Maria Zhdanova, Julian Urbansky, Anne Hagemeier, **Daniel Zelle**, Isabelle Herrmann, Dorian Höffner

Local Power Grids at Risk – An Experimental and Simulation-based Analysis of Attacks on Vehicle-To-Grid Communication

Introduction

Current grid situation

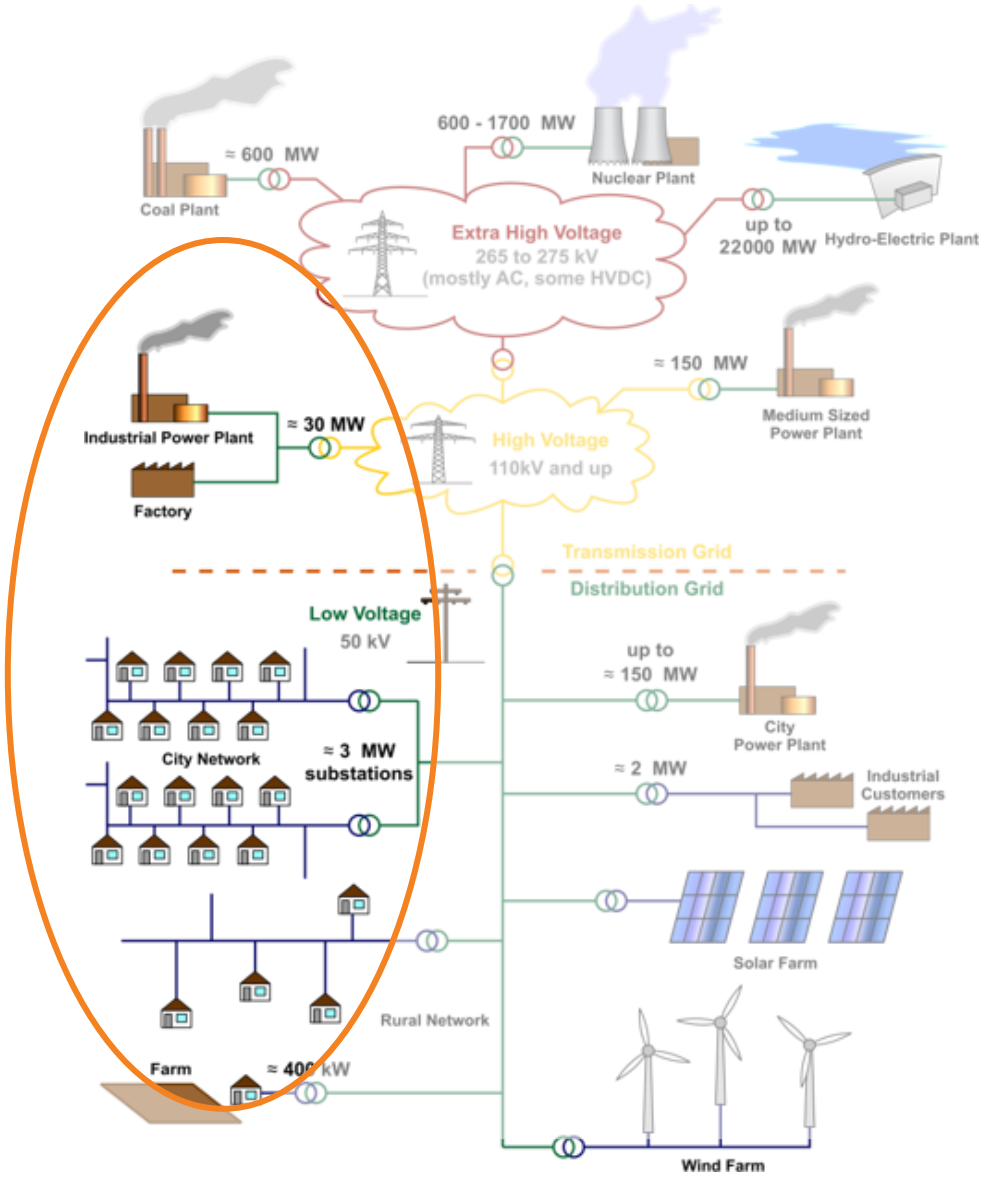
- **10 million electric vehicles worldwide**
- **EV charging already has grid impacts**
  - California advised to avoid EV charging to save energy during heat wave
  - Norway restricted EV charging times to avoid peak-hour charging
- **Operators have two options:**
  - Grid expansion
    - ➢ requires enormous local investments
  - Digital load management solutions
    - ➢ already integral part of present discussions on improving LV grid capacity

BACKGROUND

- Distribution Grids
- Protocols for Electric Vehicle Charging

BACKGROUND
Distribution Grids

- Focus on European low voltage (LV) grids
- Increasing number of power consumers
  - Heat pumps, electric vehicles -> increased grid loads.
  - LV grids vary in structures, sizes, capacities -> different stress levels.
- Risk of local blackouts
  - Grids that are already close to capacity limit could overload with increased consumers if no countermeasures are taken.
  - Overload leads to accelerated aging and possibly damage cables or transformers.
  - To prevent damage, safety devices will disconnect grid from power supply.

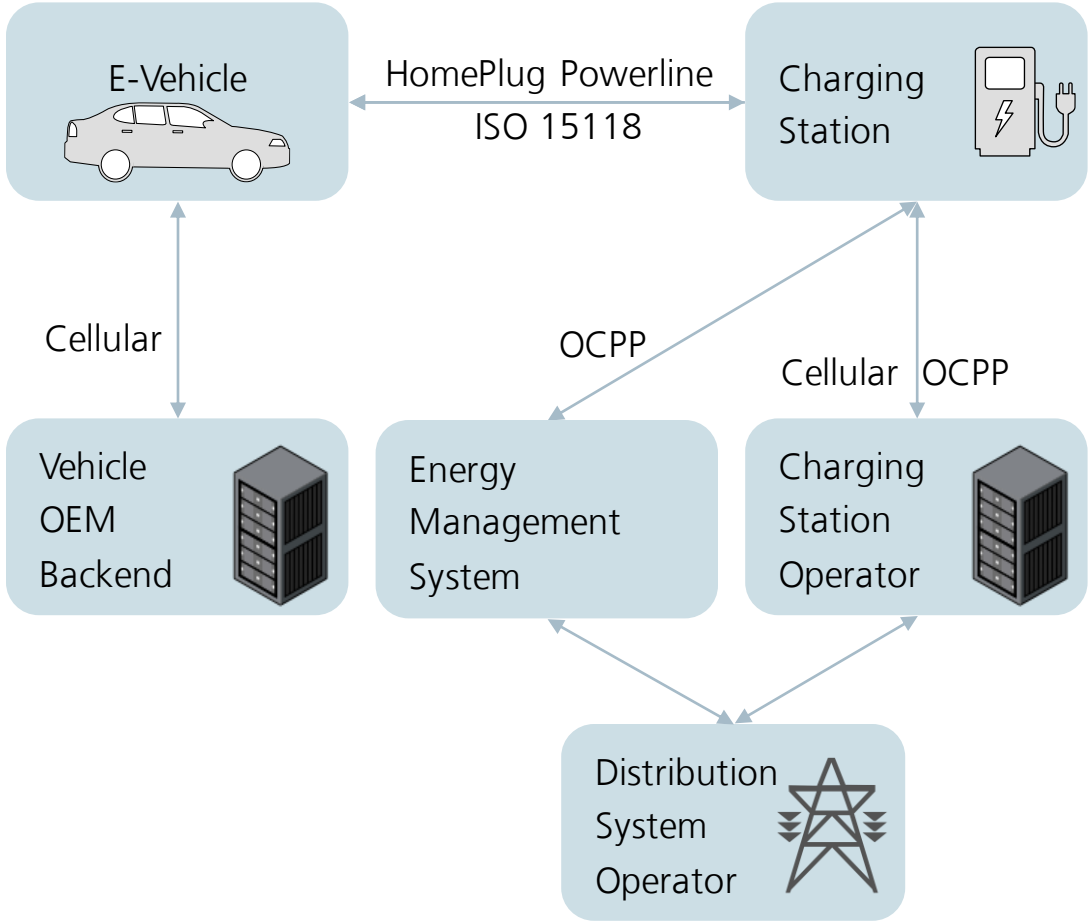


Source: MBizon, licensed under CC BY3.0, Electricity Grid Schematic English

BACKGROUND

Protocols for Electric Vehicle Charging

- EV <-> CS: ISO 15118
  - HomePlug Powerline
  - Plug and Charge
  - Negotiate Charging Parameters
- Open Charge Point Protocol (OCPP)
  - Control Charging Station
  - Authorization
  - Schedule Charging Process



SIMULATION

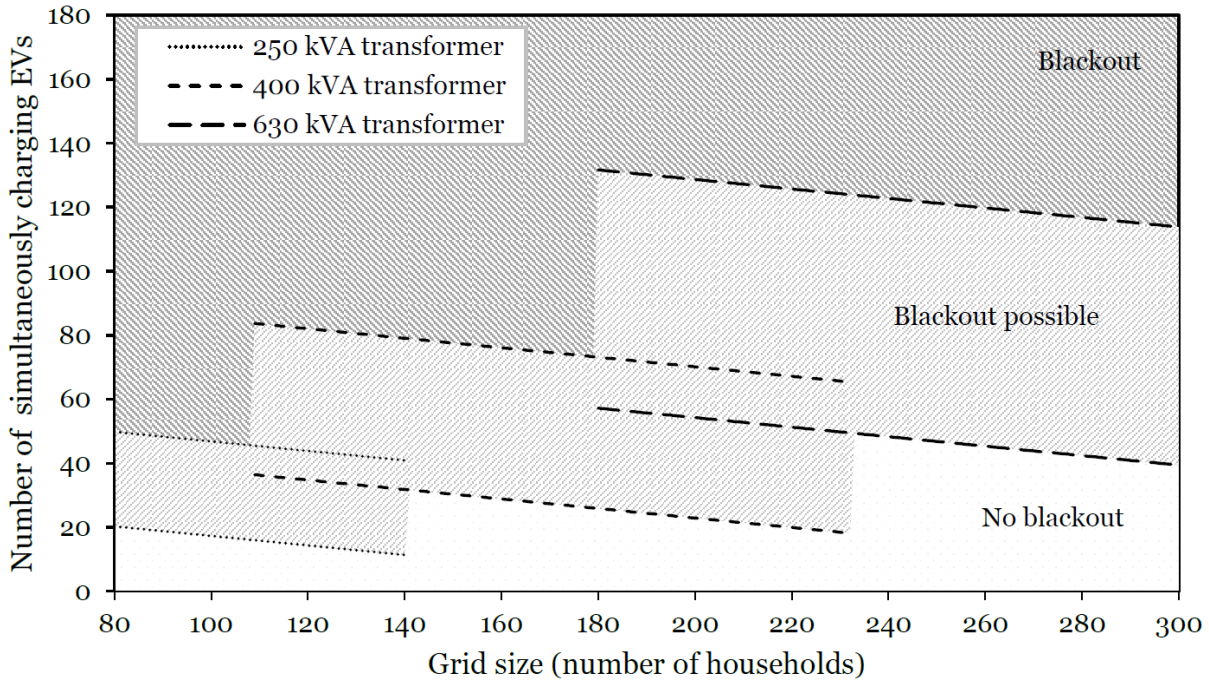
- Preliminary Considerations
- Modeling
- Simulation results

GRID SIMULATION

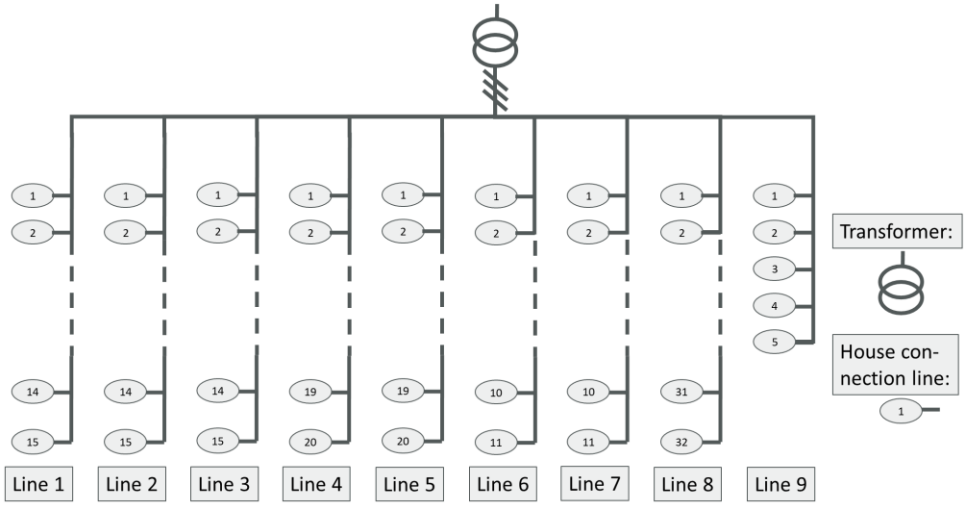
Preliminary considerations

- Aim of the simulation
  - Demonstrate a critical load situation due to manipulation of the load management in a typical European LV grid
  - No simulation of the actual blackout mechanism, but of the loads that would lead to a blackout.

- Estimation of critical amount of charging EVs
  - Based on typical grid configurations, the number of simultaneously charging EVs is determined, that might/will surely lead to a blackout.
  - Load management will prevent simultaneous charging, therefore a manipulation could lead to an overload.
  - The actual load situation highly depends on weather data und load simultaneity.
- Modeling environment



GRID SIMULATION
Modelling



- Model definition
  - Modelling language and framework: Modelica/TransiEnt library
  - Suburban district with mostly one family houses, dating from the mid 90s.
  - Load management will reduce maximum EV charging power if total grid loads exceed limit.

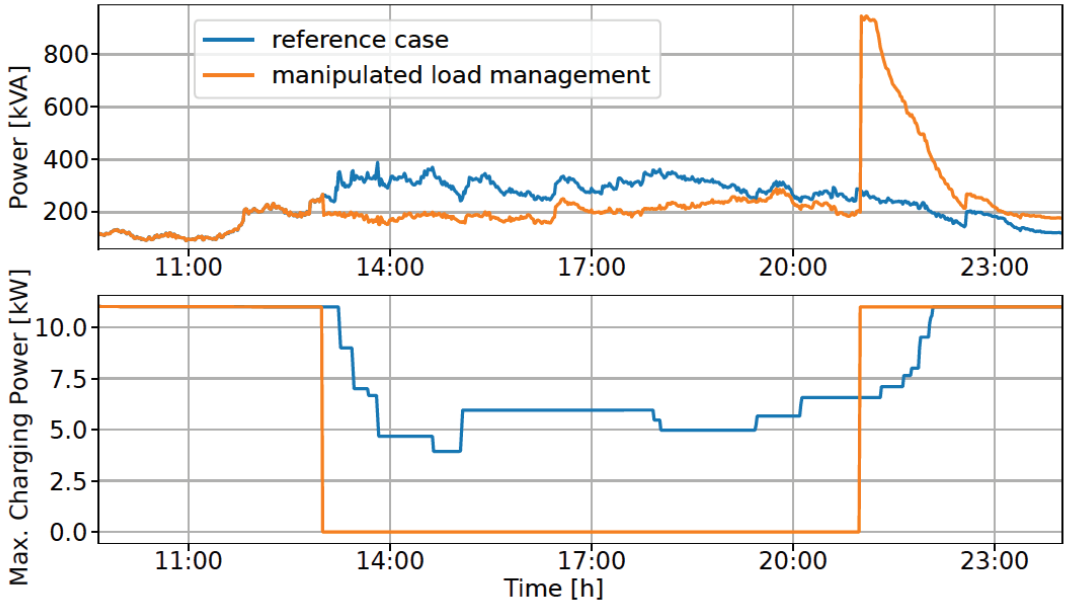
- Model parameters
  - 170 households in total (14-21 MWh electrical power)
  - 43 households equipped with PV and heat pumps
  - 85 households equipped with charging station (11 kW)

- Load profiles
  - Realistic profiles for electricity loads, hot water loads, driving and location profiles generated with a stochastic tool[1]
  - Heating profiles generated by building simulation.

[1]LoadPofileGenerator https://loadprofilegenerator.de/

GRID SIMULATION

Simulation results



- Analysis of annual load curves
  - EV charging adds a significant additional load to the grid.
  - On most days, no high simultaneity of EV charging.
  - Few days with critical loads, where load management reduces charging power.

- Manipulation of load management
  - Manipulation disables EV charging for several hours.
  - Sudden re-enabling of full power charging and disabling load management leads to high simultaneity.
  - Grid power reaches critical value, that will trigger safety equipment to disconnect local grid.

- Results
  - Number of charging stations that have to be manipulated highly depends on the structure of the grid.
  - Higher penetration of EVs will lead to higher simultaneities and grids that are more stressed.
  - Less equipped grids need lower number of manipulated charging stations or a shorter period of blocking the charging.

SECURITY ISSUES OF V2G PROTOCOLS

- Insecure channels
- Version downgrade
- Insecure PLC
- Session hijacking
- No end-to-end guarantees
- Cryptographic key reuse
- Non-existent PKI services

EXPERIMENTAL SECURITY ANALYSIS OF V2G COMMUNICATION

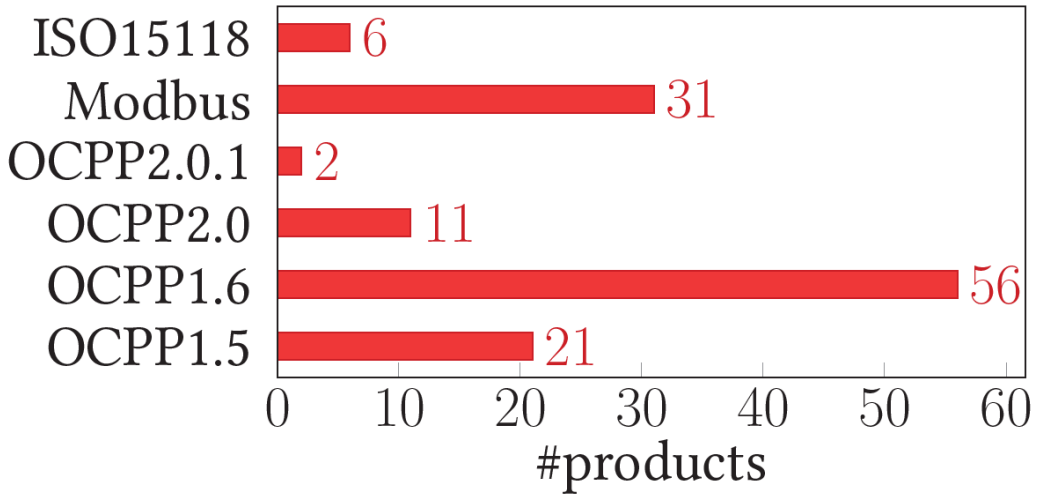
- Charger↔CPO
- Charger↔EV

EXPERIMENTAL SECURITY ANALYSIS OF V2G COMMUNICATION

Evaluation of Charging Station Communication

Practical analysis of 3 charging solutions

- Wallbox A: OCPP 1.5, 1.6; TLS 1.0, 1.1, 1.2
- Wallbox B: OCPP 1.6, 2.0; TLS 1.0, 1.1, 1.2; SSL 3.0
- HPC: OCPP 1.5, 1.6; TLS 1.0, 1.1, 1.2; SSL 3.0



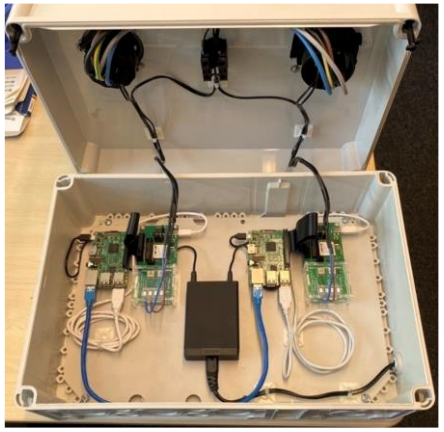
Practical Attack

- own self signed certificates
- read and modify the communication
- alter a charging schedule
- interrupt the charging process at will

EXPERIMENTAL SECURITY ANALYSIS OF V2G COMMUNICATION

Evaluation of ISO 15118 Communication

- Become part of low-level HPGP/PLC network
- Simply inject SessionStop for DoS
- Injecting unexpected or malformed messages also result in DoS
- MitM attack on ISO 15118 communication
- Inject charging schedules
- Gather private information



LIMITATIONS AND MITIGATION

Practicality of the Attack

- Damaging the equipment or causing a blackout in the LV grid is possible but takes a significant load accumulated over time.
- Adequate detection by DSO or CPO may prevent an attacker from experimenting for a long time to find the correct timing (is unlikely)
- Larger-scale attacks can exceed the grid limit:
  - Normal energy consumption in the neighborhood
  - Charging shifted by a DoS attack like Brokenwire
  - Attacker-manipulated schedule
  - Direct control of charging stations
  - Attack using other high-wattage devices, e.g. air conditioners, heat pumps and other systems

LIMITATIONS AND MITIGATION

Mitigation Strategies

- **Improving overall grid capacity**
  - Most effective countermeasure
  - Cost intensive
- **Improving the security of load management**
  - Proper device authentication
  - Device integrity measurements
- **Safety and fallback mechanisms for load management**

Conclusion

- Manage grid load can be impacted by targeted manipulation of large consumers such as EVs.
- We showed the conditions under which local grids can collapse.
- Explain possible attack strategies in the paper.
- Blackouts are possible if the grid's capacity is close to its limit.
- Experiments have shown the vulnerability of charging infrastructure.

Questions?

Contact

Daniel Zelle
Team Leader Automotive Security
Tel. +49 6151 869-263
daniel.zelle@sit.fraunhofer.de

Fraunhofer SIT
Rheinstraße 75
64295 Darmstadt
Germany
https://www.sit.fraunhofer.de/en/