Erreichbarkeit von digitalen Steuergeräten Ein Lagebild

Jan-Ole Malchow, Johannes Klick
Freie Universität Berlin - Arbeitsgruppe Sichere Identität
Takustraße 9, 14195 Berlin
<vorname>.<nachname>@fu-berlin.de

Zusammenfassung

Digitale Steueranlagen sind fest in sämtlichen Produktions- und Steuerabläufen integriert. Durch Stuxnet wurde die Verwundbarkeit dieser Systeme einer breiten Masse bewusst gemacht. Es scheint Handlungsbedarf im Hinblick auf die Sicherheit der Steuerungssysteme zu bestehen. Bisher war jedoch nicht klar, ob tatsächlich ein großflächiges Problem besteht. Es war weitgehend unbekannt in welchem Maße direkte Angriffe möglich sind. Basierend auf Daten der Suchmaschine SHODAN ist mit der interaktiven *Industrial Risk Assessment Map (IRAM)* zum ersten Mal eine visuelles Lagebild verfügbar. Direkt über das Internet erreichbare Geräte werden auf einer Karte aufgetragen. Zusätzlich können bekannte Sicherheitslücken sowie Exploits für jedes Gerät angezeigt werden. Anhand bestimmter Selektionen können gezielt sowohl Regionen, als auch bestimmte Typen oder Hersteller dargestellt werden. Eine Evaluation der Daten hat eine gute Qualität im Hinblick auf die Verteilungsdichte ergeben.

1 Einleitung

Digitale Steueranlagen, im allgemeinen auch als SCADA bezeichnet, bilden das Rückgrat moderner Produktionsanlagen, Gebäudemanagementsystemen und der Steuerung kritischer Infrastrukturen. In zunehmendem Maße hält diese Art von Steuerung auch in privaten Haushalten Einzug. SCADA Systeme werden genutzt um Anlagen in Kraftwerken oder anderen Produktionsstätten zu steuern. SCADA Systeme bestehen aus drei wesentlichen Komponenten: Zentraler Leitstand (SCADA Center), Feldgeräte (PLC) sowie den angeschlossenen Sensoren und Aktuatoren [2].

Noch vor wenigen Jahren wurden diese Systeme in geschlossenen Umgebungen betrieben. Der Einsatz separater Bussysteme und spezifischer Programmiergeräte machte sie weitgehend sicher gegen Eingriffe von außen. Aus verschiedenen Gründen wurde diese Trennung jedoch

aufgegeben und eine Vernetzung auf Basis von Ethernet eingeführt. Neben großen Vorteilen machte dieser Technologiewechsel die Geräte jedoch auch angreifbar [5].

Diese Anlagen wurden nicht konzipiert, um über ein öffentlich zugängliches Netz erreichbar zu sein. Deshalb besitzen sie wenige oder gar keine Schutzmechanismen gegen unbefugten Zugriff oder Manipulation. Trotzdem werden diese Systeme häufig an das Internet angeschlossen.

Um das Ausmaß des Problems einschätzen zu können, wurde die *interaktive Industrial Risk Assessment Map (IRAM)* entwickelt. Auf einer interaktiven Karte stellt die IRAM farblich unterschieden dar, wo industrielle Systeme welchen Typs offen am Internet zu finden sind. Zu jedem dargestellten Kontrollgerät können bekannte Schwachstellen und Schadcode direkt angezeigt werden. Als Datenbasis für die *IRAM* dient die bekannte *SHODAN* Datenbank, sowie weitere öffentlich zugängliche Datenbanken.

Geographische Verortung, farblich unterschiedene Gerätetypen sowie die Einbeziehung des Alters eines Datensatzes machen *IRAM* zu einem wertvollen Werkzeug. Die Bedrohungslage kann schnell erfasst und eingeschätzt werden. Genauere Analysen werden durch den Einsatz graphischer Metaphern unterstützt.

Durch die Verortung der mit dem Internet verbundenen industriellen Kontrollsysteme auf einer Karte wird zum ersten mal deutlich, dass es sich auch um ein geographisch und international flächendeckendes Problem handelt.

Der Rest der Arbeit ist wie folgt gegliedert: Abschnitt 2 - Beschreibt den Ausgangspunkt des Projekts, Abschnitt 3 - Beschreibt das verwendete Material und die angewandten Methoden, Abschnitt 4 - Zeigt die Ergebnisse des Projekts, Abschnitt 5 - Erläutert die Evaluation der Ergebnisse, Abschnitt 6 - Zeigt zwei Fallstudien zur Verwendung von IRAM, Abschnitt 7 - Beschreibt verwandte Arbeiten, Abschnitt 8 - Nennt weiterführende Arbeiten, Abschnitt 9 - Fasst die Arbeit zusammen.

2 Problemstellung

Ziel des Projekts ist es zu erforschen in welchem Maße Steueranlagen bzw. SCADA Systeme tatsächlich mit dem Internet verbunden werden. Bisher war nicht klar, ob es sich tatsächlich um ein flächendeckendes, internationales Problem handelt. Dabei sollten die Ergebnisse möglichst intuitiv präsentiert werden.

Es mussten also zunächst die Datenquellen identifiziert und instrumentalisiert werden. Weiterhin musste eine einfache visuelle Repräsentation gefunden werden. Die erhaltenen Daten sollten nach Möglichkeit auf Plausibilität geprüft werden um Aussagen über die Genauigkeit des resultierenden Lagebildes zu ermöglichen.

3 Material und Methoden

Im Weiteren werden die verwendeten Materialien und angewandten Methoden beschrieben. Im Einzelnen sind dies die verwendeten Datenquellen, die Geolokalisierung, Methoden zur Klassifizierung von Geräten sowie die Datenaufbereitung.

3.1 Arbeitsregeln

Da in dieser Arbeit Steuergeräte ohne explizite Kenntnis der Betreiber untersucht wurden, mussten besonders strenge Verhaltensregeln angelegt werden.

1. Der direkte Zugriff auf Geräte ist nur im Ausnahmefall möglich. Sollten Zugriffe durchgeführt werden, ausschließlich mit Standard Browsern über das HTTP Protokoll.
2. Es wird unter keinen Umständen versucht einen Login durchzuführen.
3. Wird eine Manipulationsmöglichkeit erkannt wird die Verbindung sofort beendet.
4. Es werden ausschließlich öffentlich zugängliche Datenquellen genutzt.
5. Gewonnene Daten werden dem BSI kommuniziert.

3.2 Hauptdatenquelle

Als Hauptdatenquelle kommt SHODAN zum Einsatz, dessen Methodik in 7.1 SHODAN genauer beschrieben wird. SHODAN stellt eine API zur Verfügung, mit deren Hilfe die Suchergebnisse extrahiert werden können. Die von SHODAN heruntergeladenen Suchergebnisse werden anschließend mit dem jeweiligen Suchbegriff in eine Datenbank eingepflegt. Die verwendeten Suchbegriffe werden in der Regel durch eine manuelle Recherche gefunden. Es wurden zwei Arten von Recherchen durchgeführt. Zum einen wurde nach Listen von bestehenden SHODAN Suchbegriffen für Kontrollsysteme im Internet gesucht. Zum Anderen wurden Hersteller und Produktnamen solcher Systeme recherchiert um diese anschließend in SHODAN einzugeben. Denn nicht selten identifizieren sich diese Produkte mittels ihres Produkt- oder Herstellernamens selbst. Zurzeit umfasst die Liste 123 Suchbegriffe.

3.3 Weitere Datenquellen

Um weitere Informationen zwecks Bedrohungsanalyse über die gefunden Steuerungen zu erhalten, sind die Steuerungsdaten mit Schwachstellen- und Exploit-Datenbanken verknüpft. Damit IRAM stets über aktuelle Datenbanken verfügt, werden diese nicht offline gespeichert, sondern nachfrageinduziert online abgerufen.

Zusätzlich werden noch weitere Dienste angeboten, welche es ermöglichen mehr Informationen über den Inhaber der IP oder die Internet-Konnektivität der Steuerung zu ermitteln. Folgende Dienste werden über Web-Proxy-Services zur Verfügung gestellt:

- Ping
- Traceroute
- Whois
- Reverse DNS

3.4 Geolokalisierung

Für die Geolokalisierung anhand der IP der Kontrollgeräte wird die frei verfügbare GeoIP-Datenbank *GeoIP light* der MaxMind , Inc. genutzt. Gemäß der von Maxmind zur Verfügung gestellten Informationen besitzt die verwendete GeoIP-Datenbank eine Genauigkeit von über 99% auf Länderebene.

3.5 Klassifizierung

Zwecks Visualisierung werden die gefundenen Kontrollgeräte in folgende Kategorien unterteilt und farblich gekennzeichnet:

- PLC (Rot): Als *Programmable Logic Controller* werden Geräte identifiziert, die zur Steuerung oder Regelung einer Maschine eingesetzt werden.
- PLCND (Grün): *PLC Network Devices* sind Netzwerkkomponenten oder Module, welche PLCs mit dem Netzwerk verbinden.
- SCADA (Pink): Als *SCADA* sind alle Systeme die zum Steuern und Überwachen von technischen Prozessen dienen kategorisiert.
- HMI (Orange): *Human Machine Interfaces* sind Geräte, die eine Interaktion zwischen Mensch und Maschine ermöglichen.
- UPS (Hellblau): *Uninterruptable Power Supplies* sorgen für eine unterbrechungsfreie Stromversorgung im Falle eines Stromausfalls.
- PDU (Braun): *Power Distribution Units* sind eletrisch schaltbare Mehrfachsteckdosen, die ferngesteuert werden können.
- BMS (Gelb): *Building Management Systems* dienen der Gebäudeautomatisierung und steuern Klimaanlagen bis hin zu Schließanlagen.
- ERP (Lila): *Enterprise Rescource Planning* Software dient zur Planung und Steuerung von Geschäftsprozessen von Unternehmen.
- TM (Blau): Die Kategorie *Traffic Management* beschreibt alle Systeme, die zur Steuerung und Überwachung des Straßenverkehrs dienen.

3.6 Datenaufbereitung

Die in der Datenbank gespeicherten Kontrollgeräte inklusive der bereits verknüpften Daten, werden extrahiert und in das KML-Format überführt. KML steht für *Keyhole Markup Language* und ist ein Standart des *Open Geospatial Consortiums*, der für die Beschreibung von Geo-Daten dient. Wenn sich mehrere Geräte am selbem Ort befinden, würden sich diese auf einer Karte überlagern, wodurch aus der Sicht des Betrachters Information verloren gehen würden. Aus diesem Grund werden Geräte mit gleichen Geo-Positionen in größer werdenden Ovalen rearrangiert. Wobei der Mittelpunkt der Ovale die eigentliche Position der Geräte darstellt. Der i-te Oval enthält 2^i Geräte.

Geräte können unterschiedlich genau verortet werden. Geräte in einem Umkreis von 40 km um den tatsächlichen Standort (Stadt genau), werden mit einen farblich ausgefüllten runden Kreis

dargestellt. Geräte mit ungenauerer geografischer Auflösung, werden mit einem farblichen ausgefüllten Rechteck visualisiert.

Da SHODAN seit 2010 kontinuierlich das Internet durchsucht, werden folglich die Geräte zu unterschiedlichen Zeitpunkten gefunden. Da es für eine Bedrohungsanalyse relevant ist, wie groß der Zeitraum ist seitdem das Gerät gefunden wurde, wird das Alter des jeweilgen Datums durch verschiedene Transparenzlevel codiert. Als Intervall für eine Transparenzstufe wurde ein Jahr gewählt. Dies bedeutet, dass Geräte die ohne eine Transparenzstufe dargestellt werden weniger als ein Jahr alt sind.

4 Ergebnisse

Als Ergebnis des Projekts sind eine Reihe von Werkzeugen entstanden, mit deren Hilfe die IRAM erstellt wird. Zusätzlich zur visuellen Aufbereitung der Daten werden noch eine Reihe von Kennzahlen erhoben.

4.1 Karte und Werkzeuge

Die IRAM ist als Werkzeug zur Aggregation und visuellen Aufbereitung verschiedener Datenquellen designed. Als Basis zur Visualisierung kommt die frei verfügbare Version von *Google Earth* zum Einsatz. Auf Kartenebene werden gefundene Geräte als Punkte dargestellt. Farbliche Kennzeichnung und Transparenz kodieren bereits Informationen über Type der Anlage und Alter des Datensatzes. Abbildung 4a und Abbildung 4b zeigen beispielhaft alle gefundenen und nur die Verwundbaren Geräte in Europa. Durch das Anklicken einzelner Datenpunkte öffnet sich ein User-Interface, welches es dem Nutzer ermöglicht weitere Informationen über das ausgewählte Gerät zu erhalten. Direkt angezeigt werden die Anzahl bekannter Verwundbarkeiten und verfügbarer Exploits.

Im erweiterten User-Interface werden weitere Datenquellen zusammengefasst. Die Integration der Datenquellen ist hierbei jeweils durch eine lose Kopplung realisiert. Dadurch können Datenquellen leicht ausgetauscht oder hinzugefügt werden. Zudem können bestimmte Informationsdienste strategisch im Netz platziert werden und sind nicht vom Analyse Sytem Abhängig.

Basis Informationen im erweiterten User-Interface sind neben einem Bild der Anlage auch das exakte Datum der Entdeckung und die IP-Adresse sowie der Port über die Anlage erreichbar war. Zusätzlich werden Optionen angeboten, sich mit freien Web-Proxy-Services über den integriereten Browser zu verbinden. Diese Web-Proxy-Services ermöglichen es das Gerät zu Pingen, einen Traceroute zu erstellen, sich den Whois-Eintrag anzuschauen und eine reverse DNS-Lookup Anfrage zu stellen. Es können auch gerätespezifische Einträge über Schwachstellen und vorhandene Exploits direkt angezeigt werden. Zusätzlich können Informationen über das Umfeld der Anlage, wie Informationen über die nächstgelegene Stadt oder das aktuelle Wetter abgerufen werden. Die Informationen zum aktuellen Wetter am Standort einer Anlage wurden eingebunden um die mögliche Vielfalt verknüpfter Daten deutlich zu machen.

Um Bedrohungsanalysen für bestimmte Regionen oder Gerätetypen erstellen zu können, bietet *IRAM* die Möglichkeit, nur bestimmte Länder, Gerätekategorien oder Hersteller anzeigen zu

lassen. Abbildung 2 zeigt beispielhaft die Selektion nach bestimmten Kategorien. Zusätzlich sind beliebige manuelle Filter zum Beispiel zur Selektion aller IP-Adressen in einem Autonomen Systems möglich.

4.2 Kennzahlen

Zusätzlich zur visuellen Aufbereitung ermöglicht die vorliegende Datenbasis Kennzahlen zu bestimmen. Anhand dieser Zahlen ist ein Vergleich möglich, welcher mit dem Auge anhand der Visualisierung nicht möglich ist.

Mit Stand 28.08.2013 verfügt das Projekt über 86.181 kategorisierte und verortete Einträge. Für 16.280 Geräte der gefundenen Typen sind CVEs bekannt oder konkrete Exploits verfügbar. Eine Besonderheit stellt dabei das Produkt eines bestimmten deutschen Herstellers dar. In den Daten befinden sich 6.912 Geräte dieses Herstellers. Im Weiteren werden diese daten nicht berücksichtigt, weitere Details können an dieser Stelle noch nicht veröffentlicht werden.

Es verbleiben 79.269 kategorisierte und verortete Einträge mit 9.368 Geräte für deren Typ CVEs oder Exploits verfügbar sind. Tabelle 1 zeigt die Kategorien mit der Gesamtsumme der jeweils gefundenen Geräte. Zusätzlich weißt die Tabelle den relativen Anteil der Geräte je Kategorie für die *Common Vulnerabilities and Exposures (CVE)* oder *Exploits* existieren aus. Da nur in einigen Fällen anhand der SHODAN Daten die Firmware Version ermittelt werden kann, ist es möglich, dass einige gefundene Schwachstellen nicht mehr aktuell sind. Dennoch ist der hohe Anteil von bedrohten Geräten in den Kategorien PLC, SCADA und HMI auffällig. Da der auf den Geräten projektierten Code nicht heruntergeladen wurde, ist es nicht möglich genaue Aussagen über physische Umgebung des Gerätes zu treffen. Jedoch konnten anhand der IPs und Whois-Abfragen einige Geräte kritischen Infrastrukturen (gemäß [3]) zugeordnet werden.

Tabelle 1: 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%

Abbildung 3 zeigt die Verteilung von Steuerungssystemen, aufgeteilt nach Kategorie und Nation für die *Gruppe der Acht - G8*, welche für mehr als zwei Drittel des weltweiten Bruttoinlandsprodukts verantwortlich sind. Es zeigt sich, dass in den USA, Deutschland und Italien die meisten Steuerungen gefunden worden sind. Wobei in den USA *Building Management Systeme*

und *Power Distribution Units* den Großteil der Systeme ausmachen. Für Deutschland, Frankreich und Italien lässt sich ein überproportionaler Anteil von *PLCs* und *PLC Network Devices* erkennen.

5 Evaluation

Um die Verlässlichkeit der erhobenen Daten zu ermitteln, wurden diese anhand bestimmter Kriterien während des Projekts laufend evaluiert. Die Hypothese war, dass es eine Korrelation zwischen wirtschaftlicher Stärke einer Region und der Anzahl von digitalen Steueranlagen gibt.

Als Kriterium für die wirtschaftliche Stärke wurde das Bruttoinlandsprodukt sowie die Lichtstärke bei Nacht herangezogen. Die Hypothese wurde zunächst visuell überprüft. Für die deutschen Bundesländer und die Staaten der USA wurde außerdem der Korrelationskoeffizient bestimmt. Sowohl die visuelle als auch die mathematische Prüfung haben den Zusammenhang zwischen Anzahl gefundener Steuergeräte und wirtschaftlicher Stärke bestätigt. Das heißt die Dichte der gefundenen Geräte gibt ein realistisches Lagebild wieder. Ob die Gesamtzahl der gefunden Geräte korrekt ist kann jedoch nicht festgestellt werden.

5.1 Visuelle Evaluation

Abbildung 4a zeigt die Verteilung der Steuerungen in Europa. Abbildung 2 zeigt die Verteilung für verschiedene Typen von Steueranlagen. Es ist zu erkennen, dass es eine Korrelation zwischen wirtschaftlich starken Regionen und einer Häufung von Steuerungen gibt. Sichtbar wird dieses zum Beispiel innerhalb Deutschlands. So befinden sich in den wirtschaftlich schwächeren Gebieten weniger Systeme, als in den wirtschaftlich stärkeren. In Italien ist ebenfalls solch eine Korrelation erkennbar. Der Unterschied der Anhäufungen von Kontrollgeräten zwischen dem wirtschaftsstarken Norden und dem wirtschaftsschwächeren Süden Italiens ist gut zu erkennen. Ähnlich verhält es sich auch für Süd-England und die Küstenregionen Spaniens.

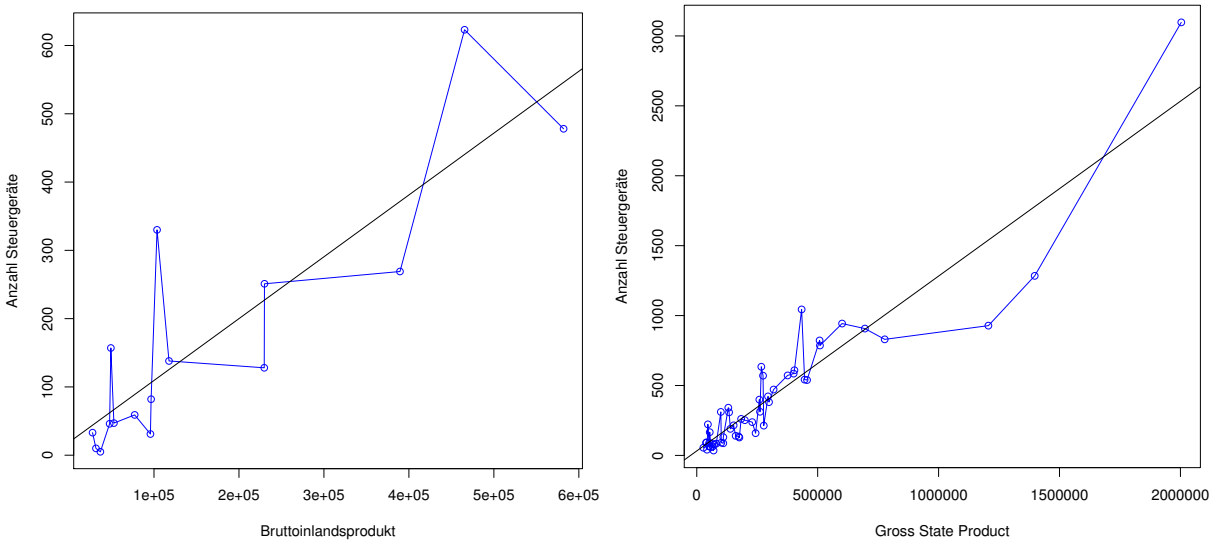
Als weiterer Indikator wurde ein Vergleich mit Nachtaufnahmen der NASA [12] herangezogen. Abbildung 5a zeigt eine Nachtaufnahme der USA. Die Nachtaufnahme zeigt deutliche Häufungen von Licht in den Ballungszentren, wie z.B. an der Nord-Ostküste. Abbildung 5b zeigt die gefundenen Steuerungen, welche auf die NASA-Karte projiziert wurden. Es zeigt sich, dass alle Ballungszentren auch ein hohes Vorkommen von Geräten aufweisen.

5.2 Korrelation in Deutschland

In der visuellen Evaluation ist deutlich geworden, dass es in Deutschland einen Zusammenhang zwischen wirtschaftlicher Stärke einer Region und Anzahl der Steuergeräte gibt. Dieser Zusammenhang wurde auch mathematisch als Koeffizient zwischen dem Bruttoinlandsprodukt eines Bundeslandes und der Anzahl der Steuergeräte überprüft. Abbildung 1a zeigt die Korrelation der Werte. Sowohl die Pearson-Korrelation ($cor = 0,86, p = 1,911 \cdot 10^{-5}$), als auch Spearmans Rho ($\rho = 0,84, p = 1,932 \cdot 10^{-5}$) bestätigen den höchst signifikanten Zusammenhang.

5.3 Korrelation in den USA

Auch für die USA hat die visuelle evaluation einen Zusammenhang zwischen wirtschaftlicher Stärke und Anzahl der Steuergeräte ergeben. Dieser Zusammenhang wurde zusätzlich mathematisch überprüft (Abbildung 1b). Es konnte auch in diesem Fall ein höchst signifikanter Zusammenhang gefunden werden (Pearson-Korrelation $cor = 0,93, p = 2,2 \cdot 10^{-16}$, Spearmans Rho $\rho = 0,89, p = 2.2 \cdot 10^{-16}$). Abbildung 1b zeigt die Korrelation der Daten.



(a) Zusammenhang zwischen Bruttoinlandsprodukt der deutschen Bundesländer im Jahr 2012 (in Millionen Euro) [1] und Anzahl der Steuergeräte

(b) Zusammenhang zwischen Gross State Product der US Staaten im Jahr 2012 (in Millionen US Dollar) [4] und Anzahl der Steuergeräte

Abbildung 1: Korrelation zwischen Anzahl gefundener Steueranlagen und wirtschaftlichen Kennzahlen für die BRD und USA.

5.4 Sonderfall Asien

Eine Betrachtung des asiatischen Raums zeigt, dass dort nur sehr wenige Geräte gefunden worden sind (Abbildung 6). Die weitere Untersuchung der Daten hat ergeben, dass die Daten durch eine lokale Verbreitung von Produkten beeinflusst sind. So werden in den Vereinigten Staaten von Amerika mehr Steuerungen eingesetzt, die von den USA selbst produziert worden sind. Dieses Verhalten konnte auch im besonderen Maße in Deutschland feststellt werden. Die in anderen Teilen der Welt beobachtete Häufung bestimmter Produkte legt nahe, dass dies auch im Asiatischen Raum der Fall ist. Durch die starke sprachliche Barriere werden die Recherchearbeiten nach asiatischen Hersteller stark erschwert. Aus diesem Grund werden bisher nur sehr wenige Produkte aus dem asiatischen Raum berücksichtigt.

6 Fallstudien

Im folgenden wird anhand von zwei Fallstudien gezeigt, wie eine Analyse ablaufen kann. Im ersten Fall wird gezeigt, wie IRAM verwendet werden kann um Anlagen des Herstellers Saia-

Burgess zu finden. Über diesen Type wurde bereits eingehend von *heise Security* berichtet. Im zweiten Fall wird die Analyse eines autonomen Systems hinsichtlich erreichbarer Steuergeräte gezeigt.

6.1 Analyse Saia-Burgess

Im Frühjahr und Sommer 2013 hat *heise Security* wiederholt über Sicherheitslücken in Industriesteuerungen der Firma Saia-Burgess [13], [10] berichtet. Diese Regler kommen unter Anderem auch in Heizungen der Firma Vaillant zum Einsatz [14]. In den verschiedenen Berichten werden verschiedene Zahlen hinsichtlich betroffener Geräte genannt. Laut Angabe des Herstellers sind 200.000 Geräte [10] weltweit im Feld. Vaillant spricht von 1.500 Betroffenen Kunden [10] in Deutschland. Offen sind bisher die Fragen, wie sich diese Zahlen zu den Daten von SHODAN verhalten und wo sich die betroffenen Anlagen befinden.

6.1.1 Kennzahlen

Im vorliegenden Auszug der SHODAN Datenbank konnten 2897 Geräte dieses Typs identifiziert werden. Tabelle 2 weißt die Verteilung in verschiedenen Ländern aus. Die Daten wurden im Zeitraum zwischen dem 01.05.2013 und dem 19.08.2013 erfasst. Es sind also 859 Anlagen in Deutschland auffindbar, welche einem direkten Risiko ausgesetzt waren.

Tabelle 2: Verteilung von Geräten des Herstellers Saia-Burgess. Aufgelistet sind 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
Rest	170

6.1.2 Verortung

Aus der Berichterstattung war nicht zu entnehmen wie sich die Anlagen in Deutschland verteilen. So stellt sich zum Beispiel die Frage ob eine Stadt oder Region besonders stark betroffen ist. Durch die IRAM ist es möglich schnell einen Eindruck von der konkreten Lage zu gewinnen.

Abbildung 7 zeigt die Verteilung der Geräte in Deutschland und den angrenzenden Ländern. Auch in diesem Fall ist die Relation zur Besiedlungsdichte deutlich zu erkennen.

In einem weiteren Artikel berichtete *heise* über den Fall einer Kirche mit einer betroffenen Anlage [11]. Dies gibt uns die Chance unsere Verortung direkt einem konkreten Standort zu zuordnen. Abbildung 8 zeigt unsere Verortung am oberen linken Rand der Stadt, während sich die eigentliche Kirche in der Stadtmitte befindet. Die Abweichung beträgt in diesem Fall weniger als zwei Kilometer.

6.1.3 Diskussion

Die Zahl gefundener Anlagen in Deutschland ist etwa halb so groß, wie die von Vaillant genannte Zahl von 1.500 betroffenen Kunden. Dies kann unter anderem daran liegen, dass im betrachteten Zeitraum die Warnung öffentlich wurde und viele Anlagen daher bereits nicht mehr am Netz waren. Es bleibt jedoch festzuhalten, dass 50% der im Feld befindlichen Geräte direkt angreifbar waren.

Es ist jedoch positiv zu bewerten, dass die Gesamtzahl gefundener Anlagen weltweit deutlich unter dem vom Hersteller genannten Maximum von 200.000 Geräten [10] bleibt. Es sind also 1% der im Feld befindlichen Geräte im Internet auffindbar. Fraglich ist nun, ob sich dieser Wert auf andere Hersteller übertragen lässt.

6.2 Analyse ASN680 (DFN)

Das autonome System (AS) 680 wird vom DFN Verein zur Foerderung eines Deutschen Forschungsnetzes e.V. betrieben und bildet das Rückrad der Vernetzung deutscher Hochschulen. Die einem AS zugeordneten Netzwerk Prefixe sind öffentlich bekannt. Aus diesen Netzbereichen werden alle möglichen IP Adressen generiert und gegen die Datenbasis geprüft. Insgesamt konnten so 132 erreichbare Geräte identifiziert werden. Tabelle 3 schlüsselt die gefundenen Geräte pro Kategorie auf.

Tabelle 3: 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

6.2.1 Verortung

Abbildung 9 zeigt die Verteilung der gefundenen Geräte. Es wird sofort deutlich, dass Hochschulen im gesamten Bundesgebiet betroffen sind. Anhand der IP Adressen kann die jeweilige Hochschule identifiziert werden. In allen Fällen zeigt die Verortung zumindest die korrekte Stadt an. Die genaue Lage in den Gebäuden kann zurzeit nicht bestimmt werden.

6.2.2 Diskussion

Betroffene Hochschulen können anhand der verwendeten IP Adressen leicht identifiziert werden. Trotzdem bietet die IRAM durch die schnelle Erfassbarkeit einen Mehrwert. Insbesondere die direkte Einbeziehung verfügbarer Exploits erlaubt eine Priorisierung des Handlungsbedarfs.

Die Zahl der gefundenen Geräte ist im Hinblick auf die Größe des untersuchten Netzwerks erfreulich niedrig. Bisher ist nicht klar bei wie vielen Anlagen es sich um Honeypots zur Forschungszwecken handelt. Wir gehen jedoch davon aus, dass sich einige in den Daten wiederfinden.

7 Verwandte Arbeiten

Im Folgenden werden Arbeiten und Projekte welche einen Bezug zur vorliegenden Arbeit haben vorgestellt. Die Projekte werden kurz beschrieben und die Unterschiede zu IRAM heraus gestellt.

7.1 SHODAN

SHODAN ist eine Suchmaschine, die nach Geräten sucht, welche mit dem Internet verbunden sind. Die SHODAN Search Engine wählt zufällig eine IPv4 Adresse und versucht eine Verbindung zu 33 definierten Ports aufzubauen [15] . Dies sind unter anderem:

- 21 FTP
- 22 SSH
- 23 Telnet
- 80 (443)HTTP(S)
- 137 NetBIOS
- 161 SNMP

Die genaue Funktionsweise von SHODAN ist nicht öffentlich dokumentiert. Es ist nicht bekannt ob bestimmte IPv4 Adressbereiche ausgeschlossen werden. Ebenso kann nicht sicher gesagt werden, dass SHODAN alle gefundenen Banner tatsächlich suchbar macht.

Kommt eine Verbindung zustande speichert SHODAN den vom Server übermittelten Banner. Diese Banner werden indiziert und können vom Nutzer durchsucht werden. Da viele Geräte Informationen wie Hersteller, Typ oder Seriennummer im Header übermitteln können sie

leicht identifiziert werden. Die Voraussetzung ist jedoch die genaue Kenntnis von im Header enthaltenen Strings. Daher besitzt SHODAN zwar die notwendige Datenbasis, ohne die für IRAM verwendeten Suchstrings sind die Daten jedoch nicht nutzbar.

Erhält SHODAN eine Antwort von einer IP, für welche bereits ein Eintrag vorhanden ist wird dieser aktualisiert. Aufgrund des teilweise großen Alters der Einträge kann auf eine lange Suchperiode geschlossen werden. Daher muss bei der Verwendung von SHODAN stets berücksichtigt werden, dass es sich nicht um ein Lagebild zum jetzigen Zeitpunkt handelt.

Die Existenz von SHODAN führte zu einem Sicherheitshinweis des US-Amerikanischen ICS-CERT. Dieser warnte Betreiber und Eigentümer von industriellen Kontrollanlagen vor den möglichen Konsequenzen von SHODAN, da das Finden solcher Geräte durch SHODAN stark vereinfacht wurde [7].

7.2 Master Thesis - Eireann P. Leverette

Die Masterarbeit *Quantitatively Assessing and Visualising Industrial System Attack Surfaces* [9] ist eine der ersten akademischen Forschungsarbeiten, die sich mit dem Auffinden von industriellen Kontrollsystemen und anderen Steuerungseinheiten im Internet beschäftigt. Mithilfe der Suchmaschine SHODAN und definierter Suchtags ermittelte der Autor 7.500 SHODAN-Einträge für Kontrollgeräte weltweit. Die IP-Adresse der ermittelten Geräte wurden anschließend mittels GoogleMaps visualisiert. Zusätzlich wurden die Geräte mit Exploit-Datenbanken verknüpft, so dass auf der Karte farblich visualisiert wurde ob für ein Gerät möglicherweise ein Exploit vorliegt.

Diese Arbeit war für uns richtungsweisend und IRAM implementiert einen Teil der in der Arbeit vorgeschlagenen Erweiterungen: a) Durch intensive Recherche verwendet IRAM deutlich mehr Banner b) Die direkte Integration von Netzwerktools wie WHOIS und Traceroute ermöglichen eine bessere Identifikation des Betreibers c) Eine verbesserte GeoIP Lokalisierung ermöglicht ein genaueres Bild. Im Hinblick auf visualisierte und zusätzliche Informationen geht IRAM deutlich über die Arbeit von Leverette hinaus.

7.3 Project SHINE / US ICS-CERT

Das Project SHINE (SHODAN INtelligent Extraction) von InfraCritical konzentriert sich seit April 2012 auf die Suche von SCADA Systemen im Internet mithilfe der Suchmaschine SHODAN. Bis Oktober 2012 haben die Betreiber von Project SHINE über 460.000 solcher Kontrollgeräte gefunden. Die gesammelten Daten wurden anschließend dem *US ICS-CERT* übergeben. Das ICS-CERT hat die IP Adressen 98.000 Organisationen in den USA zuordnen können. Anschließend hat eine genauere Analyse der Daten gezeigt, dass 7.200 [8] dieser Geräte einen direkten Bezug zu Kontrollsystemen haben. Eine Nachfrage im Mai ergab, dass ihre Datenbank auf über 800.000 Einträge gewachsen ist.

Im Gegensatz zu IRAM hat Project SHINE weder eine Visualisierung noch werden erweiterte Informationen integriert.

8 Weiterführende Arbeiten

Das Projekt ist noch nicht beendet und wird kontinuierlich weiter entwickelt. Dabei steht zurzeit die Visualisierung im Vordergrund, welche neben besserer Skalierbarkeit erweiterte Möglichkeiten zur Interaktion erhalten soll.

Für die vorliegende Arbeit werden ausschließlich Daten von SHODAN verwendet. Die Qualität konnte zwar positiv evaluiert werden, letztlich sind die Daten jedoch eingeschränkt. So unterstützt SHODAN beispielsweise keine spezifischen Protokolle wie Modbus oder DNP3. Daher wäre die Erhebung eigener Daten wünschenswert, ist aber aufgrund unklarer rechtlicher Aspekte bisher schwierig.

Zusätzlich wäre eine weitere Verbesserung der GeoIP Lokalisierung wünschenswert. Aktuelle Forschungsarbeiten sind im Hinblick auf Aktualität und Abdeckung sehr vielversprechend [6].

9 Zusammenfassung

Stuxnet bildet das Epizentrum für die allgegenwärtige Einsicht, dass heute Steuerungssysteme direkt verwundbar sind. Eine aktuelle Studie von TrendMicro [16] zeigt, dass Industriesteuerungen bereits aktiv angegriffen werden. Das Problem beschränkt sich also nicht nur auf ausgewählte und besonders relevante Ziele. Es war bisher jedoch nicht klar und insbesondere nicht intuitiv erfassbar, wie groß das Risiko tatsächlich ist. Mit IRAM konnte gezeigt werden, dass Steuerungssysteme weltweit und flächendeckend mit dem Internet verbunden sind. Dieser Zustand ist für alle Arten von Systemen zu beobachten, wenn gleich Gebäudesteuerungen bereits heute den größten Teil ausmachen. Für viele erreichbare Geräte sind zumindest Verwundbarkeiten bekannt.

Es muss also allen Beteiligten und Verantwortlichen klar werden, dass ein massives Problem vorliegt. Die tatsächlichen Auswirkungen verschiedener Angriffsszenarien sind bisher vollkommen unklar. Mit den durch IRAM neu geschaffenen Möglichkeiten kann nun mit der bisher als fehlend beklagten Bestandsaufnahme begonnen werden.

Literatur

[1] ARBEITSKREIS VOLKSWIRTSCHAFTLICHE GESAMTRECHNUNGEN DER LÄNDER: *Bruttoinlandsprodukt in jeweiligen Preisen 1991 bis 2012*. Technischer Bericht, Statistische Ämter des Bundes und der Länder, März 2013.

[2] BARR, DALE: *TECHNICAL INFORMATION BULLETIN 04-1,Supervisory Control and Data, Acquisition (SCADA) Systems*. Technischer Bericht, U.S. NATIONAL COMMUNICATIONS SYSTEM, 2012.

[3] BUNDESMINISTERIUM DES INNEREN: *Schutz Kritischer Infrastrukturen - Risiko- und Krisenmanagement (Leitfaden für Unternehmen und Behörden)*, 2011.

[4] CHRISTOPHER CHANTRILL: *Comparison of State and Local Government Revenue and Debt in the United States Fiscal Year 2012*. Technischer Bericht, usgovernmentspending.com, September 2013.

[5] DACEY, ROBERT F: *Critical infrastructure protection: Challenges in securing control systems*. U.S. General Accounting Office, 2003.

[6] HU, ZI, JOHN HEIDEMANN und YURI PRADKIN: *Towards geolocation of millions of IP addresses*. In: *Proceedings of the 2012 ACM conference on Internet measurement conference*, IMC '12, Seiten 123–130, New York, NY, USA, 2012. ACM.

[7] ICS-CERT: *Alert (ICS-ALERT-11-343-01)*. Technischer Bericht, Industrial control systems cyber emergency response team, 2012.

[8] ICS-CERT: *ICS-CERT Monitor October/November/December 2012*. Technischer Bericht, Industrial control systems cyber emergency response team, 2012.

[9] LEVERETT, EIREANN P.: *Quantitatively Assessing and Visualising Industrial System Attack Surfaces*. Diplomarbeit, University of Cambridge, Computer Laboratory, Darwin College, 2011.

[10] LOUIS-F. STAHL, RONALD EIKENBERG: *Kritisches Sicherheitsupdate fÃ¼r 200.000 Industriesteuerungen*. http://heise.de/-1934787, August 2013. Zugegriffen am 2013-08-26.

[11] LOUIS-F. STAHL, RONALD EIKENBERG: *Verwundbare Industrieanlagen: Fernsteuerbares Gotteshaus*. http://heise.de/-1902245, Juni 2013. Zugegriffen am 2013-08-26.

[12] NASA EARTH OBSERVATORY: *Earth at Night 2012: It's the end of the night as you know it; you'll see fine.* http://earthobservatory.nasa.gov/Features/ NightLights, 2012. Zugegriffen am 2013-08-20.

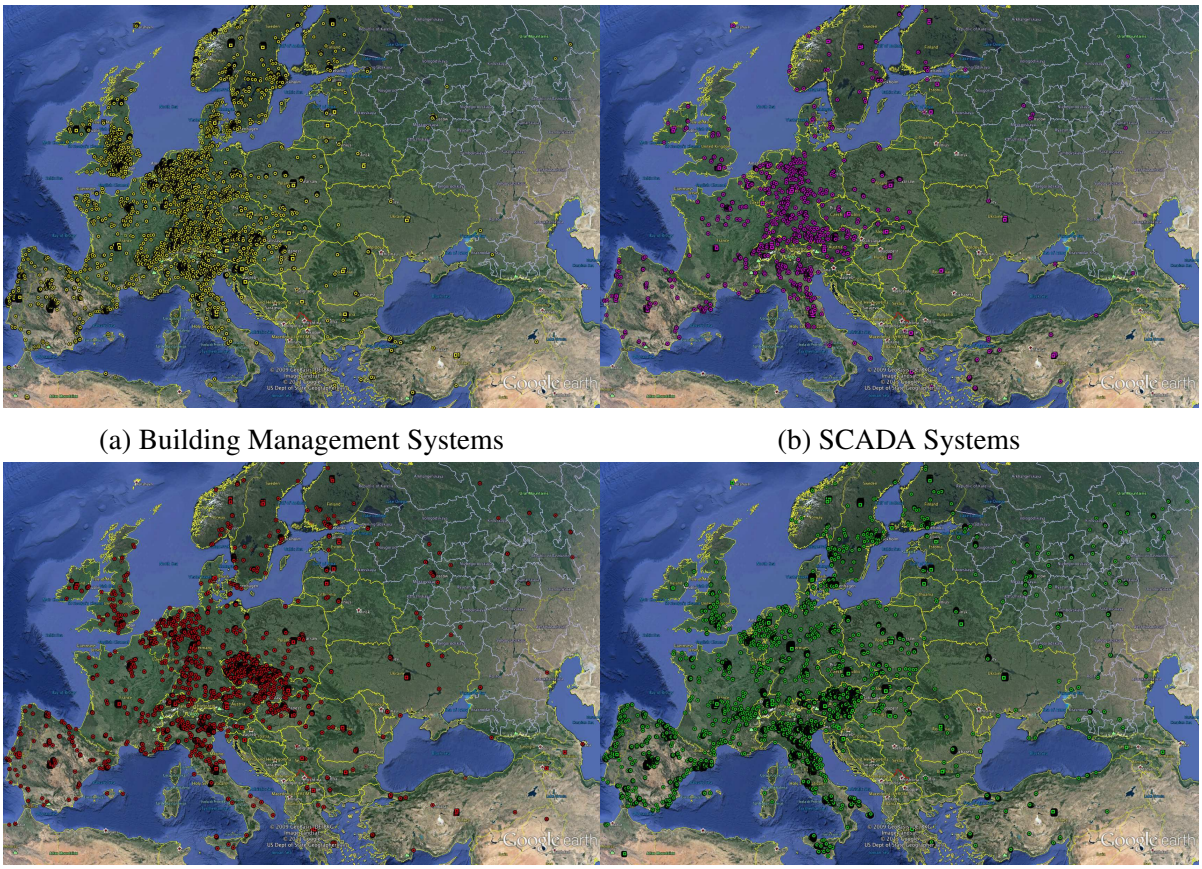
[13] RONALD EIKENBERG: *Kritische Schwachstelle in hunderten Industrieanlagen*. http://heise.de/-1854385, Mai 2013. Zugegriffen am 2013-08-26.

[14] RONALD EIKENBERG: *Vaillant-Heizungen mit Sicherheits-Leck*. http://heise.de/-1840919, April 2013. Zugegriffen am 2013-08-26.

[15] SAM CLEMENTS, MOTHERBOARD: *The Inventor of Shodan Will Help You Hack Our Internet-Enabled, Security-Free Infrastructure.* http://motherboard.vice.com/blog/shodan-can-help-you-access-our-internet-enabled-security-free-infrastructure. Zugegriffen am 2013-08-22.

[16] WILHOIT, KYLE: *The SCADA That Didn't Cry Wolf - Who's Really Attacking Your ICS Equipment? (Part 2)*. Black Hat Archives, 2013.

10 Bildtafeln



(a) Building Management Systems (b) SCADA Systems

(c) Programmable Logic Controller (d) PLC Network Devices

Abbildung 2: Selektion verschiedener Kategorien

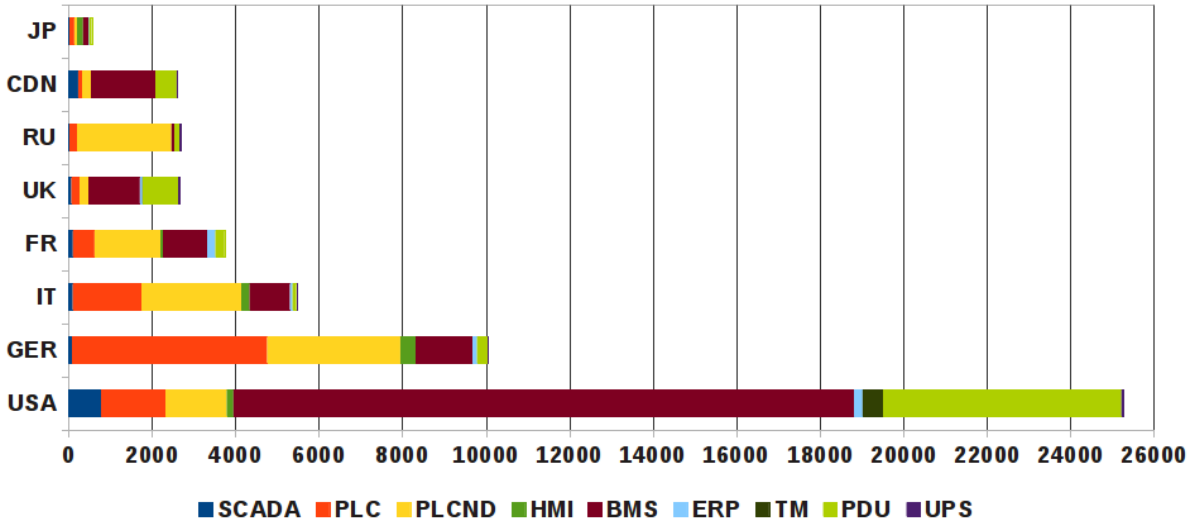
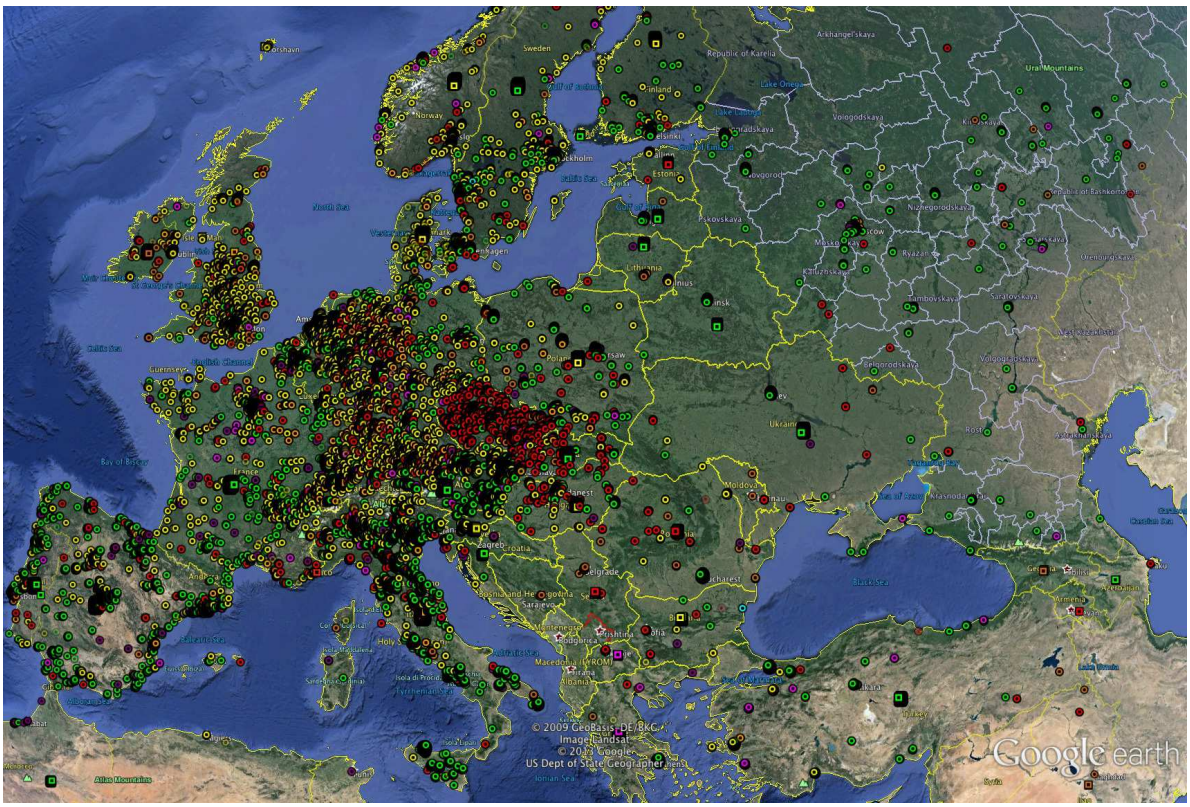
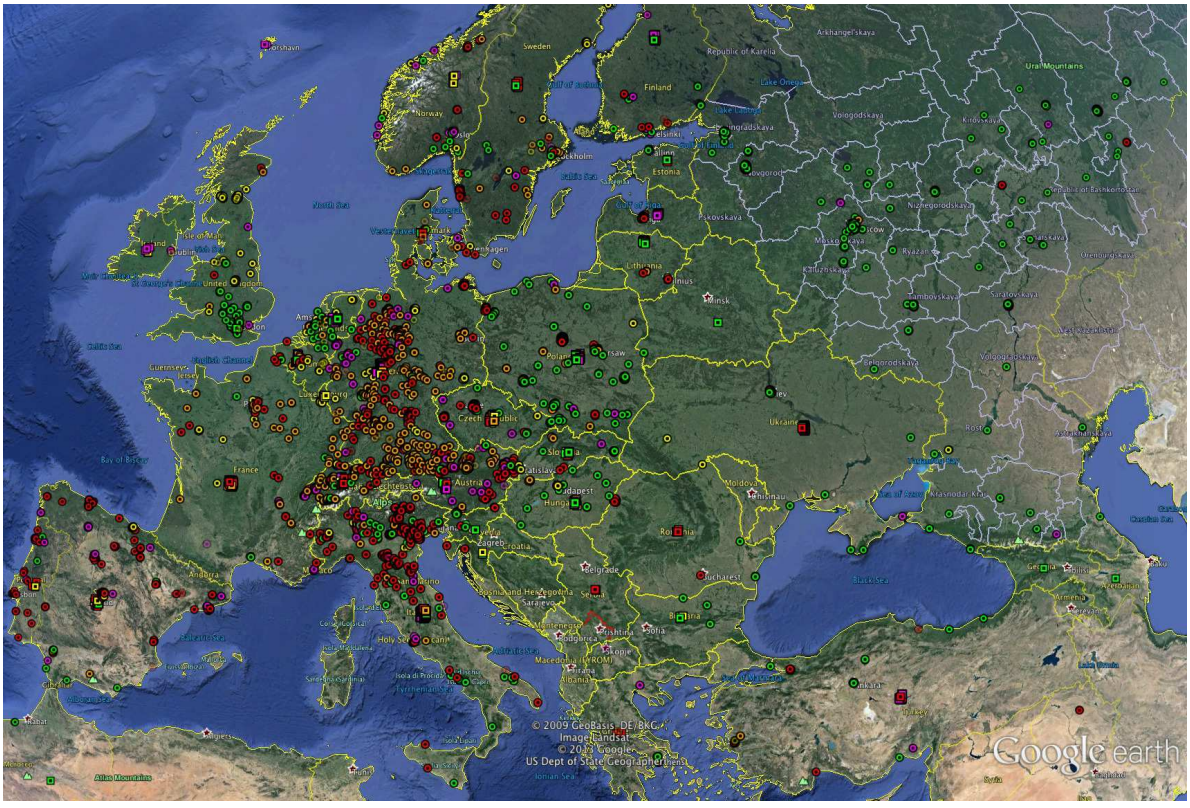


Abbildung 3: Verteilung der verschiedenen Gerätekategorien in den G8 Staaten

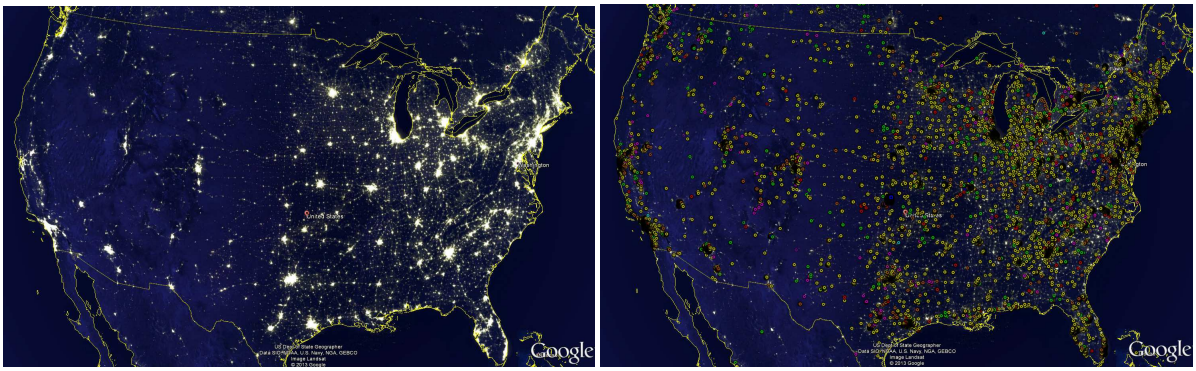


(a) Erreichbare Systeme im europäischen Raum. Jeder Punkt repräsentiert ein System. Die Farben entsprechen der Liste in Unterabschnitt 3.5 - Klassifizierung.



(b) Verwundbare Systeme im europäischen Raum. Die Farben entsprechen der Liste in Unterabschnitt 3.5 - Klassifizierung.

Abbildung 4: Gefundene Geräte in Europa



(a) Nächtliche Lichtquellen in den USA [12] (b) Steuerungssysteme in den USA

Abbildung 5: Vergleich Lichtstärke und Dicht von Steueranlagen in den USA

Abbildung 6: Bekannte Geräte im asiatischen Raum

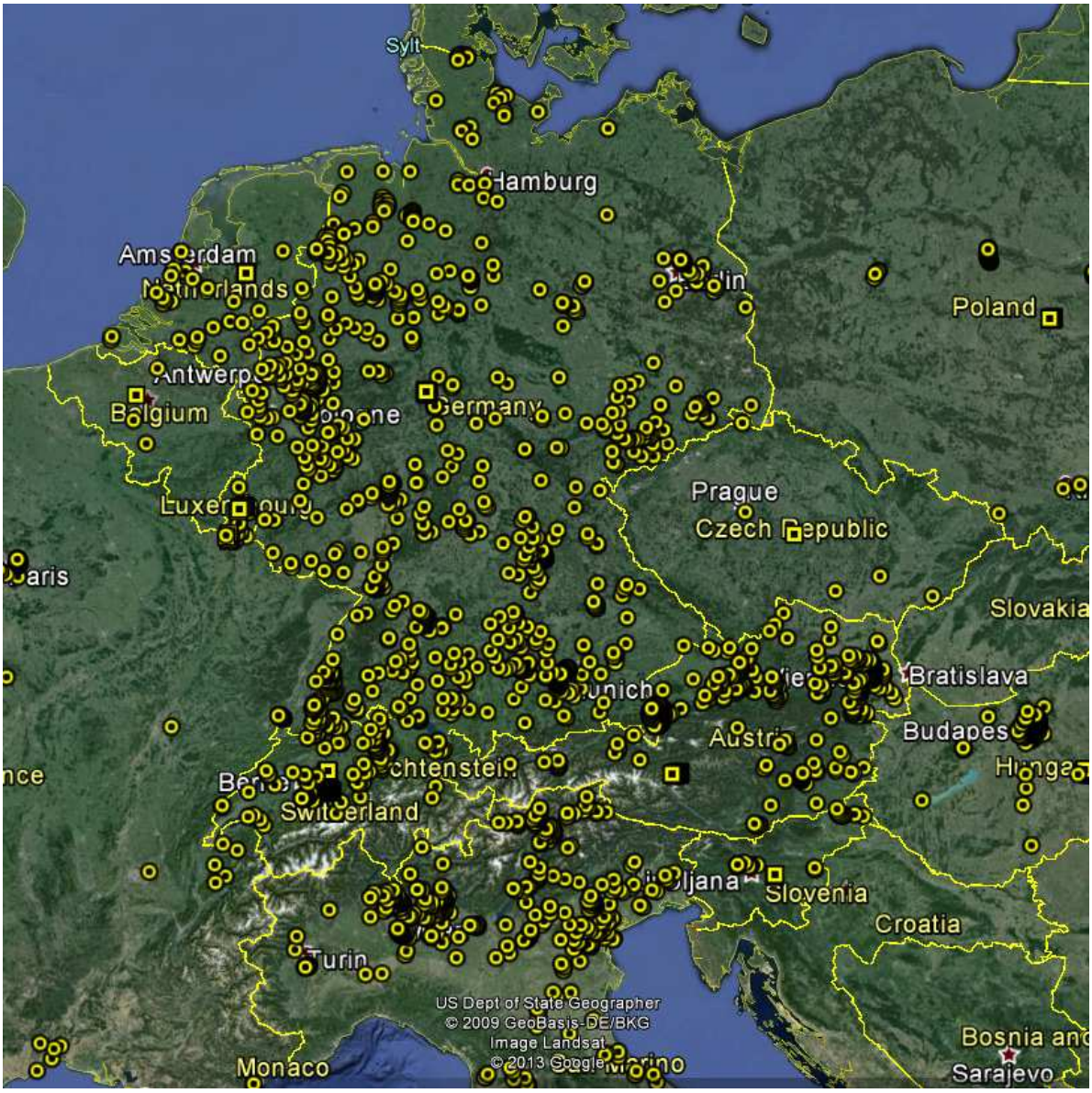


Abbildung 7: Geräte mit Controller von Saia-Burgess

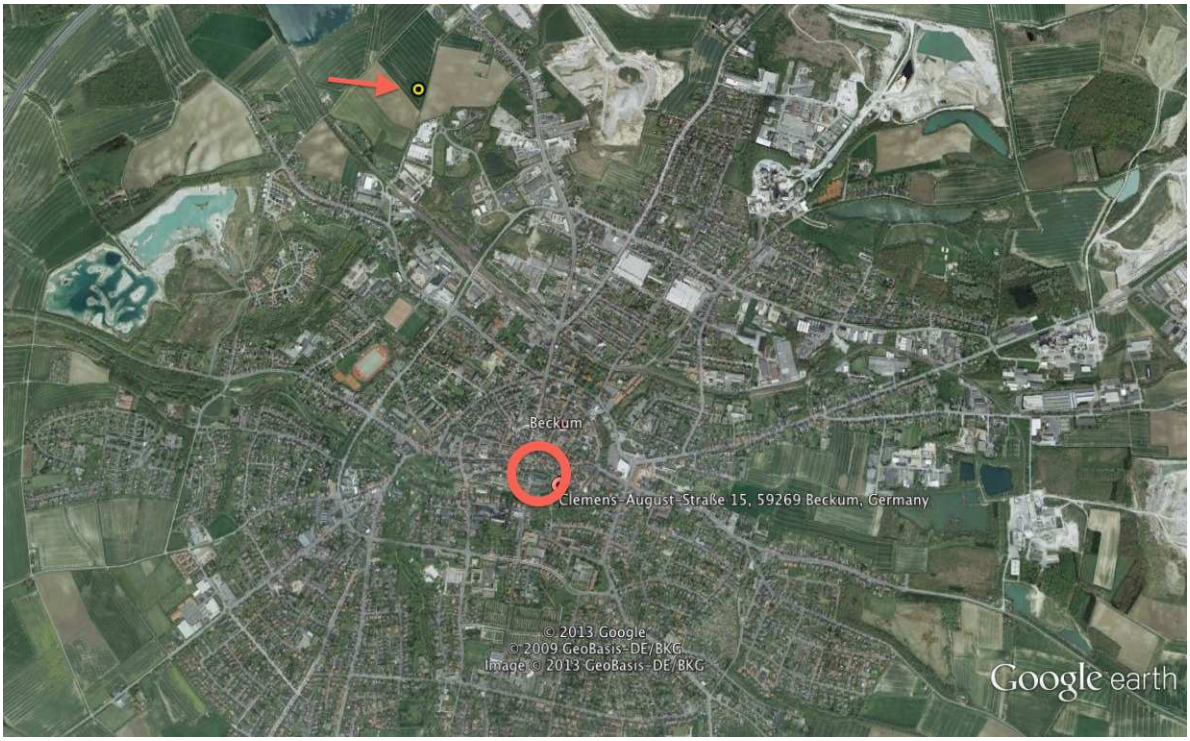


Abbildung 8: Verortung der Anlage in einer Kirche in Beckum [11]. (Pfeil = Verortung, Kreise = realer Standort)

.

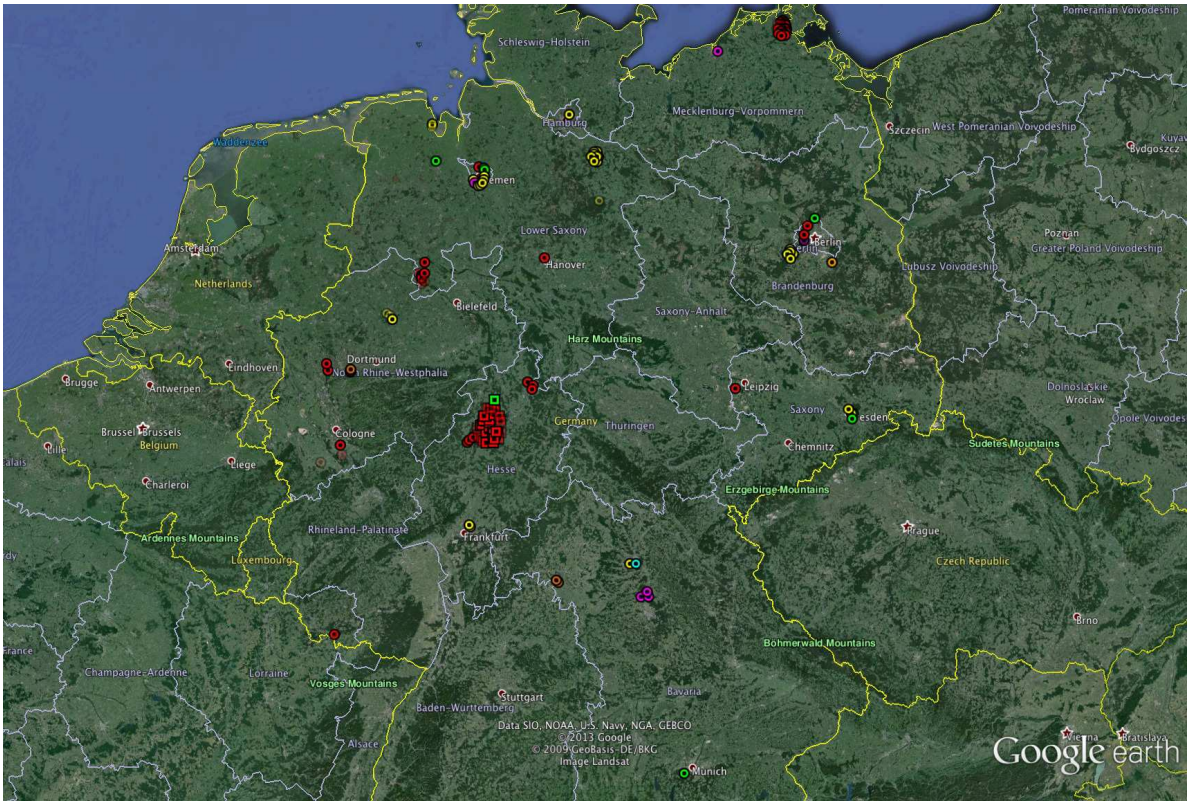


Abbildung 9: Gefundene Anlagen im DFN