Energetic Neighborhoods

Chances & Challenges of Smart Districts

08.01.2020

Energetic Neighborhood

Fliegerhorst Oldenburg

- Development of a smart city residential area with about 110 residential units
- Participation in research

Energetic Neighborhood

Fliegerhorst Oldenburg

- Maximizing local consumption of locally produced energy
- Conversion of excess energy into other forms of energy
- Coupling of the sectors electricity, heating/
  cooling and mobility in one supply network
- Construction and operation of a data and transaction platform
- Development and testing of business models
  for the construction and operation of Energetic Neighborhoods
- Transfer to other northern Germany typical districts with increasing self-supply

Surface area: ~ 3.9 hectare

Project Phases

Smart City Preliminal Study (07/2015 – 12/2015)

Citizen Participation (07/2015 – 08/2016)

Strategy & Vision Smart City Oldenburg: Administration, Research und Industry (01/2016 – 12/2016)

Project ENaQ (04/2016 – today)

- EnAQ the Centerpiece of Smart City Oldenburg
- Research of technical & social innovation
- Cooperative and incremental

Citizen Participation

Innovation Camps of „Fliegerhorst Oldenburg – City of the Future 2030+“

Healthy Living & Ageing

- Remaining in a known Environment
- Integrated into a stable Neighborhood

High Quality of Living

- Healthcare in the District
- Mobility & Freedom

Safe & Secure Home

- Reliable Serivces
- Early-warning System

Individual Needs

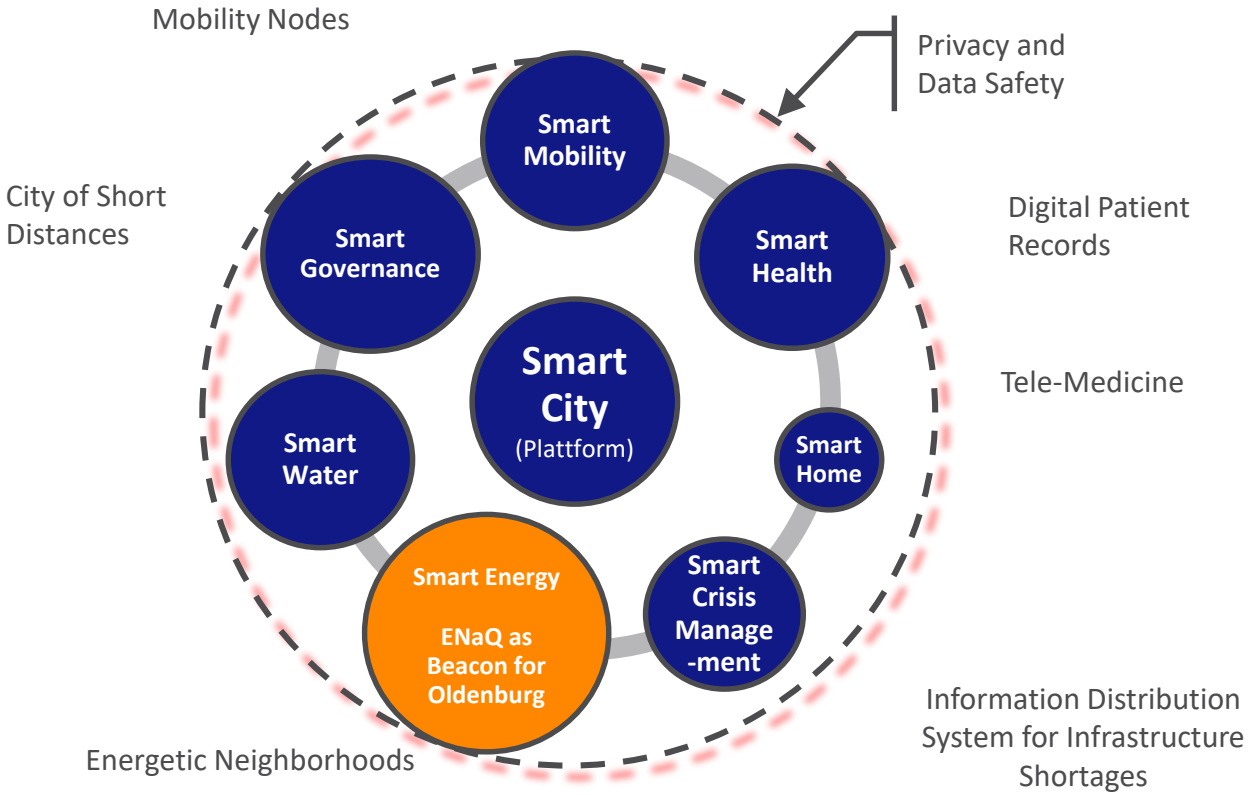
- Adaptable Environment
- Privacy

Sustainable Supply

- Partially self-sufficient power/water/gas supply
- Trade power with neighbors

Smart City Strategy & Vision for Oldenburg

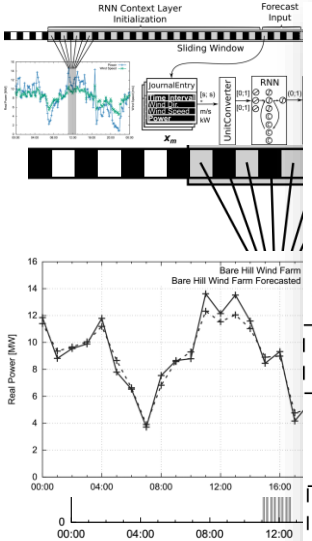
Not just for Mega Cities



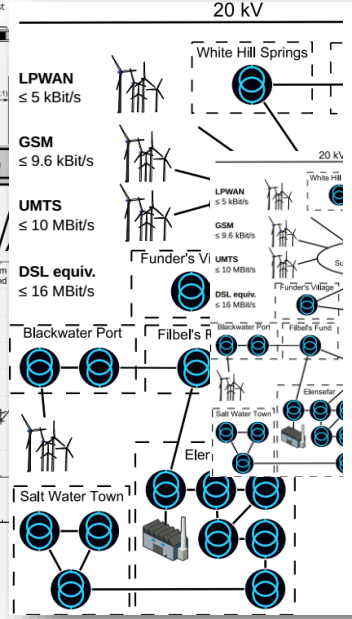
Agenten-Based Smart Grids

Universal Smart Grid Agent for Distributed Power Generation Management

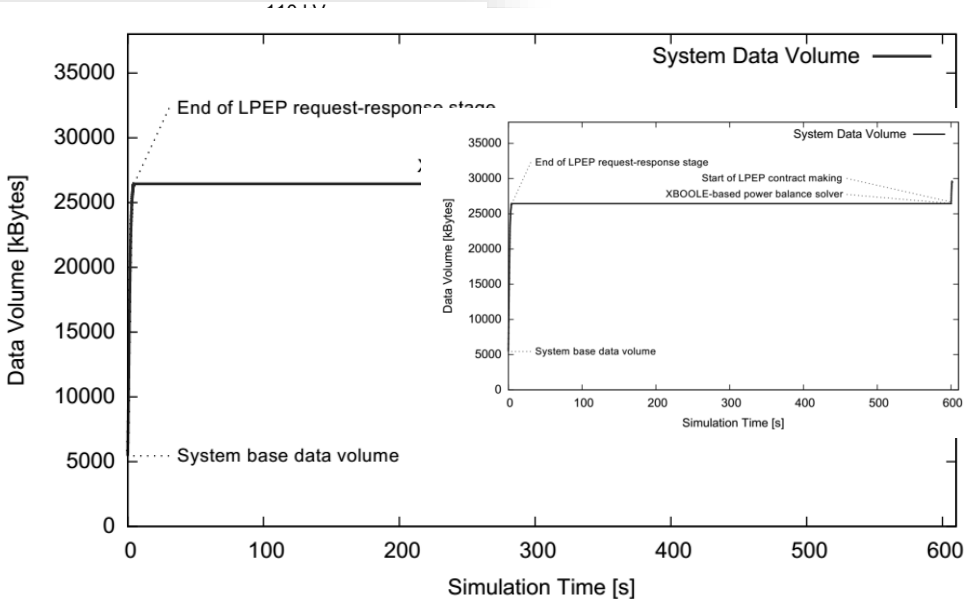
Forecasting



Cooperation



Equilibrium



17MW Line Loss Reduction in Fukui-TEPCO Benchmark ($\xi = 0{,}6\,{}^{W}/_{B}$)

Challenges for Smart Cities

1. Trends of digitalization will conquer the power grid.
2. Digitalization will lead to a new threat level, with high damage potential for society.
3. A digitalized, smart power grid is neccessary to reach environmental goals and also offers chances for resilient operation.

We do not yet fully understand how digitalization and critical infrastructures influence each other.

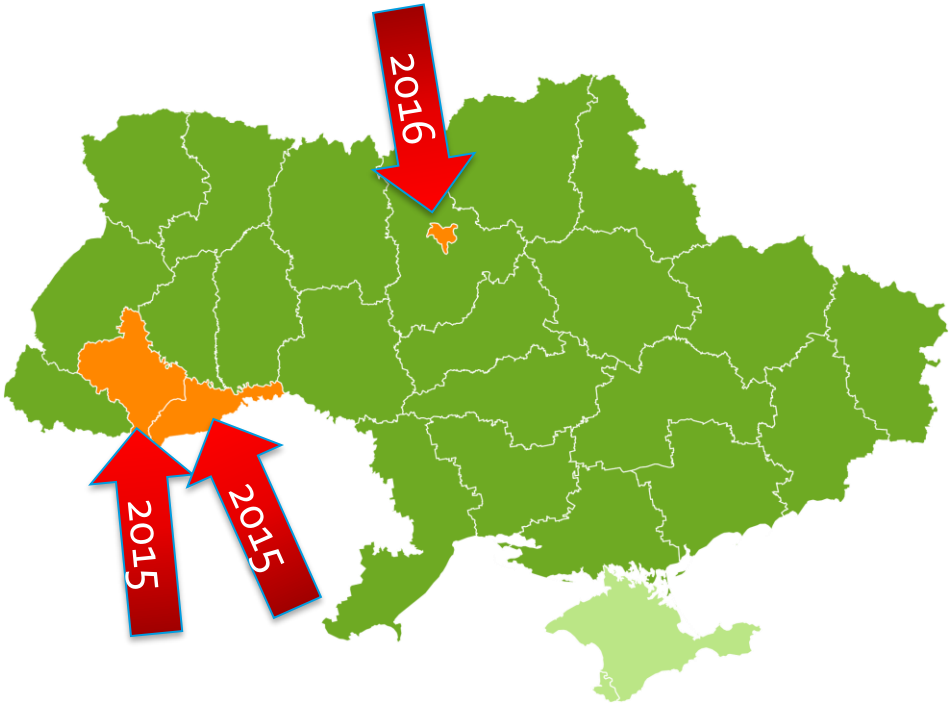
Leopoldina Nationale Akademie der Wissenschaften
acatech DEUTSCHE AKADEMIE DER TECHNIKWISSENSCHAFTEN
UNION DER DEUTSCHEN AKADEMIEN DER WISSENSCHAFTEN

Energiesysteme der Zukunft (ESYS II)


“There are two types of companies:
those that have been hacked
and those who don‘t know
that they have been hacked.“
John T. Chambers.

Das trifft auch auf Energiesysteme zu

Hackerangriff auf das Stromnetz in der Ukraine, 2015



23.12.2015

> Blackout in Ukraine through **cyber attack**

> **3 utilities**

> **High degree of automation** of distribution grid

> Operative intrusion into **OT,** disconnect of several substations.

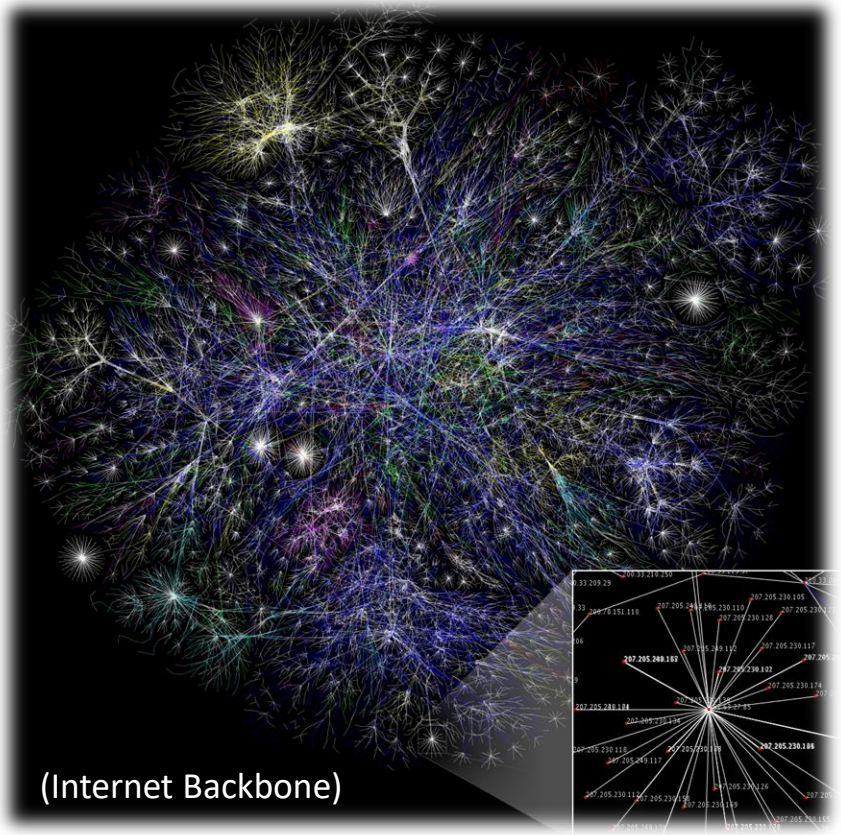
2016

> **Automated** attack

AI Learns Resilient Control

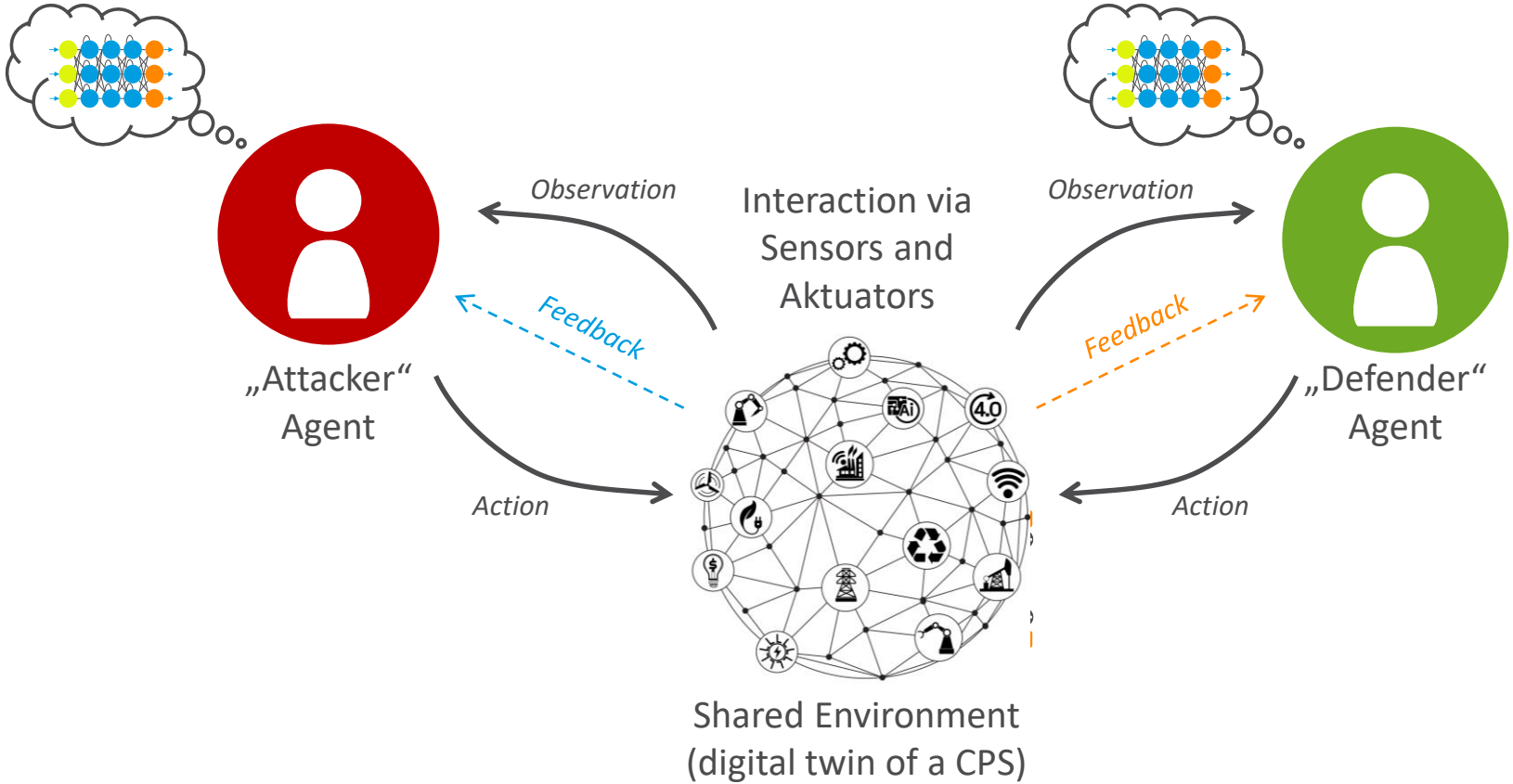
CPS inherently vulnerable

- Interconnected CPS have always attack suface **due to their inherent complexity**
  - Low latency of ICT and OT
  - High interdependence
  - Complexity in breadth and depth
  - Cricital Services as SPOF (DNS, BGP, *SCADA, SDL*)
- Learning Stratgies for **automatic issue mangement**



Adversarial Resilience Learning Concept

Competing Agents Learn in a Shared Environment



Analysis & Training of Resilient Systems

Flavors of ARL

Analysis – attacker only

- > Resilient Systems Lab
- > Angreifer explores vulnerabilities
- > „Conquest“ of a system
- > Attack vectors & log as basis of traditional analysis

Training – Attacker & Defender

- > AI for Grid Operation
- > Resilient overall system
- > Attacker trains defender
- > Attacks can be environmental factors
  - > Deviations in prognoses
  - > Accidents, etc.

Ethics of ARL

- > ARL a weapon?
- > **Lizence a soluation**?
- > **Laws of Robotics** possibly inherent?

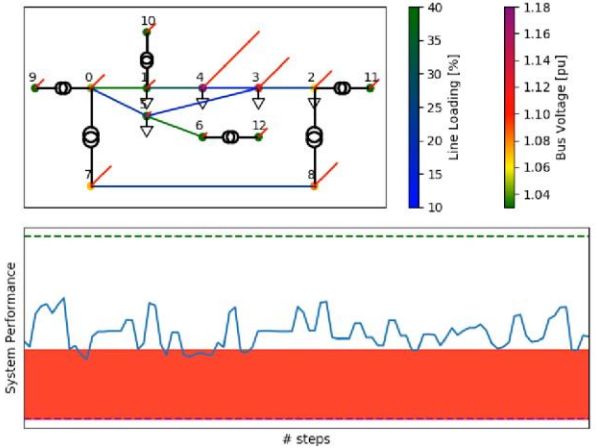
Demonstrator für Adversarial Resilience Learning

KI-basierte Analyse der Resilienz von Smart Grids

OFFIS INSTITUT FÜR INFORMATIK

```
Attacker measures (2000/3000)
-- grid.load0.change(scaling=0.76)
-- grid.load1.change(scaling=0.92)
-- grid.load1.change(scaling=0.17)
-- grid.load1.change(scaling=0.41)
Learning: Attacker ...
```

Attacker Score:
0




```
Defender measures (2000/3000)
-- grid.gen0.change(scaling=0.37)
-- grid.gen1.change(scaling=0.1)
-- grid.trafo0.change(tp_pos=7.0)
-- grid.trafo1.change(tp_pos=-9.0)
-- grid.trafo2.change(tp_pos=5.0)
-- grid.trafo3.change(tp_pos=-5.0)
-- grid.trafo4.change(tp_pos=8.0)
-- grid.trafo5.change(tp_pos=-1.0)
Learning: Defender ...
```

Defender Score:
0

Conclusion

ARL enables discovery of vulnerabilities and interdependencies

> Even when conform to regularizations! (EnWG, GridCodes, TAB etc.)

Development of defense (!) strategies

> Ethic dilemma

„Attacker-Defender-Games“

> Impact analysis in „anomalie-sensitive State Estimation“

> Risk models, investment strategies (finding an equilibirum)

> Analysing asymmetries („Rigging the Game“)

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung