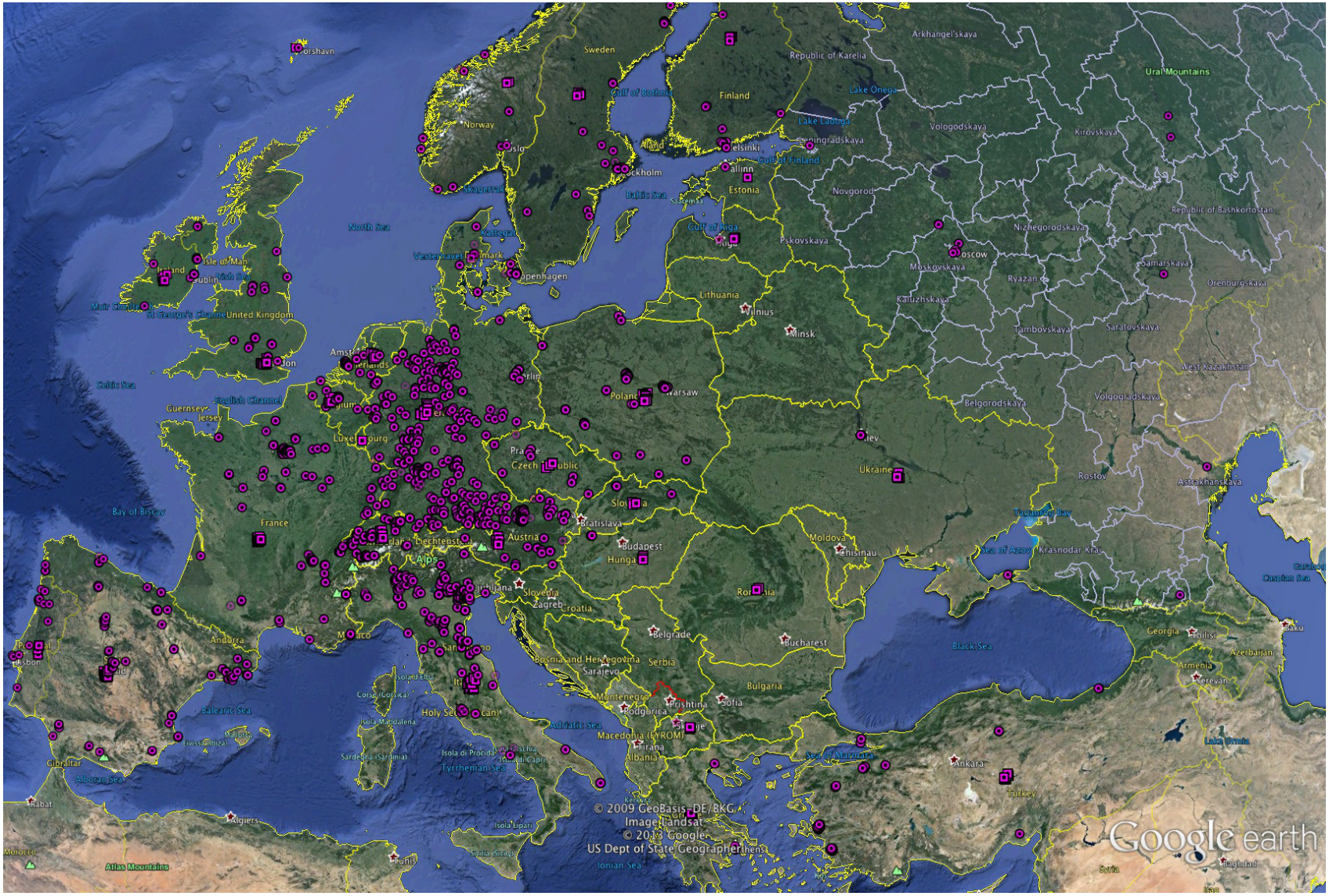
SCADACS

IRAM - Deutschland - PLCND



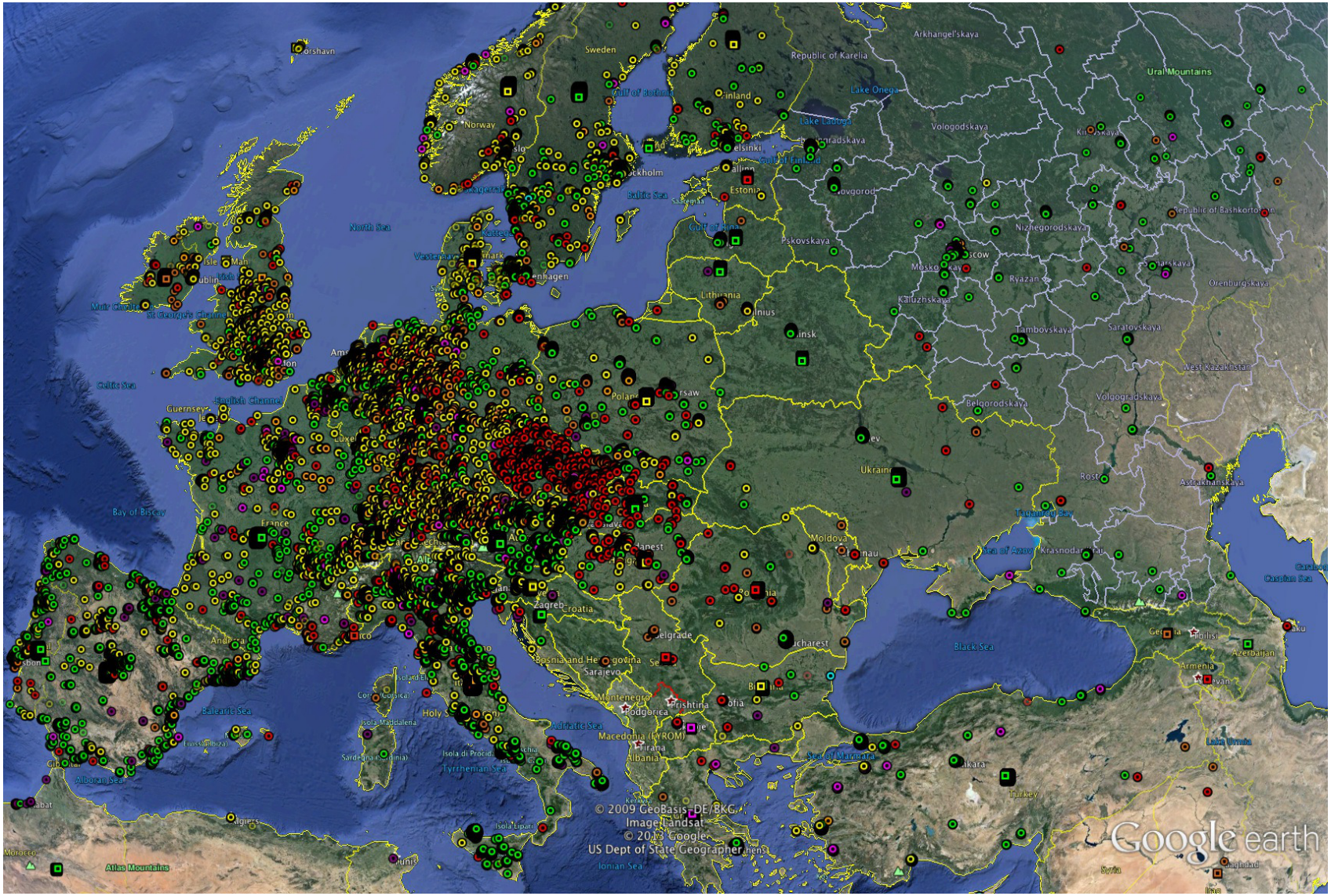
SCADACS

IRAM - Deutschland - SCADA



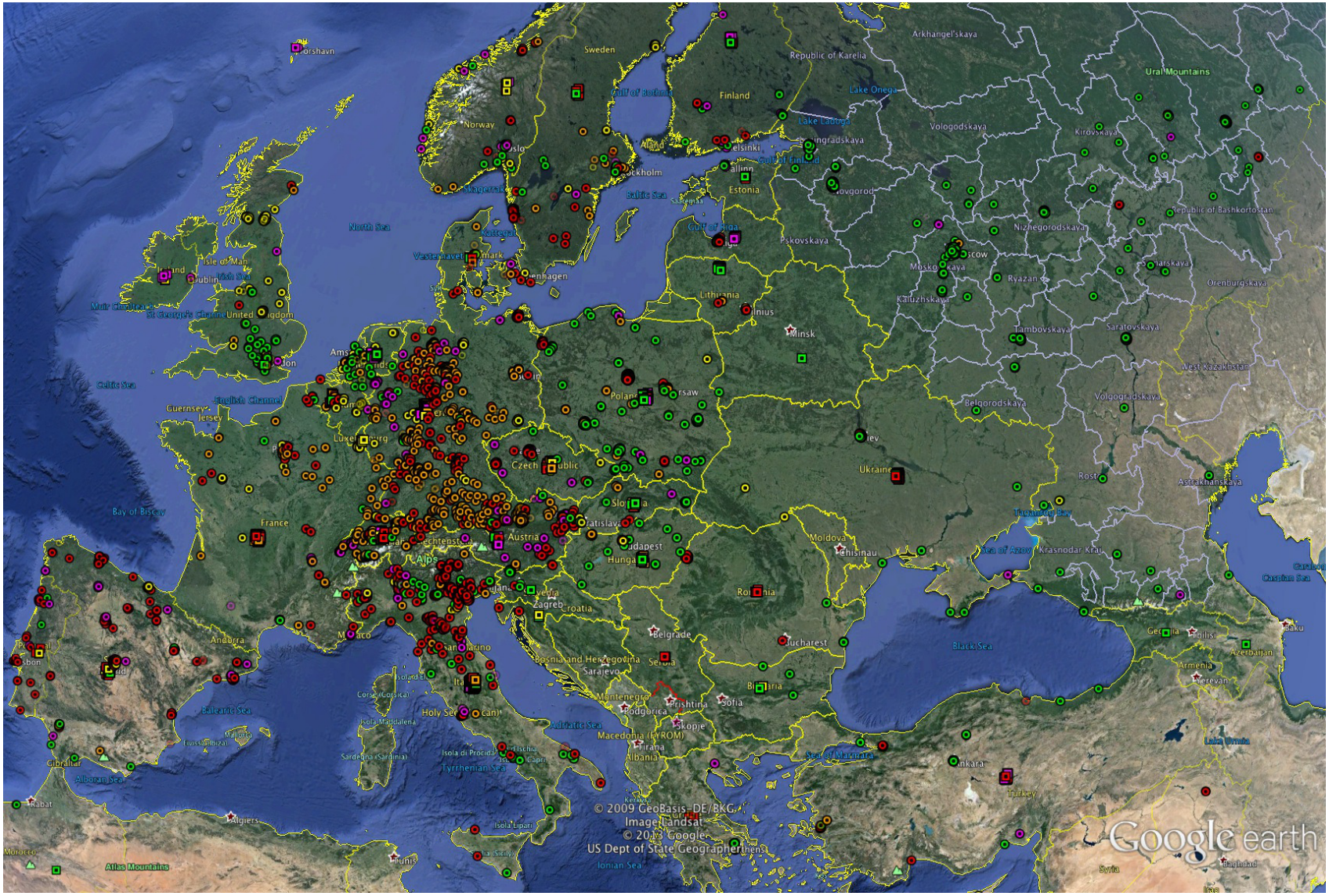
SCADACS

IRAM - Europa



SCADACS

IRAM - Europa (verwundbar)



SCADACS

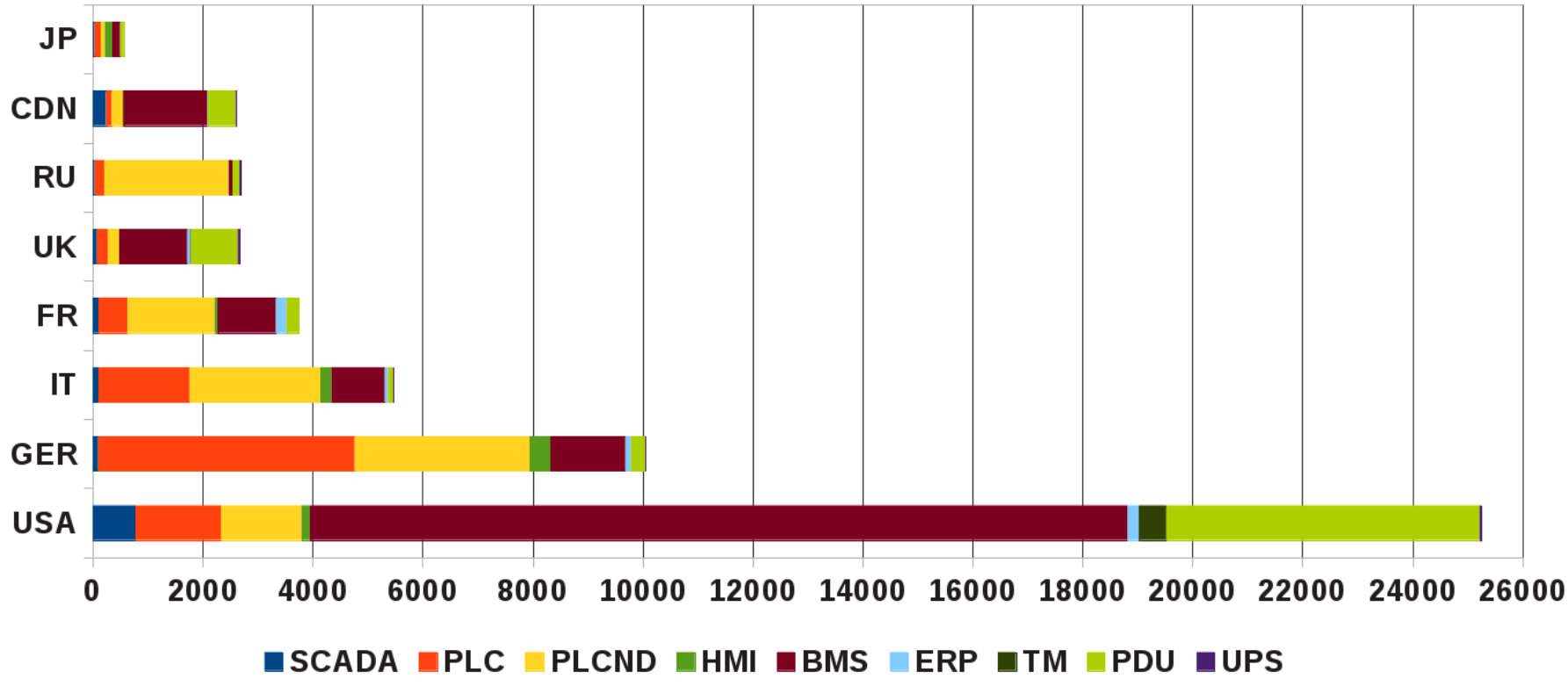
Auswertung

Kennzahlen

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

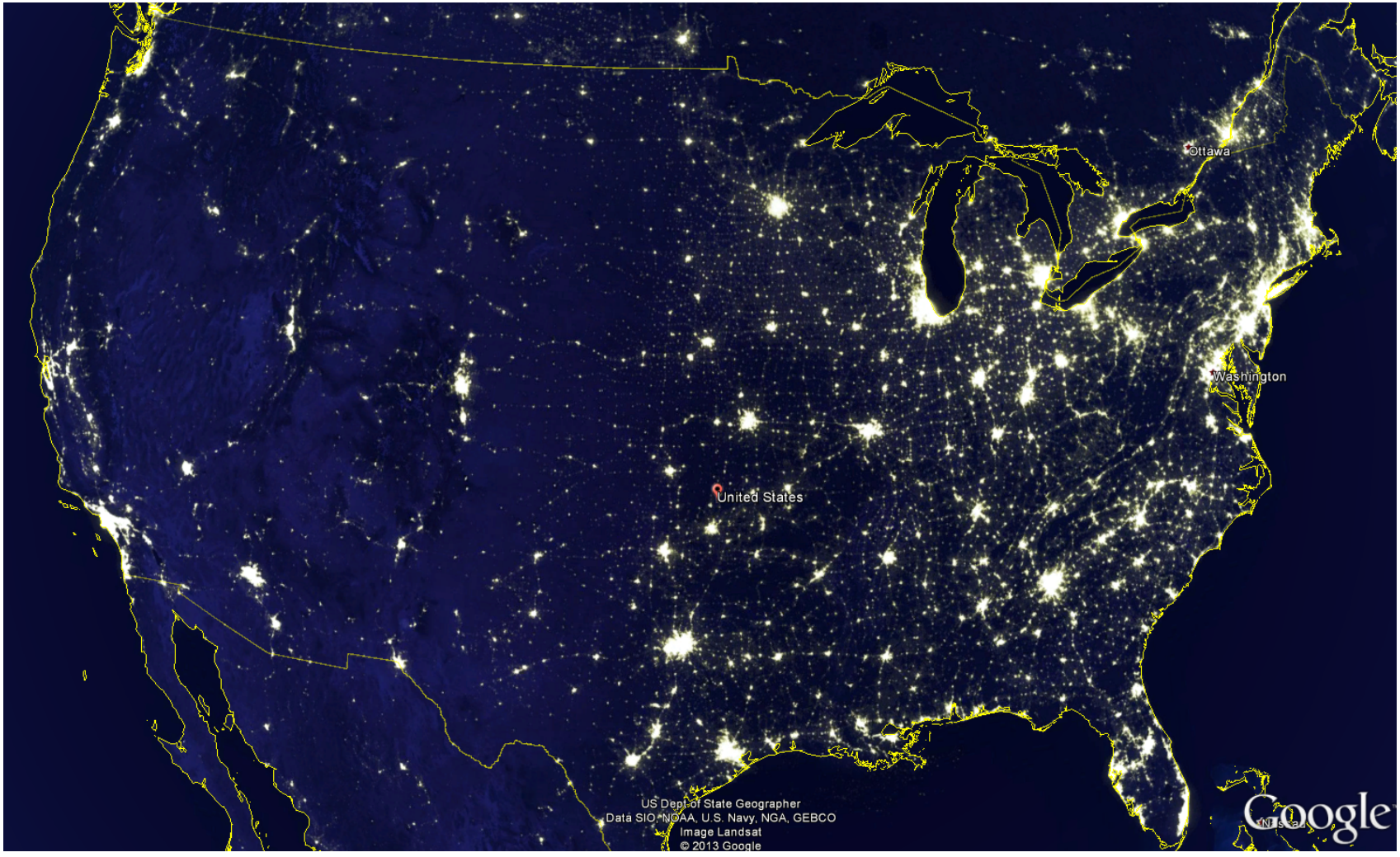
Kategorien	**Geräte**	**CVEs/Exploits**
BMS	31.411	9%
PLCND	23.873	14%
PDU	10.381	0%
PLC	7.254	26%
SCADA	2.254	28%
HMI	1.741	41%
ERP	1.400	0%
TM	788	0%
UPS	167	0%

Kennzahlen



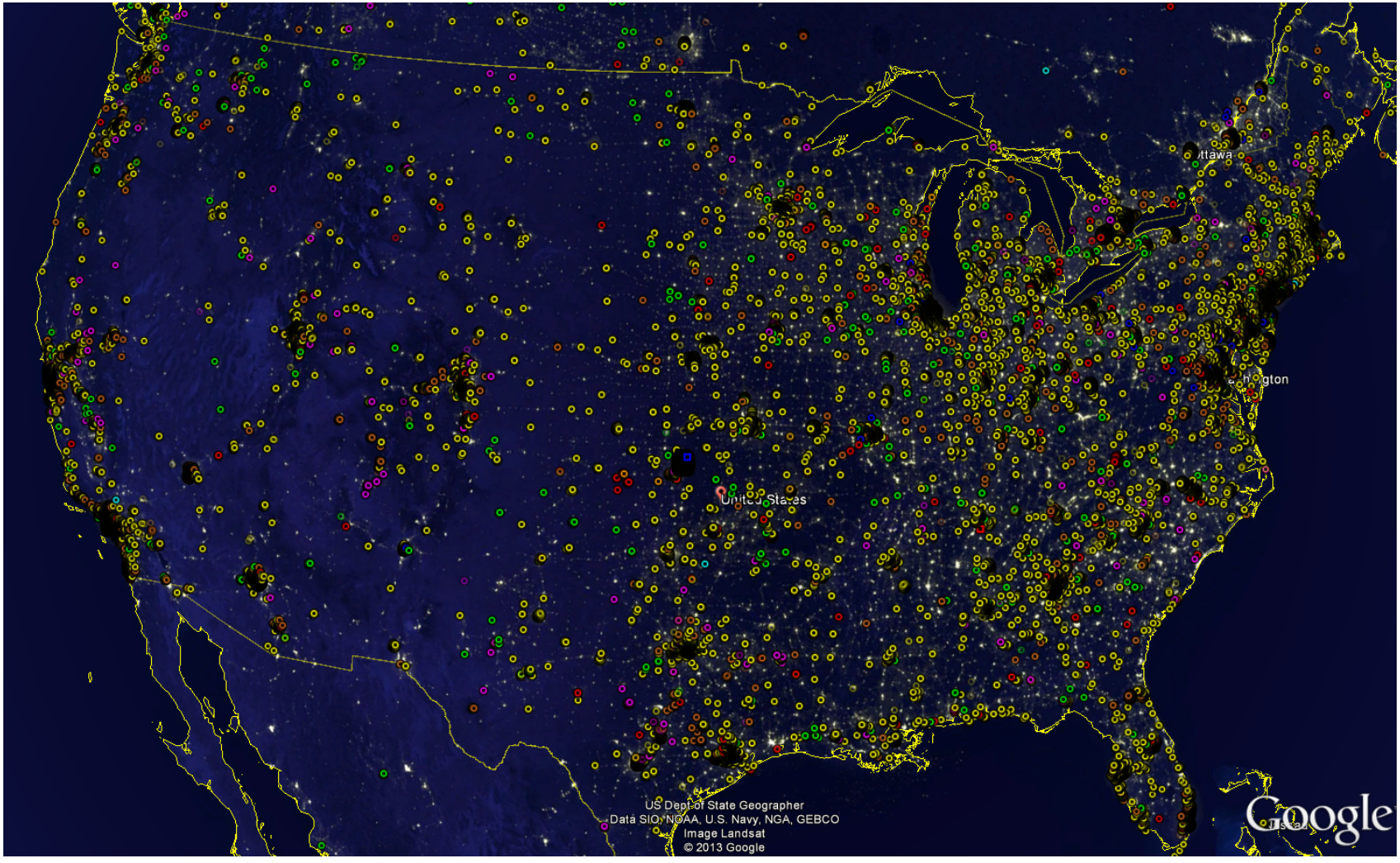
SCADACS

IRAM - USA Nachtaufnahme ohne Steuerungen



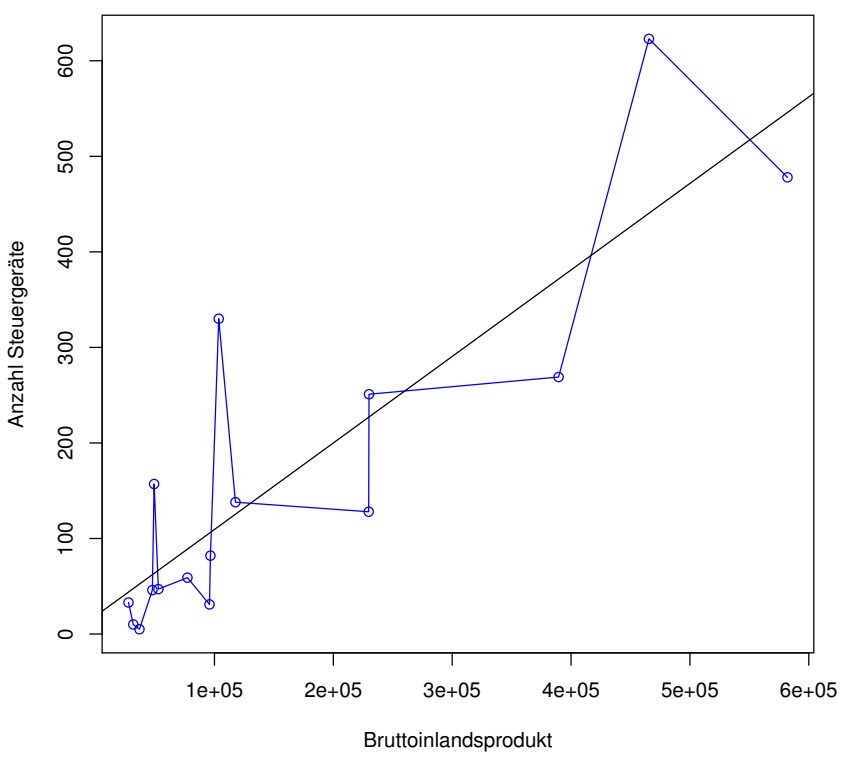
SCADACS

IRAM - USA Nachtaufnahme mit Steuerungen

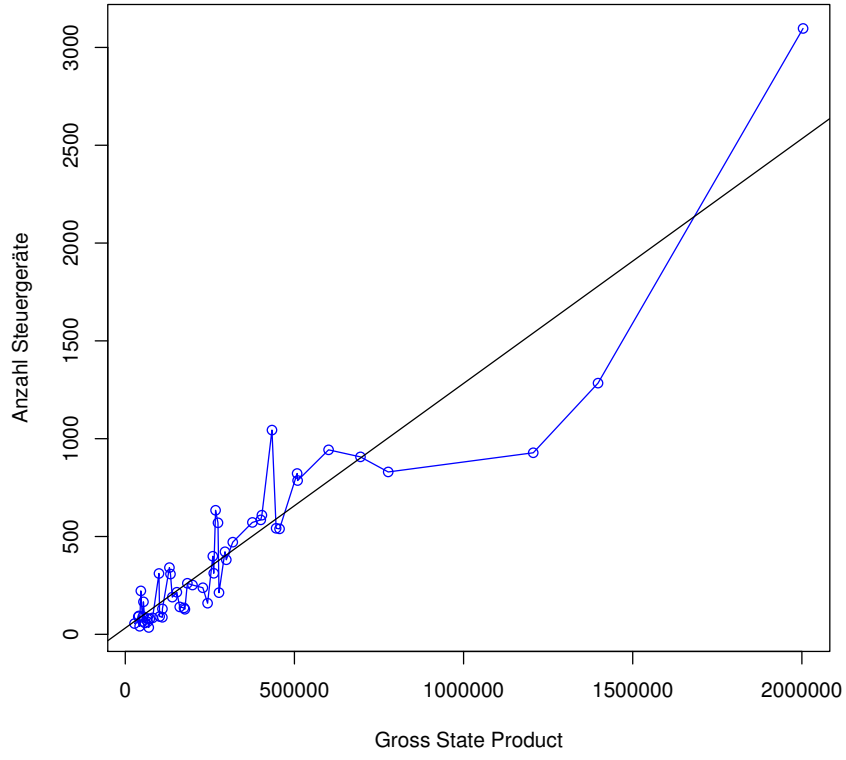


SCADACS

Korrelation zur Wirtschaftsleistung



(a) Deutschland (Jahr 2012)



(b) USA (Jahr 2012)

SCADACS

Fallstudie - Saia-Burgess

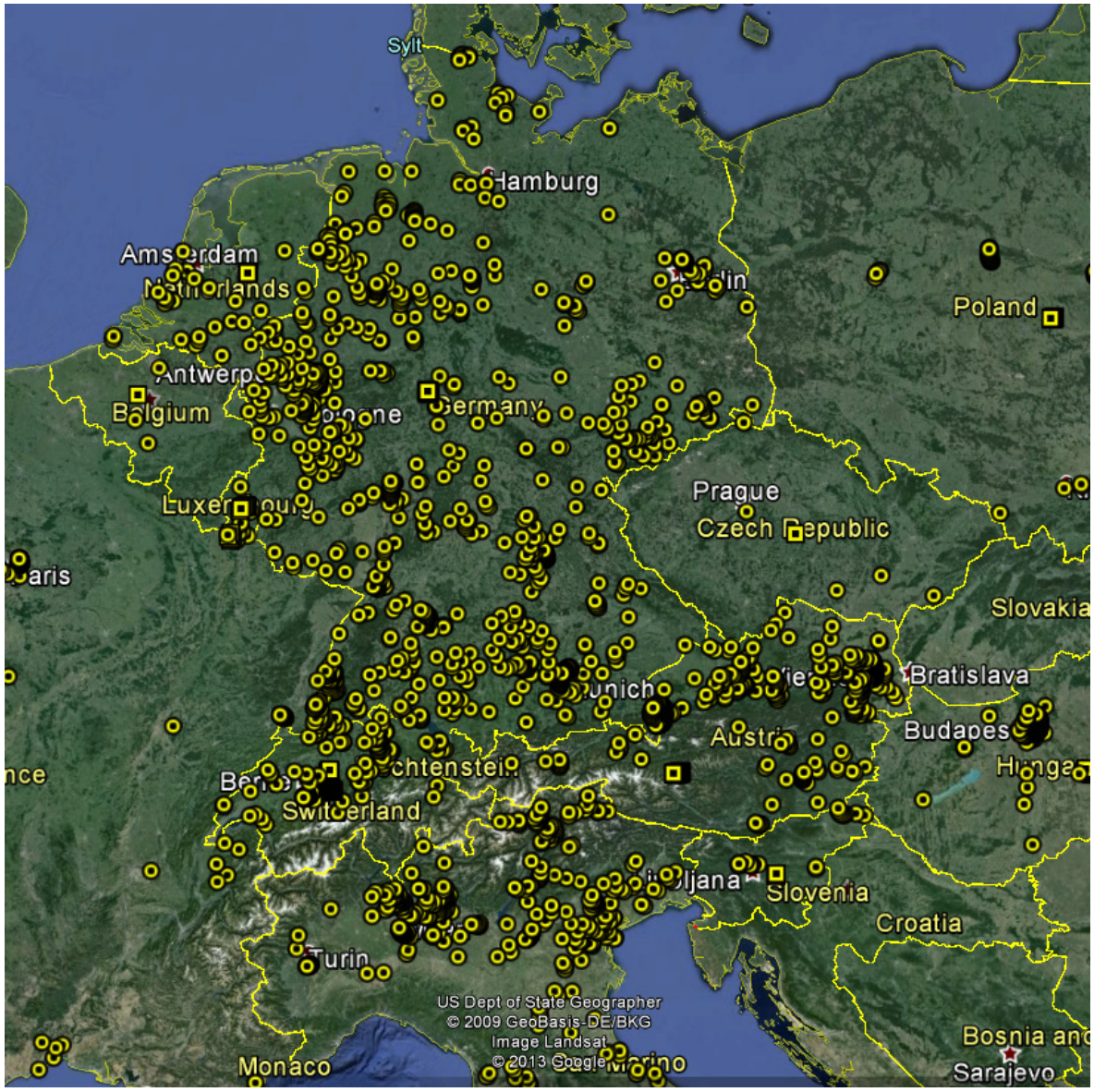
- Heise berichtete 2013 über Verwundbarkeiten
- Vaillant nennt 1.500 betroffene Geräte in Deutschland
- Saia-Burgess nennt 200.000 Geräte weltweit
- Wir haben 2.897 Geräte weltweit gefunden

Fallstudie - Saia-Burgess

Tabelle: Länder mit mehr als 50 betroffenen Anlagen.

Land	**Anzahl**
Deutschland	859
Italien	598
Österreich	414
Schweiz	201
Portugal	145
Frankreich	129
Schweden	127
Israel	101
Ungarn	97
Polen	54

Fallstudie - Saia-Burgess - Deutschland



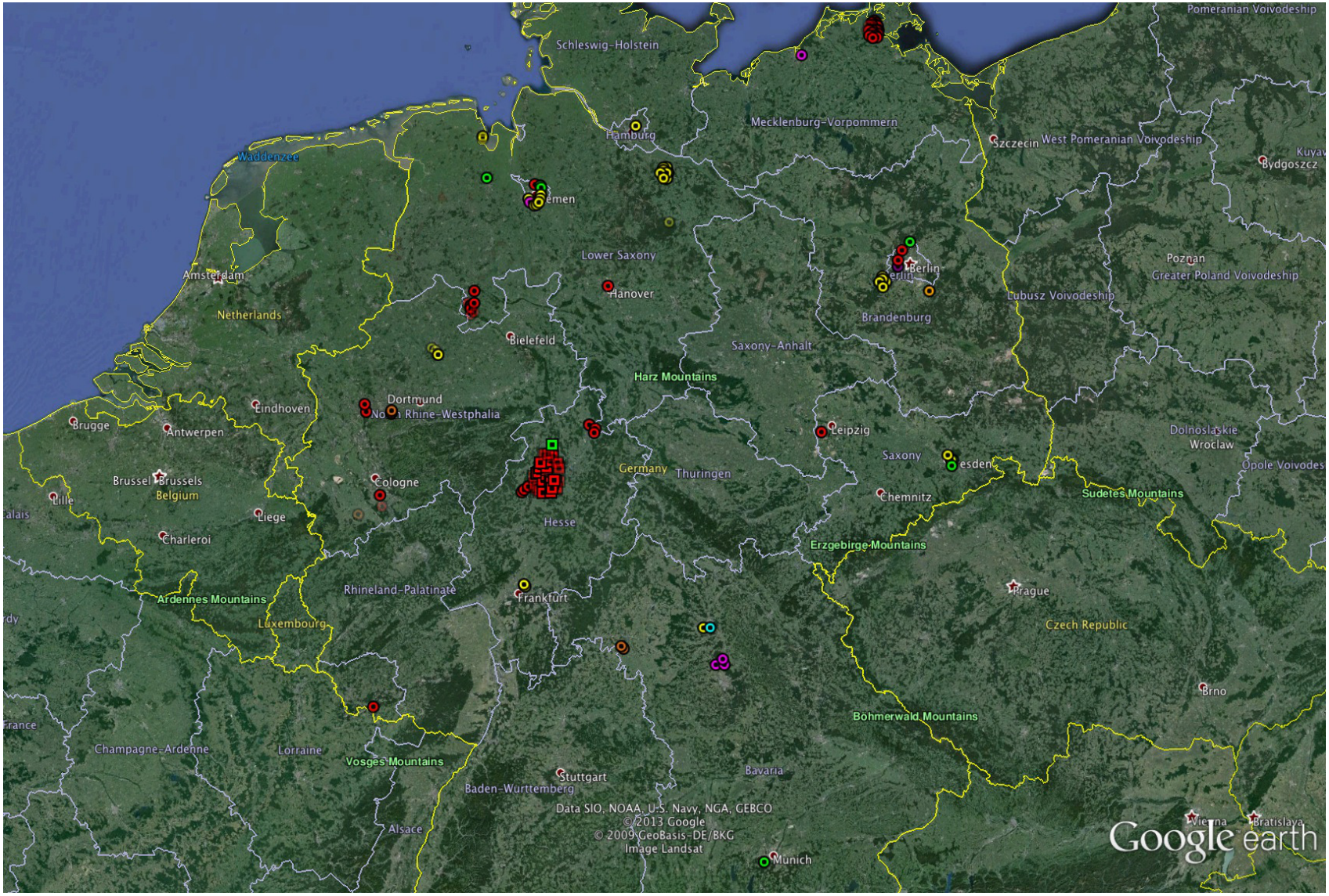
SCADACS

Fallstudie - DFN

Tabelle: Anzahl der Geräte pro Kategorie im DFN AS

Kategorien	**Anzahl**
PLC	86
BMS	32
PLCND	8
PDU	6
SCADA	5
ERP	1
HMI	1
UPS	1
TM	0

Fallstudie - DFN



SCADACS

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
- Es besteht Handlungsbedarf

IRAM - Demonstration (Video)

Video

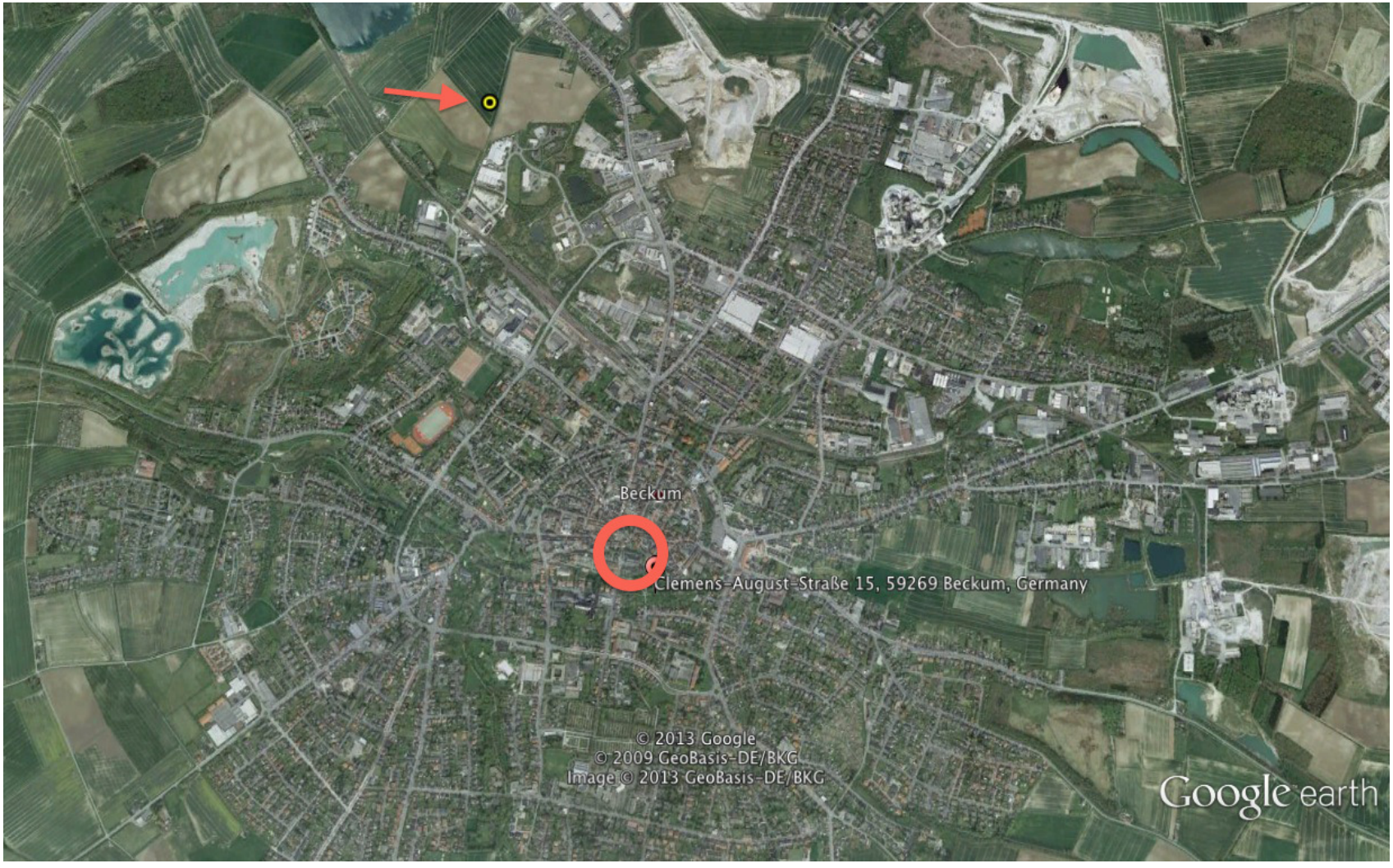
Vielen Dank für Ihre Aufmerksamkeit!

http://www.scadacs.org

IRAM - Asien

SCADACS

IRAM - Asien



SCADACS