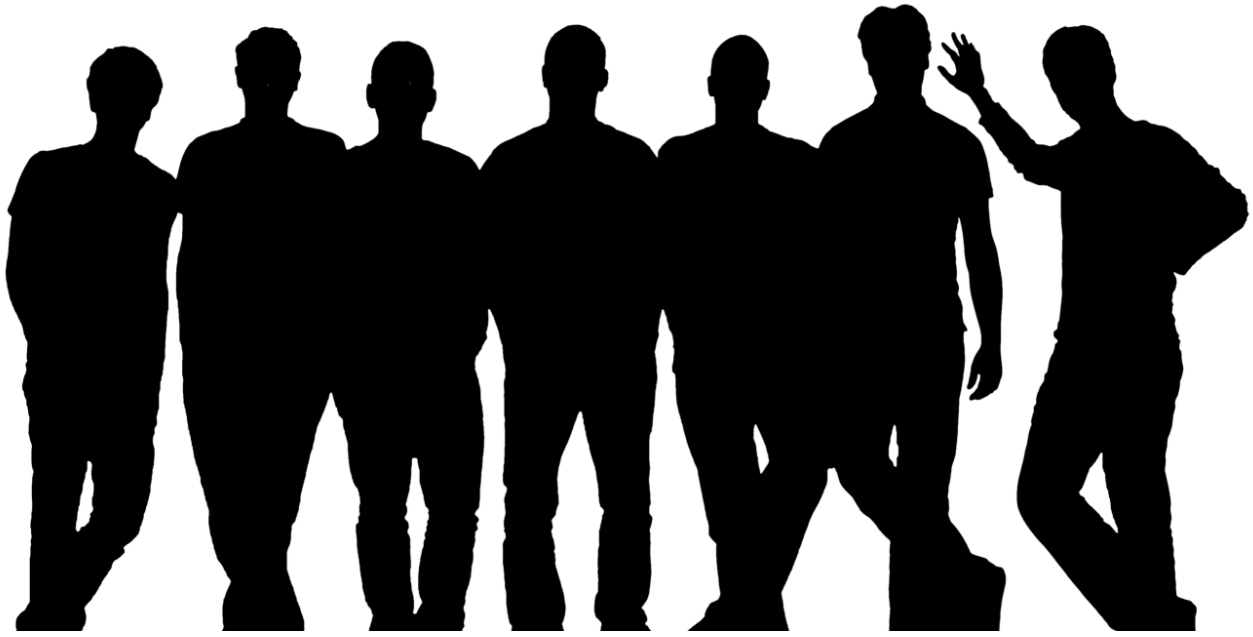
Industrial Risk Assessment Map (IRAM)

Ein graphisches Werkzeug zur Bedrohungsanalyse

Johannes Klick, Jan-Ole Malchow

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

SCADACS

Problemstellung

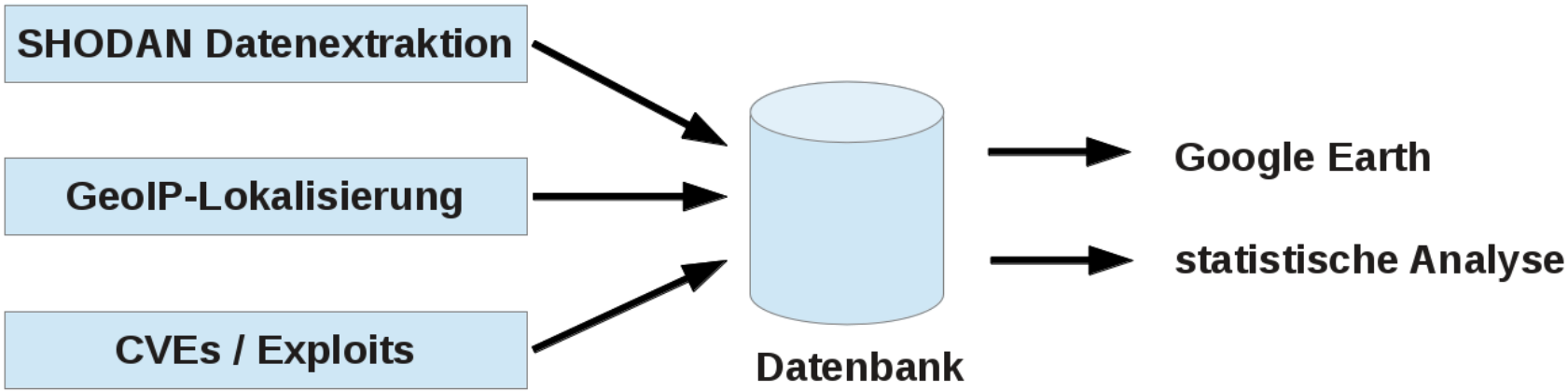
Steuerungen sind schlecht Geschützt gegen Angreifer

- 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?
- Wie groß ist die Bedrohung für eine bestimmte Region im Falle eines Angriffs?

Methodik - Prozessübersicht



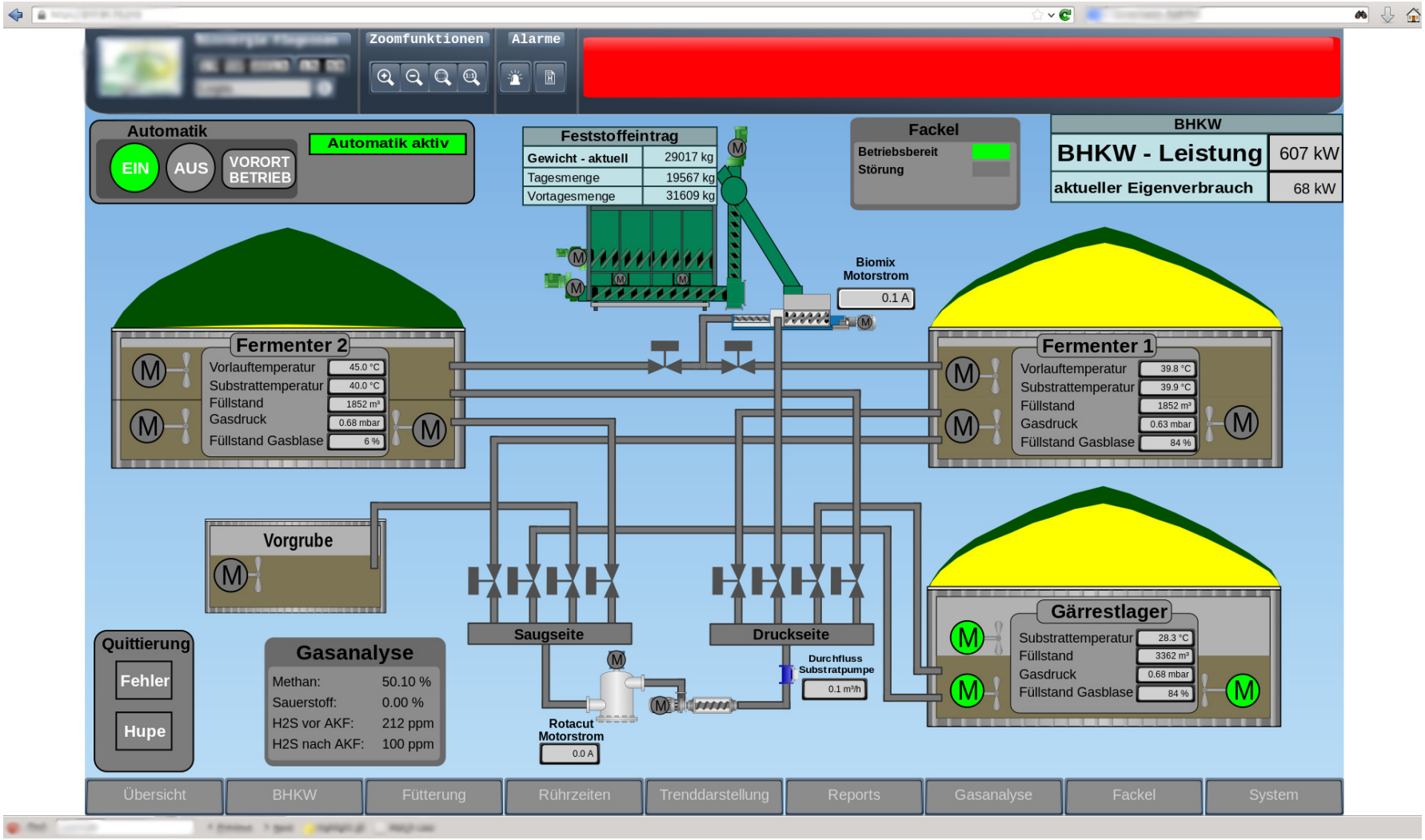
Methodik - SHODAN Funktionsweise

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
- Verbindunsgziele werden zufällig bestimmt
- findet Geräte im Internet, die WEB-Suchmachien wie Google nicht finden

Was für Steuerungen suchen wir im Internet?

SCADA Systeme



SCADACS

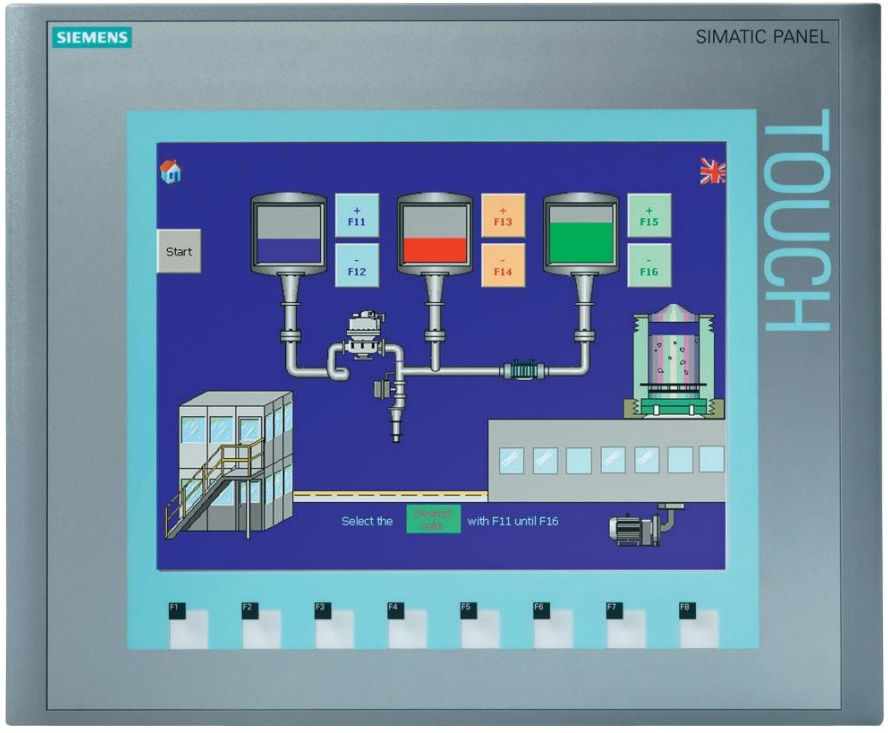
PLC - Programmable Logic Controller

SCADACS

PLC Network Devices (PLCND)

SCADACS

HMI - Human Machine Interfaces



SCADACS

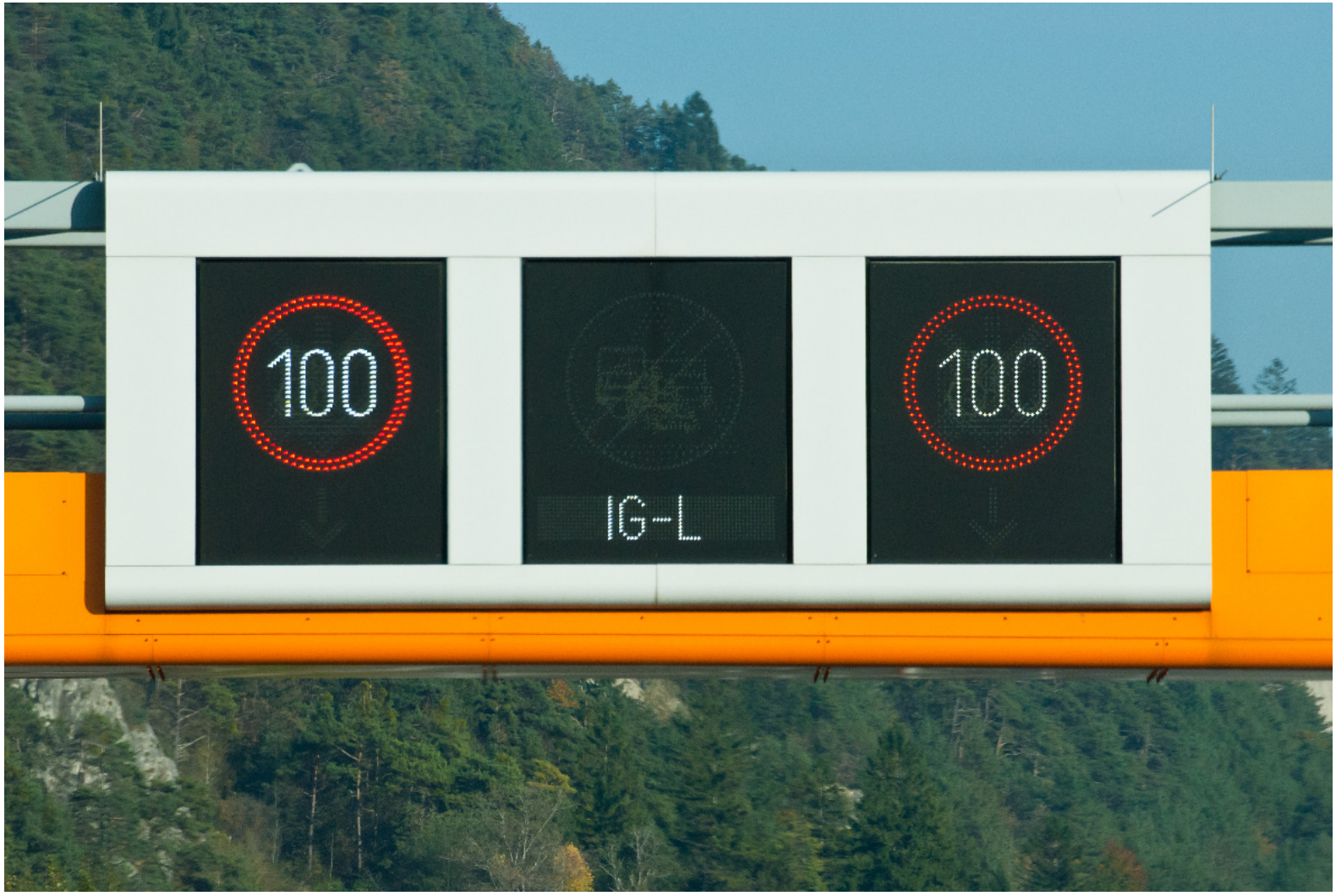
BMS - Building Management Systems

SCADACS

PDU - Power Distribution Units

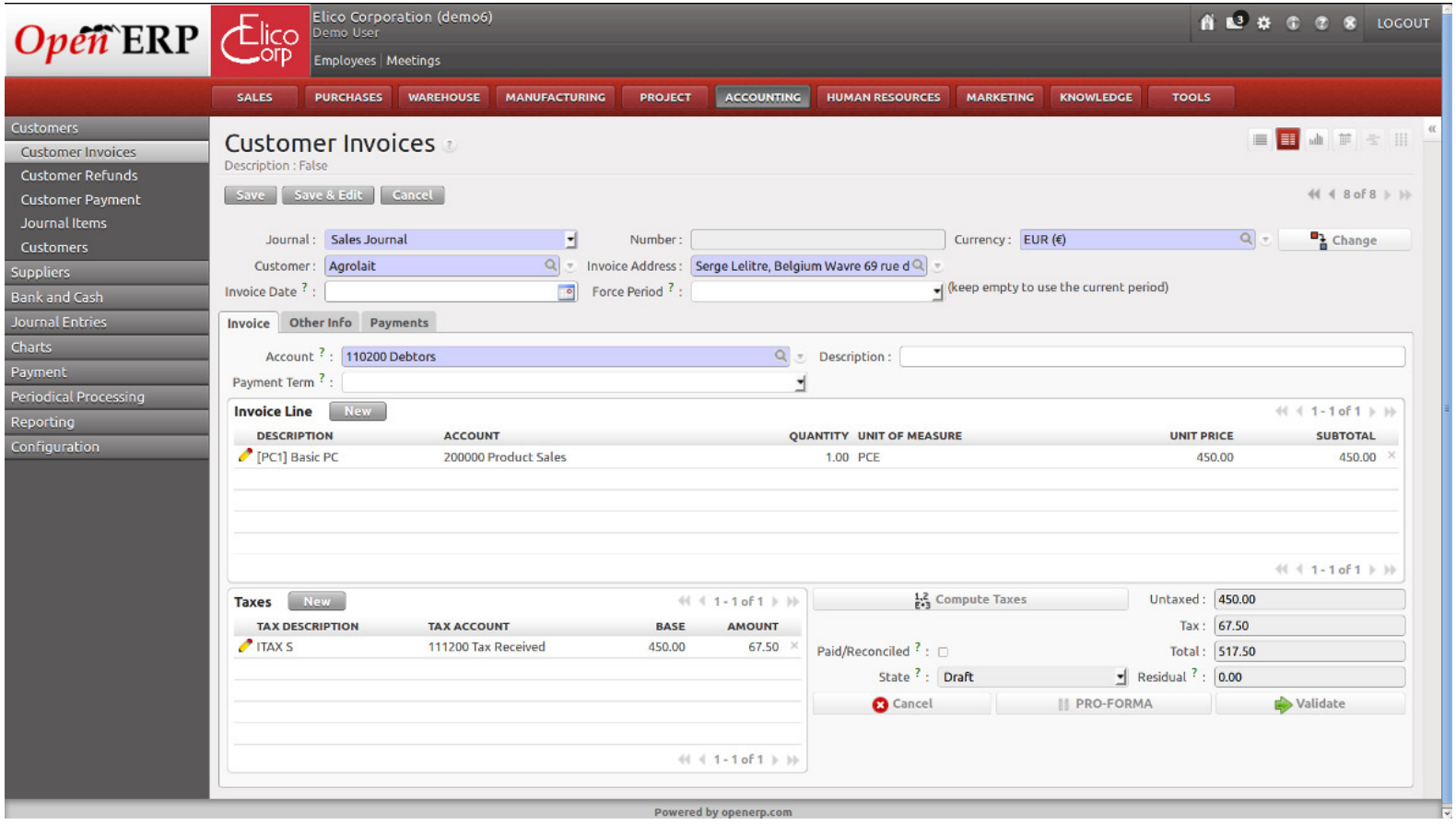
SCADACS

TM - Traffic Management Devices



SCADACS

ERP - Enterprise Rescource Planning Systems

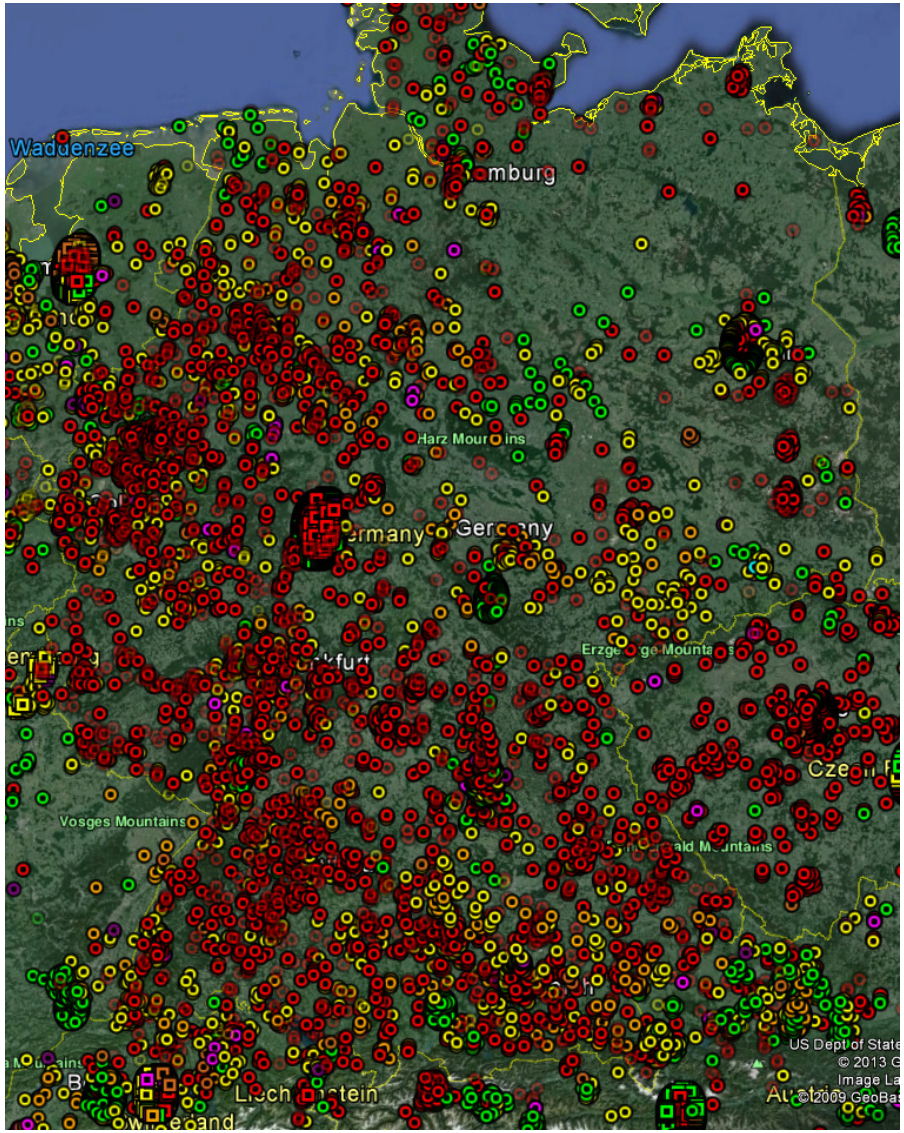


SCADACS

UPS - Uninterruptible Power Supplys

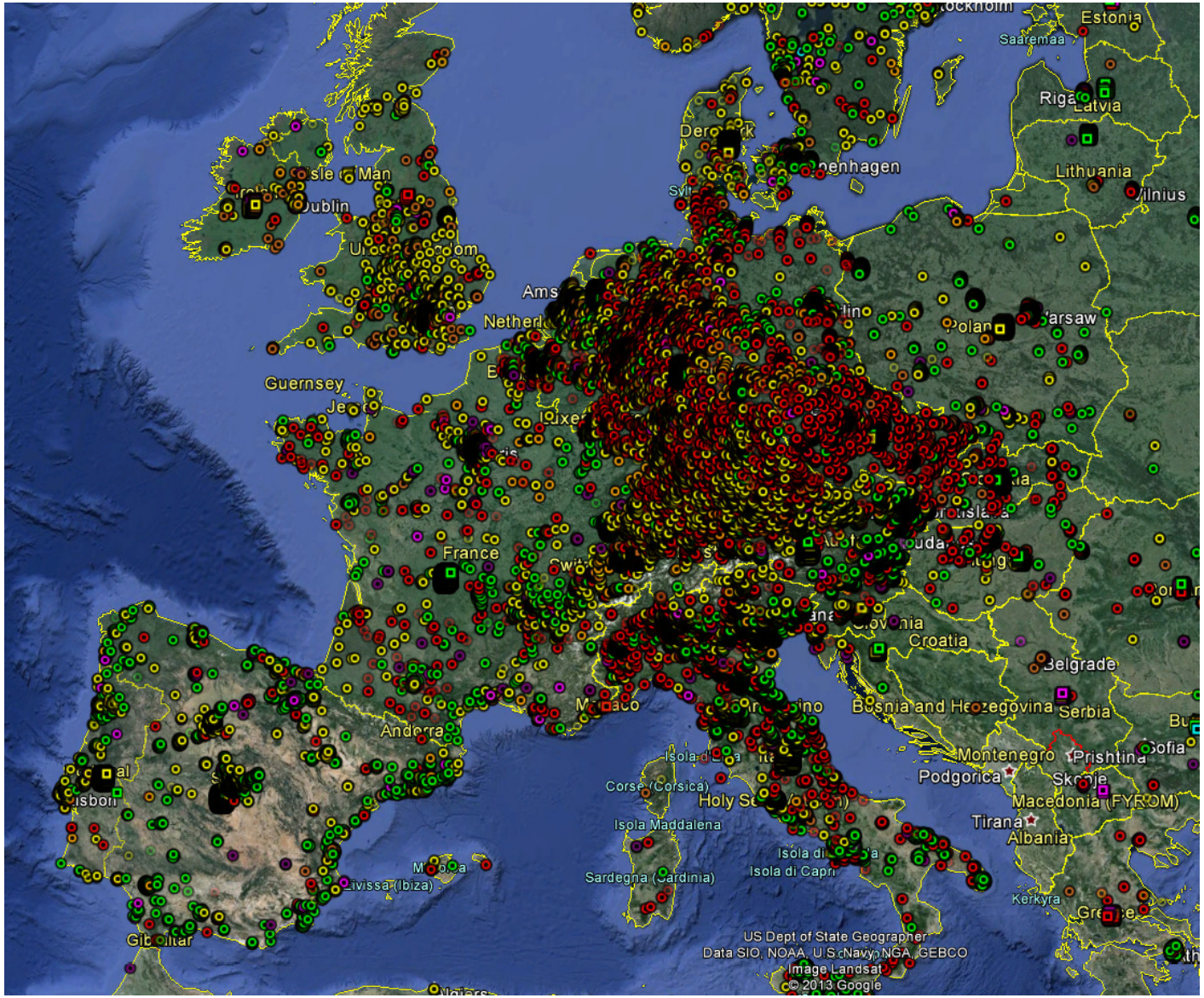
SCADACS

IRAM - Deutschland



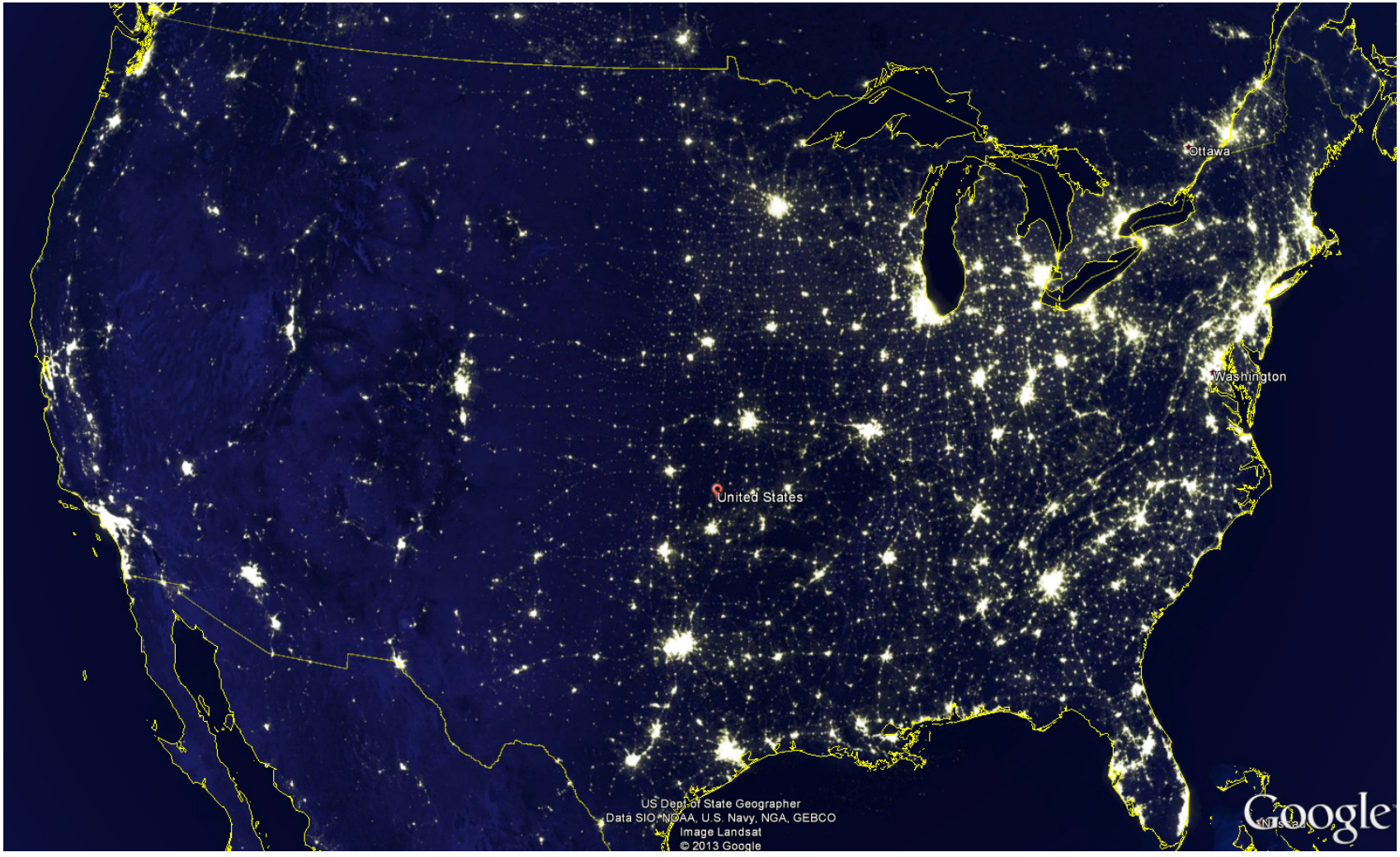
SCADACS

IRAM - Europa



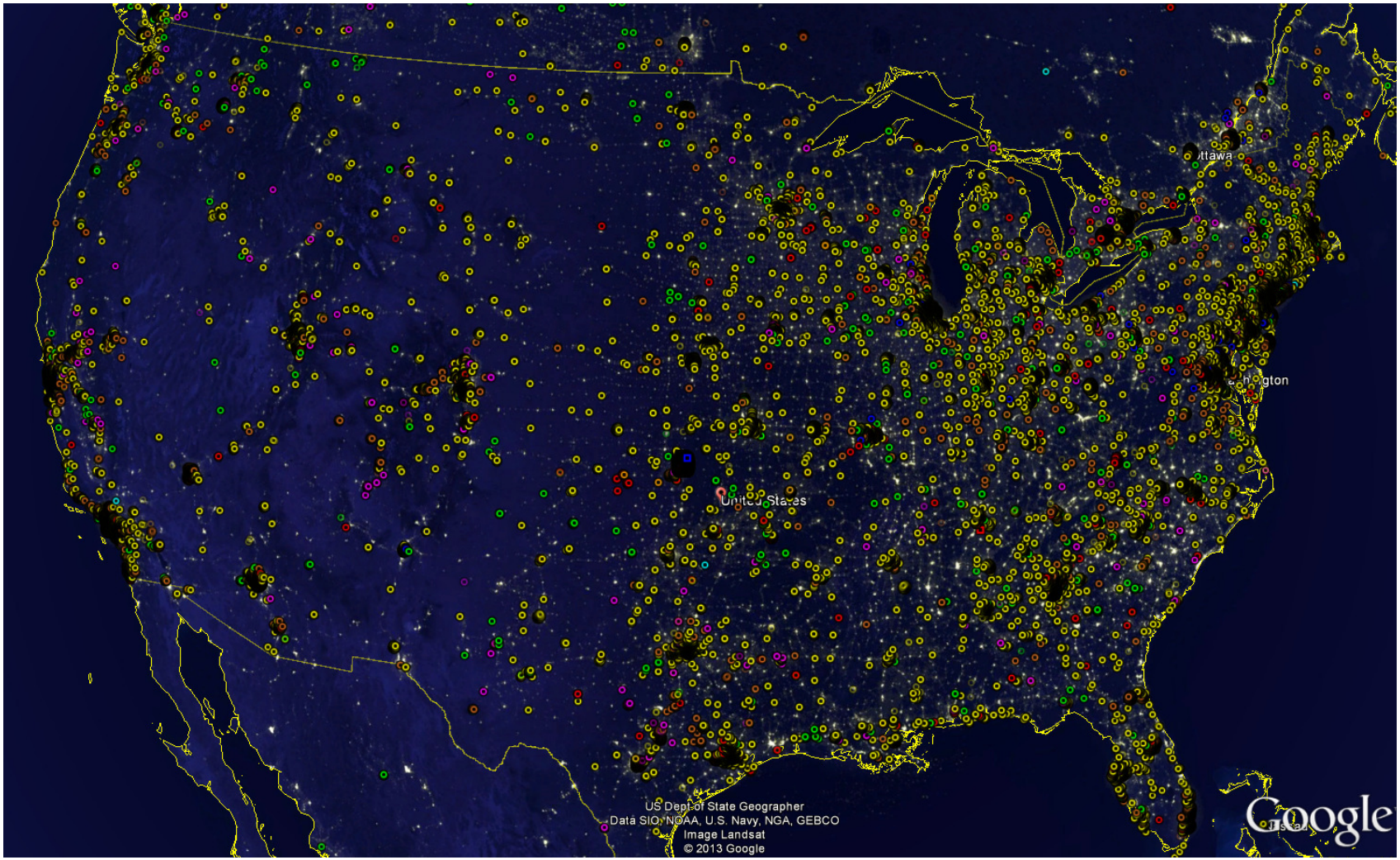
SCADACS

IRAM - USA Nachtaufnahme ohne Steuerungen



SCADACS

IRAM - USA Nachtaufnahme mit Steuerungen

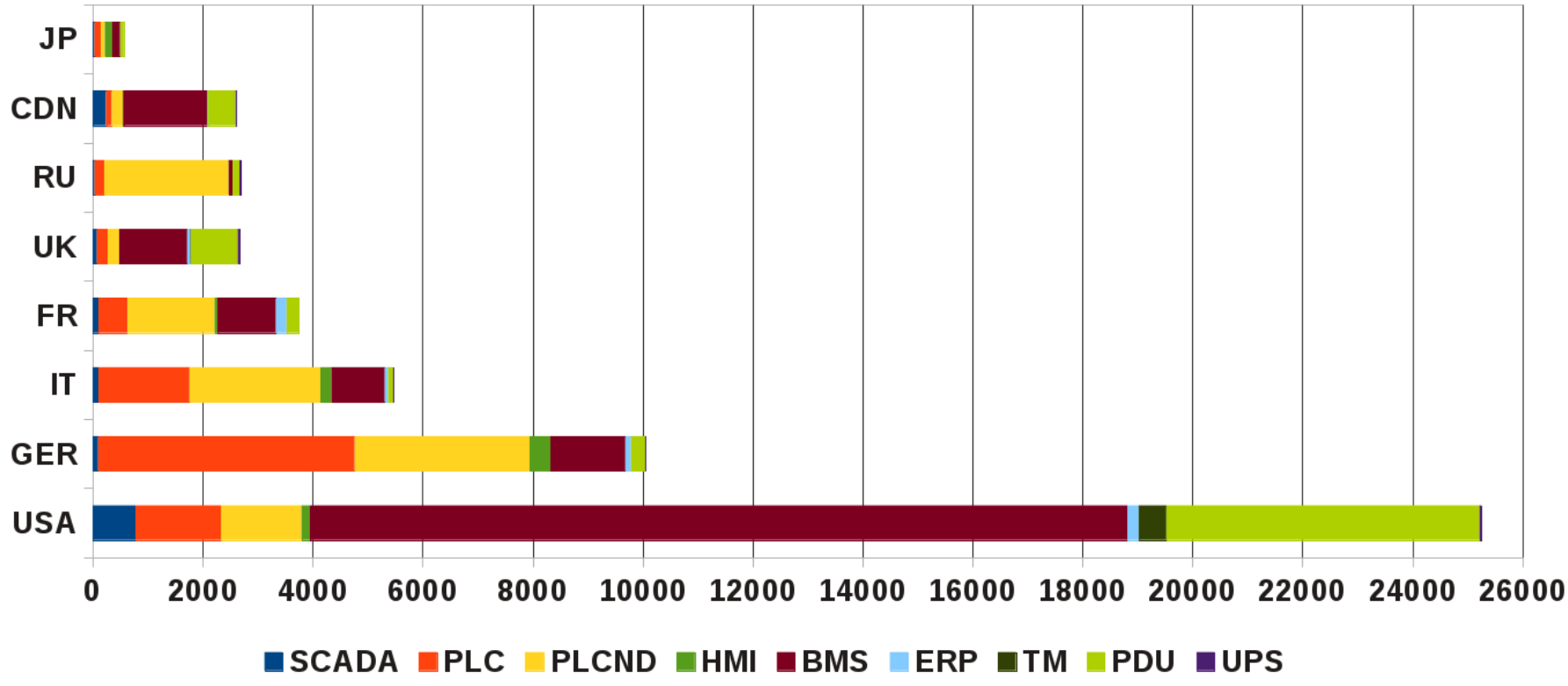


SCADACS

IRAM - Asien

SCADACS

Analyse



SCADACS

Analyse

Kategorien	Geräte	CVEs/Exploits
BMS	31411	9%
PLCND	23873	14%
PLC	14166	62%
PDU	10381	0%
SCADA	2711	28%
HMI	1735	41%
ERP	1400	0%
TM	768	0%
UPS	167	0%

IRAM - Demonstration (Video)

Video

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

Vielen Dank für Ihre Aufmerksamkeit!