CYBER SECURITY IN THE ELECTRIC VEHICLE CHARGING INFRASTRUCTURE

Harm van den Brink

Who am I?

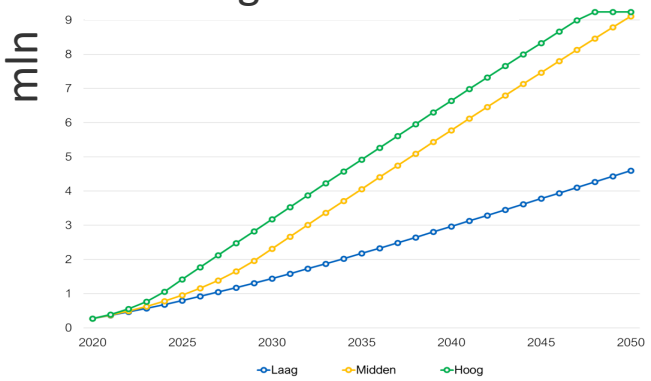
Harm van den Brink

- Background in IT & Cybersecurity
- 8+ years at ElaadNL
- Cyber Security & Innovation
- Chair taskforce cyber security National Action Plan Charging Infrastructure
- Volunteer @ Dutch Institute for Vulnerability Disclosure (DIVD)

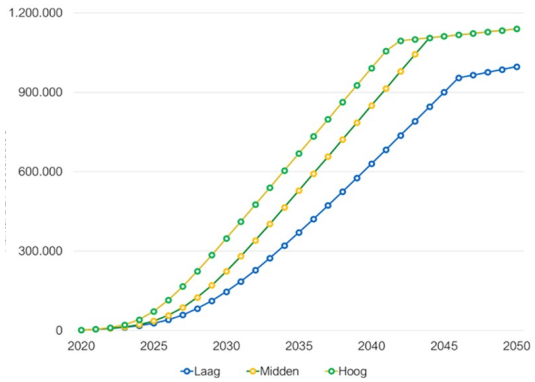
Growth of EV in *the Netherlands*

1.8 mln charging stations in 2030

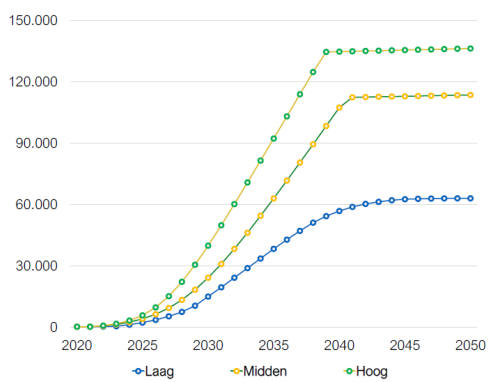
Passenger cars



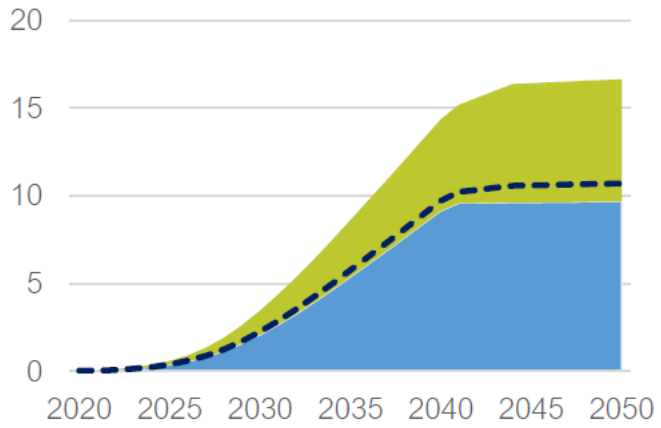
Vans



Trucks



Electricity demand in TWh

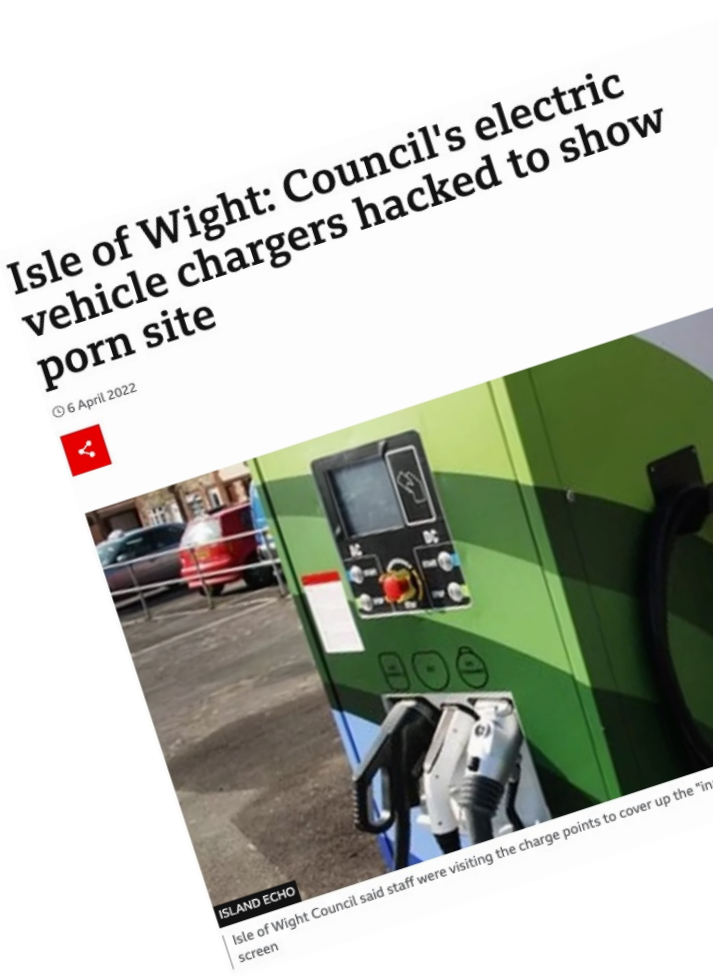


Total power demand in 2050:

Theoretical:	0-120 GW
In practice:	10-15 GW

The European incident reserve is 3GW (controlable demand/production)

The need for Cyber Security



Isle of Wight: Council's electric vehicle chargers hacked to show porn site

6 April 2022

ISLAND ECHO

Isle of Wight Council said staff were visiting the charge points to cover up the "in screen

Ungeschützte Ladesäule verrät Hunderte UIDs

Die Steuerung einer Ladesäule für E-Autos in Bayern war ungeschützt im Netz. Sie verriet UIDs, mit denen sich Ladekarten klonen und auf Kosten ihrer Besitzer Autos laden lassen.

Von Moritz Tremmel

10. März 2023, 9:00 Uhr

in Pocket speichern merken

(Bild: A. Krebs/Pixabay)

Die Steuerung von Ladesäulen sollte nicht ungeschützt im Internet sein.

Hacked Electrify America Charger Exposes Major Cybersecurity Risk

A person was able to easily gain control of an Electrify America charger using the TeamViewer app, raising concerns about customer security.

MICHAEL AKUCHIE PUBLISHED JAN 31, 2023

Risks

EV driver

- Car not charged
- Private information leaked
- Manipulation of financial details of transaction

Grid

- Local grid overload (if smart charging is overruled)
- Black-out (inter)national grid

Risks and grid impact

- A charge station is connected to the internet
- An electric vehicle (EV) typically charges with 10kW (AC)
- Data communication (ISO 15118) between EV and charge station introduces new risks to the system. (Malware, hacks, …)
- Charge stations are out in the open, everybody can access them and open them
- Vehicle to grid will add more risk, since it allows for also feeding back energy from the EV to the grid and EVs are connected for a longer period of time

https://eur-lex.europa.eu/legal-content/EN/TXT/?toc=OJ%3AL%3A2017%3A220%3ATOC&uri=uriserv%3AOJ.L_.2017.220.01.0001.01.ENG

Risks and grid impact

Analysis and advice

The scenarios studied are real and in the future will pose a real risk to the mobility of the Netherlands, the national charging infrastructure and the stability of the electrical grid. An estimate of the potential negative economic impact of such an incident could be as much as approximately 4 billion euros per day for the Netherlands. The social impact of a power failure depends largely on its duration. The social costs associated with power failures range from loss of leisure time to mobility, business activity and even life.

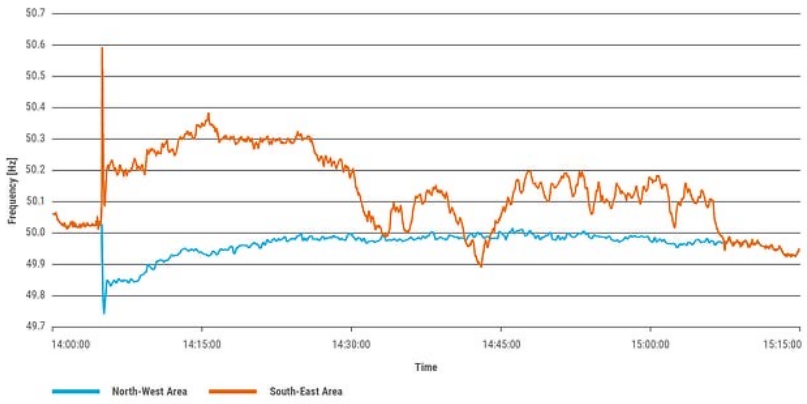
Report by Berenschot

https://www.agendalaadinfrastructuur.nl/PageByID.aspx?sectionID=208529&contentPageID=2135552

Risks and grid impact

- 300.000 cars charging equals 3GW of *collective* power
- 3GW is the European incident reserve capacity (frequency containment reserves)

A large hack, could potentially disturb the entire European grid. Vehicle to grid only adds to this challenge.



Number of charging points at the end of	2018	2019	2020	2021	2022	July 2023
Regular public + semi-public	**35,861**	**49,520**	**63,586**	**82,876**	**119,197**	**136,984**
Regular public (24/7 publicly accessible)	20,228	27,773	39,968	51,423	69,804	79,118
Regular semi-public (limited publicly accessible)	15,633	21,747	23,618	31,453	49,393	57,866
Fast charging points, public + semi-public	**1,116**	**1,262**	**2,027**	**2,577**	**4,164**	**4,625**
- of which >100 kW		433	897	1,307	1,878	2,288
Fast charging locations	197	339	467	629	972	
All regular + fast charging points	**36,977**	**50,772**	**65,613**	**85,453**	**123,361**	**141,602**
Number of plug-in passenger car (BEV + PHEV) per charging point	**3.7**	**3.9**	**4.2**	**4.5**	**4.2**	
Private charging points[1]	~80,000	~114,000	~158,000	~221,000	~345.000	~420.000

https://eur-lex.europa.eu/legal-content/EN/TXT/?toc=OJ%3AL%3A2017%3A220%3ATOC&uri=uriserv%3AOJ.L_.2017.220.01.0001.01.ENG

The challenges

- Awareness
- Technical
- Regulation

The challenges

Awareness

- Creating awareness of the need of cyber security
- Showing the real-world impact of a hack
- Inform customers about cyber security
  - 2/3rd of the market in NL are private chargers

The challenges

Technical

- Added cyber security to Open Charge Point Protocol (OCPP)
- Requirements and informal standards that secure the infrastructure (EV to backend)
  - Access control
  - Cryptography
  - Physical and environmental security
  - Operations security
  - Communication security
  - System acquisition, development and maintenance
  - Supplier relationships

- ElaadNL & European Network for Cyber Security (ENCS) requirements

EV-301-2019

Security requirements for procuring EV charging stations

Version 2.0

24 December 2019

The challenges

Regulation

- The cyber security requirements are used in different countries:
  - The Netherlands
  - United Kingdom
  - Portugal
- However the requirements are still informal and need to be formalized into international industry standards. Including certification of products.
- There is no regulation yet that covers the full EV infrastructure when it comes to cyber security requirements.

The challenges

Relevant regulation:

- NIS (Network and Information Security Directive) → implementation in 2026. Note: Implementation can differ per country.
- AFIR (Alternative Fuels Infrastructure Regulation): sets requirements for plugs and protocols, but not specifically for cybersecurity.
- EPBD (Energy Performance of Buildings Directive) → refers to the definition of charging points to AFIR.
- NCCS (Network Code on Cyber Security): new regulation from the perspective of grid operators. Primarily affects large electricity consumers or producers.
- ITS (Intelligent Transport Systems)
- RED (Radio Equipment Directive): mainly sets requirements for the (wireless) communication link between the charging point and back office; enforced by RDI.
- EU-proposal for a new Cyber Resilience Act: has a broad horizontal application, the manufacturer must support the product throughout its entire lifecycle; attains status as regulation.

What does ElaadNL/NAL do?

- Create cyber security requirements together with ENCS
- Public tenders, add cyber security since 2016. Only 1/3rd of the market are public chargers
- National Action Plan Charging Infrastructure, creating awareness and trying to standardize cyber security (in standards & legislation)
- Setting up an Information Sharing & Analysis Center (ISAC). Charge point operators and manufacturers share in a trusted environment vulnerabilities and cyber security challenges.
- Map requirements to official IEC 62443 standard and setting up certification

Recap

- The impact of a large-scale hack can be catastrophic. To the EV drivers as well to the (international) grid.
- The more we make use of IT, the more risks we introduce to our grid if we don't have proper cyber security.
- Cyber security should be the standard, in legislation and in standards.
- Standards should be aligned international, to create a level playing field.


Elaadnl