VOOR DE NIEUWE **ENERGIE**GENERATIE

CYBER ATTACKS ON ELECTRIC VEHICLE CHARGING INFRASTRUCTURE AND IMPACT ANALYSIS

Sjors Hijgenaar | 13/06/2022

WHO AM I?
SJORS HIJGENAAR

INDUSTRIAL PHD CANDIDATE

- Grid strategy @ Stedin
- Research @ Delft University of Technology

RESEARCH

- Cyber attacks on EV charging infrastructure
- Impact analysis on MV distribution grids
- Machine learning for resilience assessment
- Resilience enhancement at grid’s edge

CO-AUTHORS

Baerte de Brey (Avere/ElaadNL), Alex Stefanov and Peter Palensky (TU Delft)

BRILLIANT

CYBER RESILIENT ELECTRIC VEHICLE CHARGING IN SMART GRIDS

- EV Charging Infrastructure is a **complex** system
- No system is 100% secure: **residiual risk**
- Decreasing RoI cybersecurity
- Definition: "*the ability to continuously deliver the intended outcome despite adverse cyber events*"

FIVE PHASES CYBER RESILIENCE [2]

1. Anticipate
2. Identify
3. Absorb
4. Recover
5. Adapt

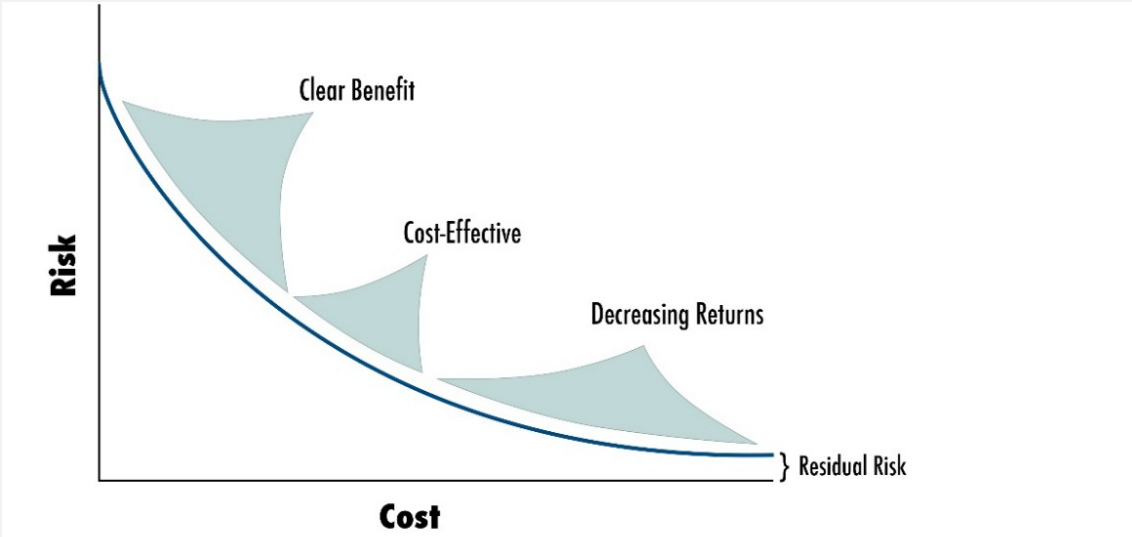
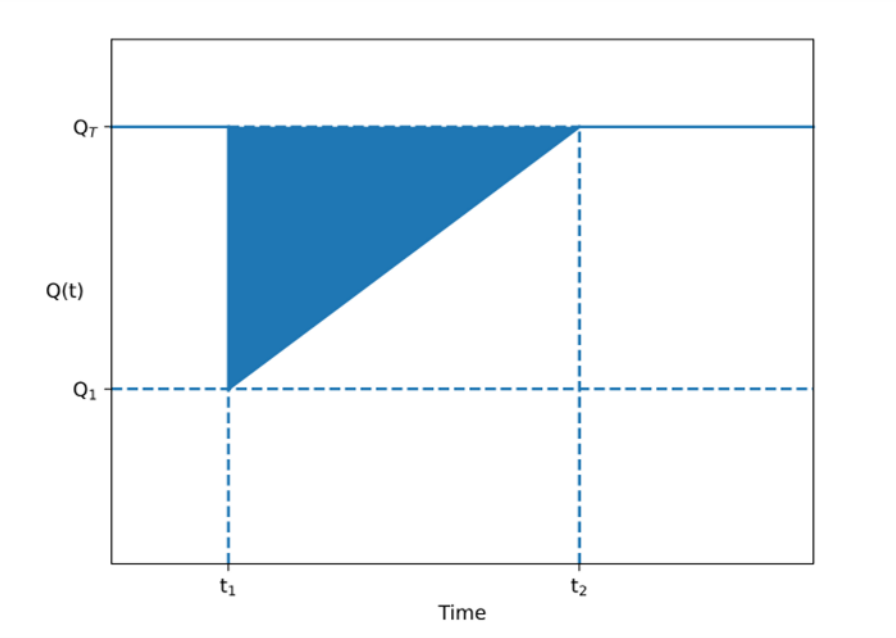


Figure 1. Conceptual diagram of the cost of buying-down risk in cyber systems.

[1: 10]



Resilience triangle, simplification of resilience trapezoid

CYBER ATTACK SCENARIOS
WHERE ARE WE AT RISK?

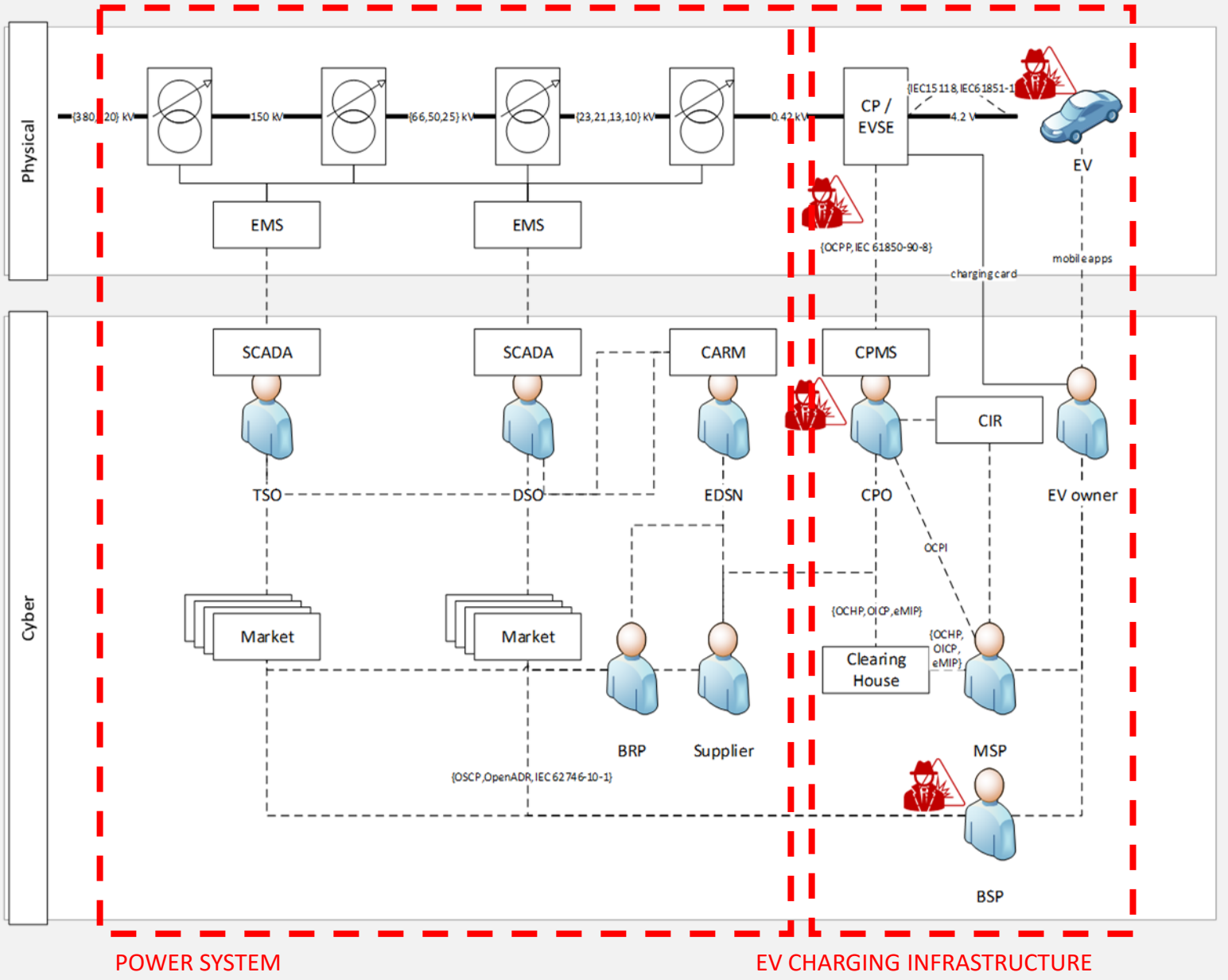
Complex *cyber-physical system* of stakeholders, systems and ICTs

Cyber attacks

- Physical (EV and CP)
- Flexibility services (CPO and BSP)
- CPMS (CPO)
- Protocol

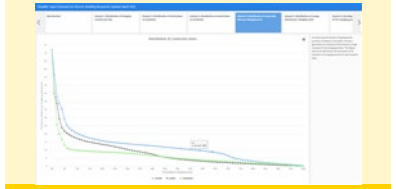
Cyber attack objectives: controllable load

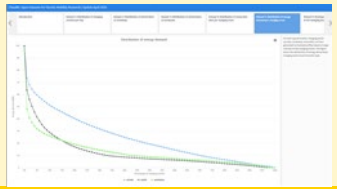
- Coordinated
- Cyclic
- Intelligent



EV CHARGING MODELLING
AGGREGATING STOCHASTIC BEHAVIOUR (1/2)


ARRIVAL TIMES


CONNECTION TIMES


ENERGY DEMAND


OUTLET POWER

[3]

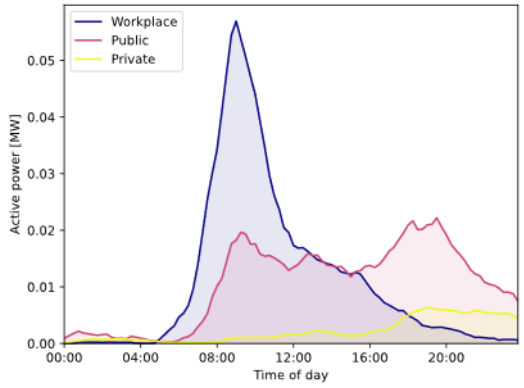
+

ELAADNL OUTLOOK

EV Charging Infrastructure development on 'CBS Buurt' level for 2021-2050

[4]

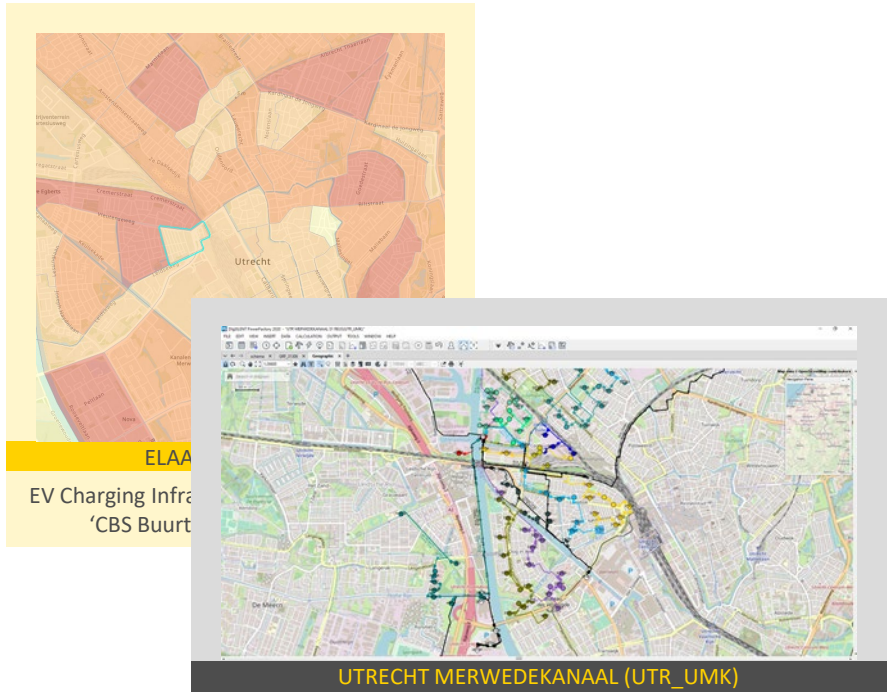
=

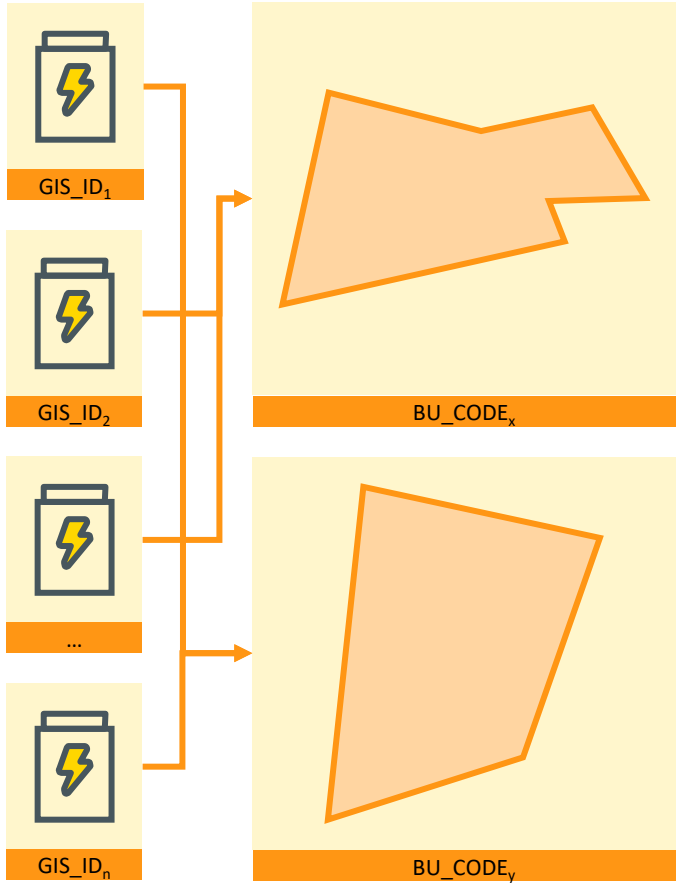


STOCHASTIC CHARGING BEHAVIOUR

DISCUSSION
- Interdependencies arrival times, connection times and energy demand (independence assumed for now)
- How will outlet power develop in future?
- How will charging behaviour change in future?

EV CHARGING MODELLING
AGGREGATING STOCHASTIC BEHAVIOUR (1/2)

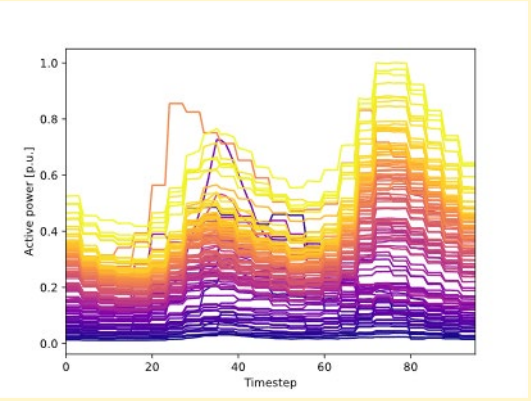




DATA

- Linking transformers to CBS Buurt

RESULT
New load profiles loaded into PowerFactory grid model for analysis



2021

EXPERIMENTAL SETUP
PSEUDO CODE

Algorithm 1 Method to Assess the Impact of Cyber Attacks on EVs

```
Data: PDF of arrival times, connection times, energy demand and charging power, number of charging points
per year per area, simulation time, timestep size, number of iterations, grid topology.
Result: average EV charging load profile on transformer level
initialization;
power flow analysis;
for each i in iterations do
        for each loads in loads do
                for each timestep in simulation time do
                        for each charge point in transformer charge points do
                                if occupied then
                                        if timestep = departure timestep then
                                                charging = false;
                                                occupied = false;
                                        if timestep = idle timestep then
                                                charging = false;
                                        if timestep < idle timestep then
                                                load += charge point outlet power;
                                else
                                        draw from arrival times PDF;
                                        if EV arrives then
                                                departure timestep = draw from connection times PDF;
                                                idle timestep = draw from energy demand PDF;
                                                load += charge point outlet power;
simulate cyber attack;
power flow analysis;
comparison of line loading and voltage levels;
```

SIMULATION RESULTS

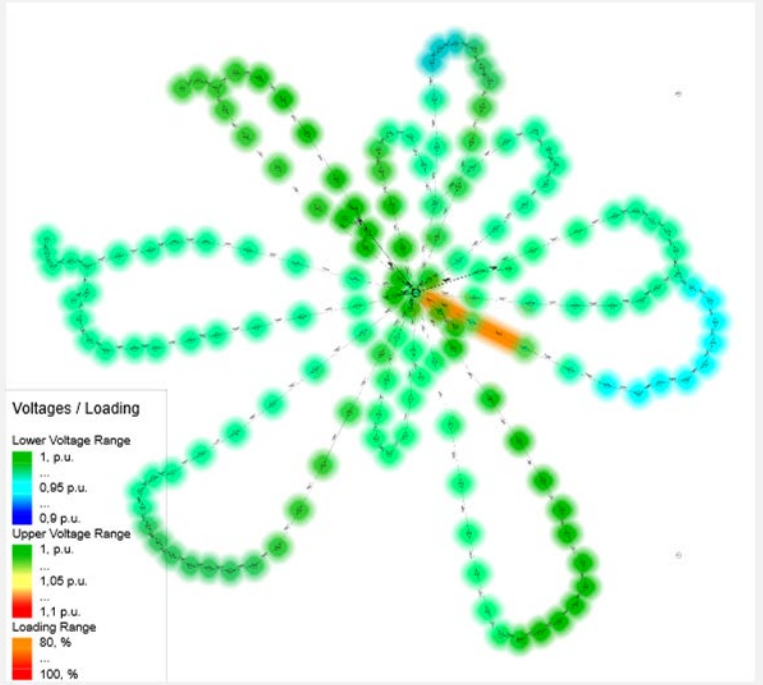
IMPACT ANALYSIS IN MV DISTRIBUTION GRID

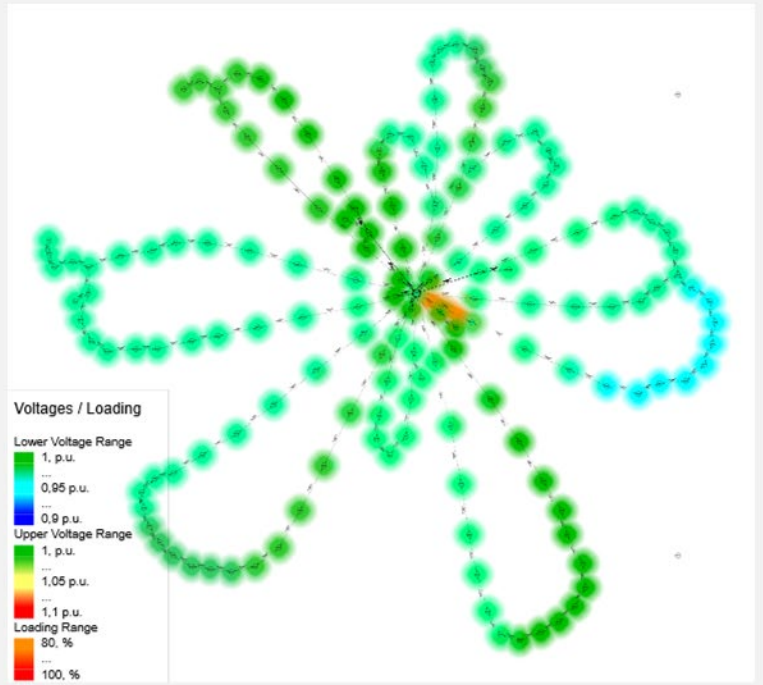
MODEL COUPLING WITH POWERFACTORY

- Using Python and PF API
- Quasi-dynamic simulation (QDS) 15 minute intervals
- Cyber attack modelling based on current tech (no smart charging no V2G)

CONCLUSIONS

- Able to simulate aggregated EV charging behaviour in MV grids
- Simulate cyber attacks on EV charging infrastructure in MV grids
- Effects on
  - DSO: Voltage stability, overloading, operational margins
  - TSO: Frequency stability
  - BRP: Loss of load, imbalances, financial losses
  - Customer: over-voltage shuts of PV, damage to appliances, loss of critical loads (e.g. electric ambulance)
  - Accross the board: reputation damages





LEGISLATIVE FRAMEWORK
FRAGMENTED, BUT THERE IS HOPE

- Alternative Fuel Infrastructure Regulation (AFIR)
- European Performance of Buildings Directive (EPBD)
- Directive on the security of Network and Information Systems (NIS Directive + NIS 2)
- Radio Equipment Directive (RED)

Are all risks covered?

- Example: OCPP not covered by AFIR
- Lack of standardisation
- Lack of concrete requirements

The European Cyber Resilience Act (ECRA)

- Potential starting point for solid legilative framework
- But will it contain EV infrastructures?

CONCLUSIONS AND FUTURE WORK
TOWARDS CYBER RESILIENT EV CHARGING!

- EV charging infrastructures rely on communications => susceptible to cyber attacks
- We demonstrate a method to analyse the impact of cyber attacks on MV distribution grids
- We highlight the disturbances to different stakeholders in the ecosystem
- We argue the fragmented legislative framework and encourage discussion on laws for EV charging infrastructure cyber security and resilience

FUTURE WORK

- Other attack scenarios, other grids
- Database generation and model learning for resilience assessment
- Improving resilience at grid's edge

VOOR DE NIEUWE **ENERGIE**GENERATIE

REFERENCES

[1] I. Linkov and A. Kott, “Fundamental Concepts of Cyber Resilience: Introduction and Overview,” in *Cyber Resilience of Systems and Networks*, New York, NY: Springer International Publishing, 2019, pp. 1–25.

[2] S. Hosseini, K. Barker, and J. E. Ramirez-Marquez, “A review of definitions and measures of system resilience,” *Reliab. Eng. Syst. Saf.*, vol. 145, pp. 47–61, 2016, doi: 10.1016/j.ress.2015.08.006.

[3] ElaadNL, “ElaadNL Open Datasets for Electric Mobility Research | Update April 2020,” 2020. https://platform.elaad.io/analyses/index.php?url=ElaadNL_opendata.php (accessed Jan. 24, 2022).

[4] N. Refa, D. Hammer, and J. van Rookhuijzen, “Elektrisch rijden in stroomversnelling; Elektrificatie van personenauto’s tot 2050,” Arnhem, 2021. [Online]. Available: https://www.elaad.nl/uploads/files/2021Q3_Elaad_Outlook_Personenautos_2050.pdf.