

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



Volker Roth

Daniel Marzin

Robert Fehrmann

Jan-Ole Malchow

Sascha Zinke

Philipp Lämmel

Johannes Klick

Mateusz Khalil

Problemstellung

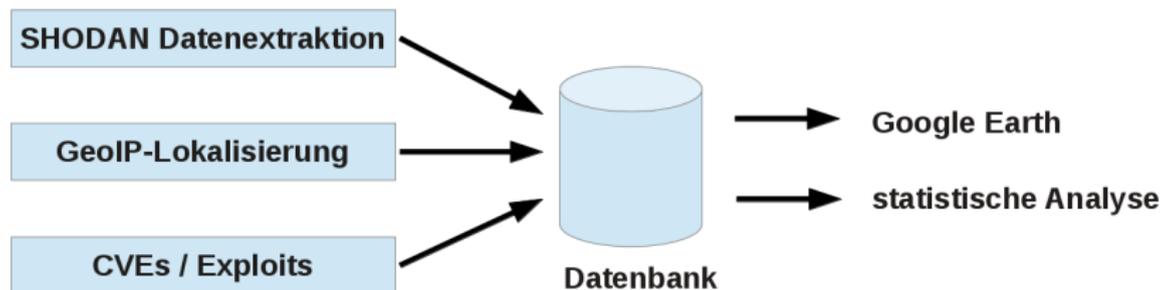
Steuerungen sind schlecht Geschützt gegen Angreifer

- ▶ 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



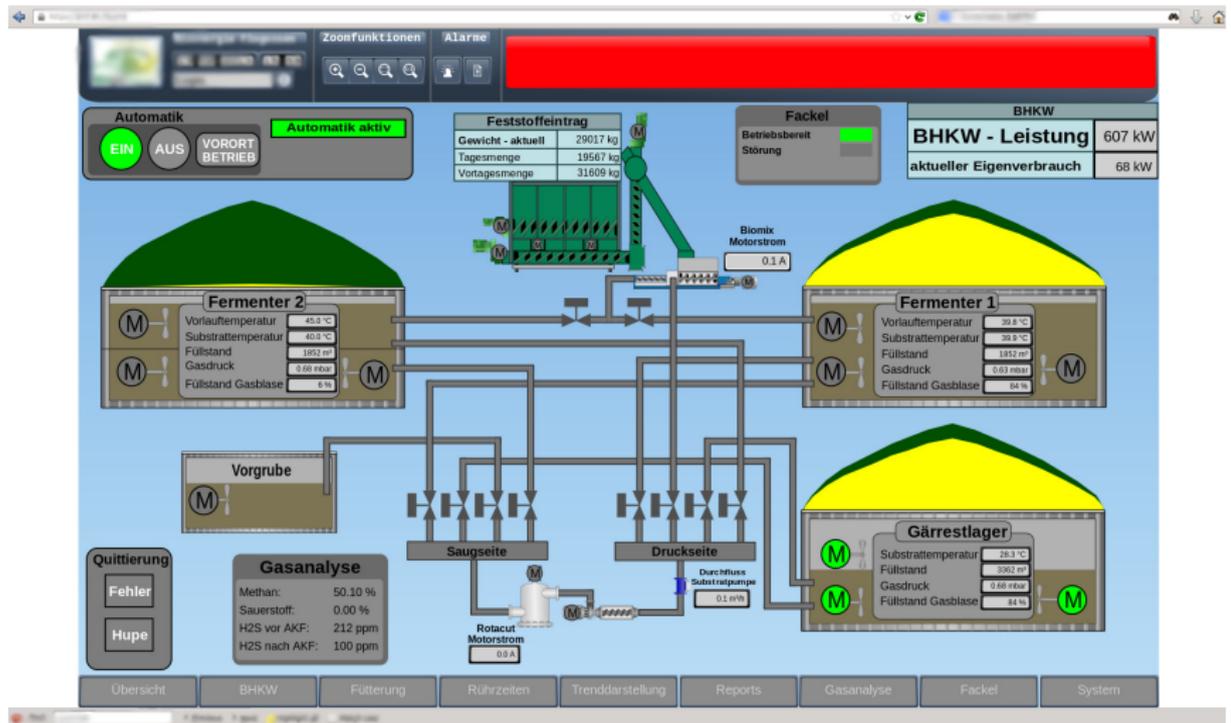
Methodik - SHODAN Funktionsweise

SHODAN ist eine spezielle Suchmaschine

- ▶ sucht im Internet nach Diensten wie SNMP, HTTP(S), Telnet etc.
- ▶ verbindet sich mit diesen Diensten und speichert bzw. fragt Identifikationsinformationen ab
- ▶ Verbindungsziele werden zufällig bestimmt
- ▶ findet Geräte im Internet, die WEB-Suchmaschinen wie Google nicht finden

Was für Steuerungen suchen wir im Internet?

SCADA Systeme



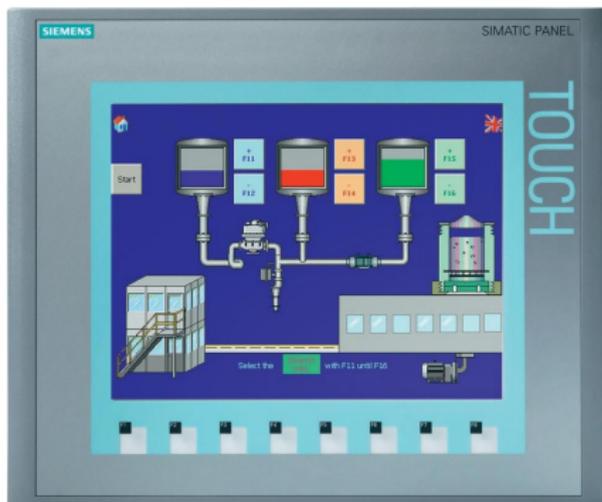
PLC - Programmable Logic Controller



PLC Network Devices (PLCND)



HMI - Human Machine Interfaces



BMS - Building Management Systems



PDU - Power Distribution Units



TM - Traffic Management Devices



ERP - Enterprise Resource Planning Systems

OpenERP Elico Corporation (demo)
Demo User
Employees Meetings

SALES PURCHASES WAREHOUSE MANUFACTURING PROJECT ACCOUNTING HUMAN RESOURCES MARKETING KNOWLEDGE TOOLS

Customer Invoices

Description: False

Save Save & Edit Cancel

Journal: Sales Journal Number: Currency: EUR (€) Change

Customer: Agrolait Invoice Address: Serge Lelitre, Belgium Wavre 69 rue d Invoice Date: Force Period: (keep empty to use the current period)

Invoice Other Info Payments

Account: 110200 Debtors Description:

Payment Term:

INVOICE LINE	DESCRIPTION	ACCOUNT	QUANTITY	UNIT OF MEASURE	UNIT PRICE	SUBTOTAL
[PC] Basic PC		200000 Product Sales	1.00	PCE	450.00	450.00

Taxes

TAX DESCRIPTION	TAX ACCOUNT	BASE	AMOUNT
ITAX S	111200 Tax Received	450.00	67.50

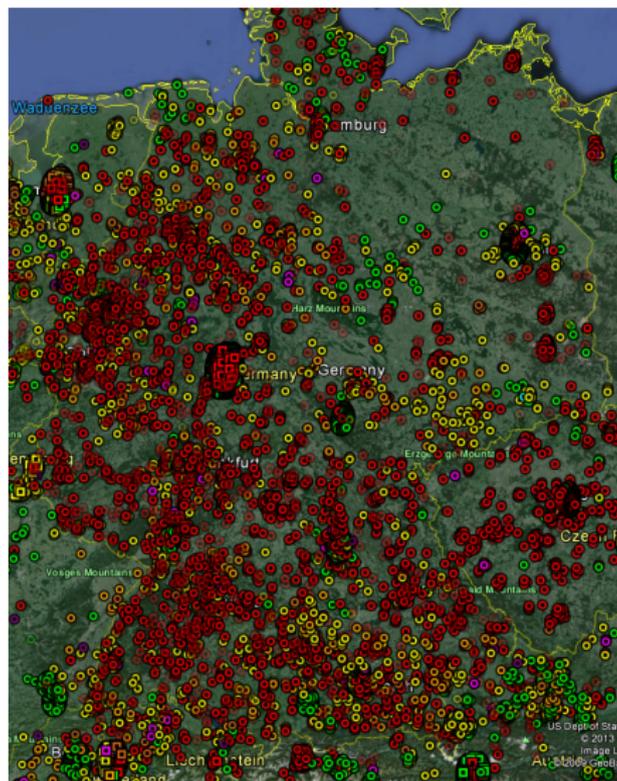
Compute Taxes Un taxed: 450.00
Tax: 67.50
Paid/Reconciled: Total: 517.50
State: Draft Residual: 0.00
Cancel PRO-FORMA Validate

Powered by openerp.com

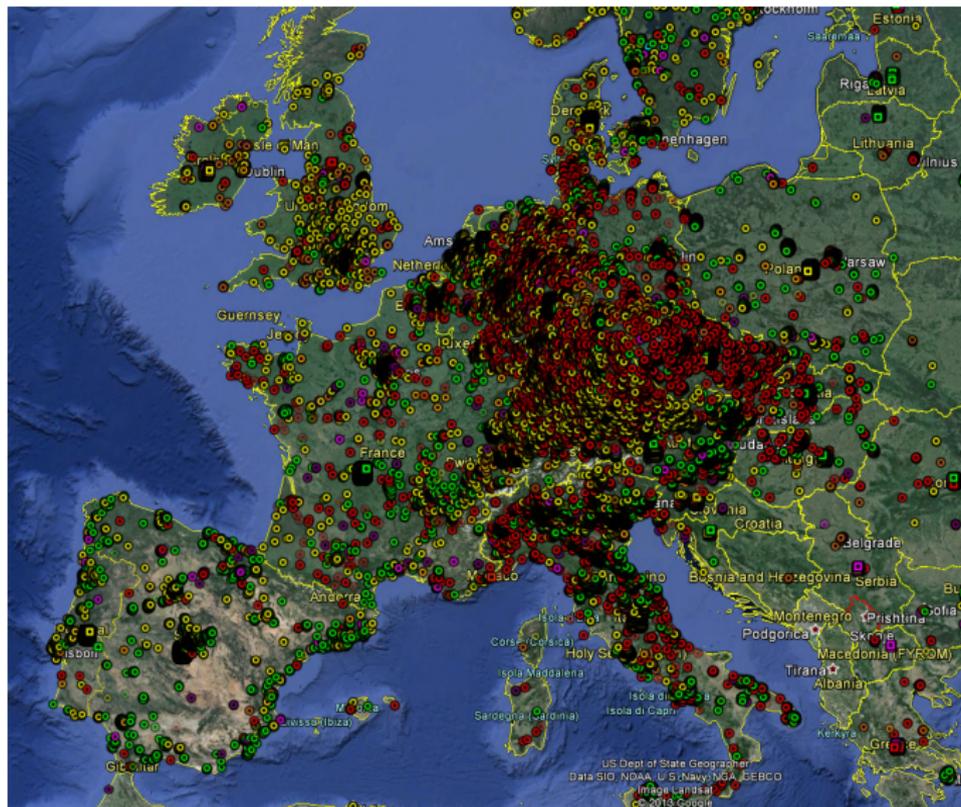
UPS - Uninterruptible Power Supplies



IRAM - Deutschland



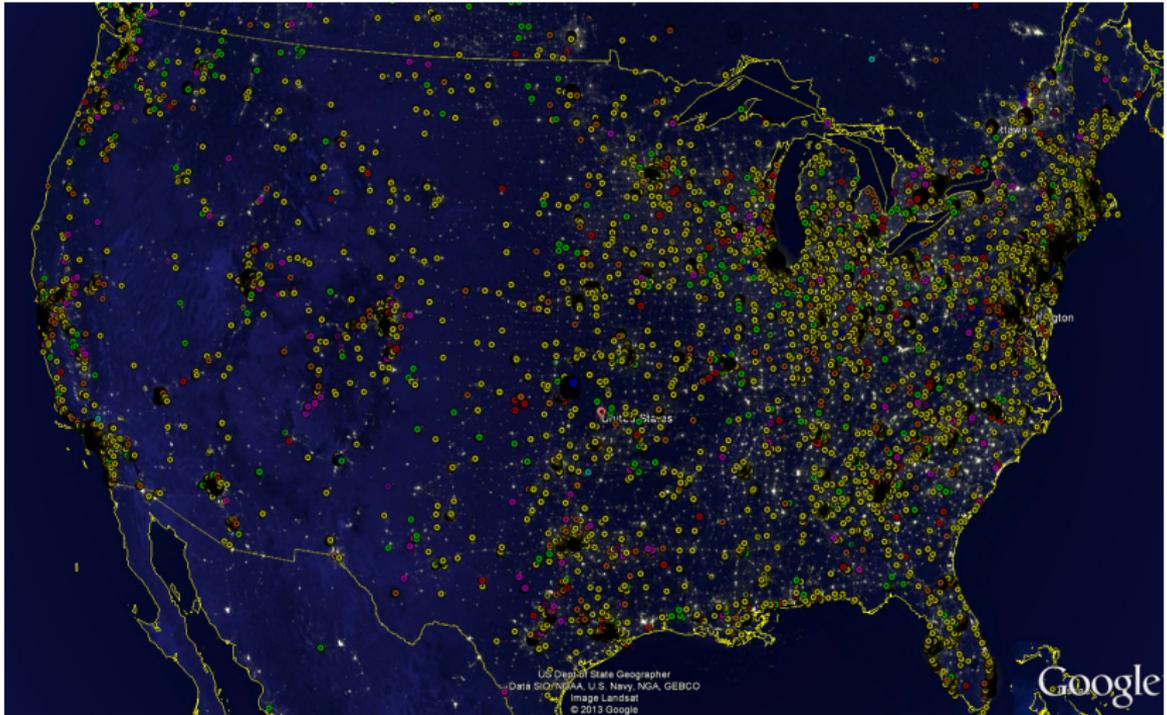
IRAM - Europa



IRAM - USA Nachtaufnahme ohne Steuerungen



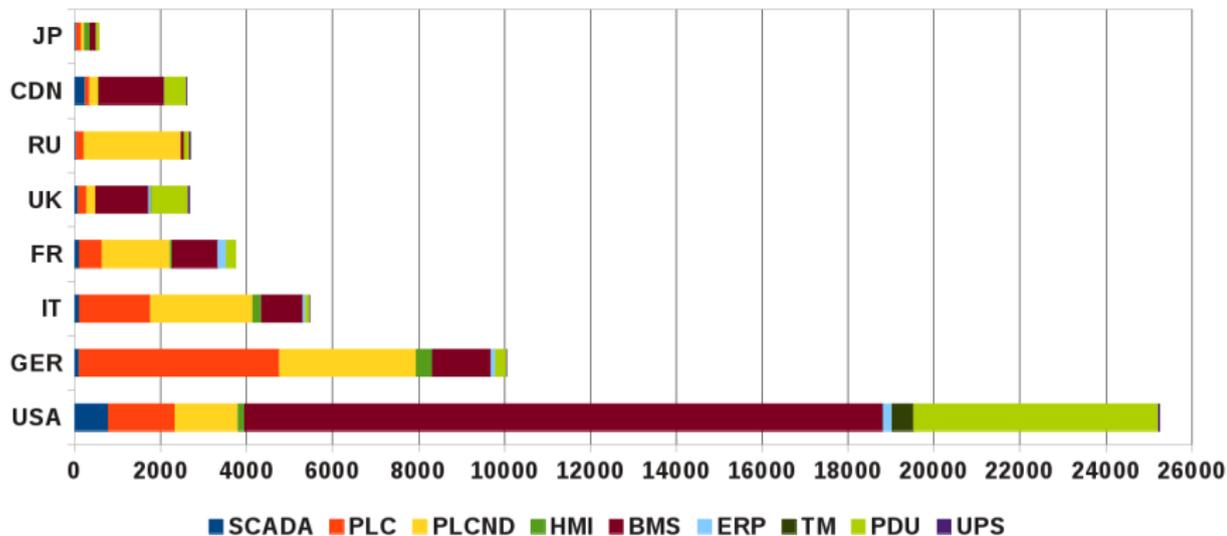
IRAM - USA Nachtaufnahme mit Steuerungen



IRAM - Asien



Analyse



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!