REPORT

Impact of cyber-security risks on the Dutch national charge point infrastructure

National charging infrastructure

30 november 2021 | 65719 | Public

NATIONAL CHARGING INFRASTRUCTURE

Impact of cybersecurity risks on the Dutch national charge point infrastructure

30 november 2021 | 65719 | Public

Auteurs:
Hans Reterink
Klara Schure
Jill van der Bijl
Rianne Zivali – De Kievit

With the experts:
Marko Kruithof en Vincent Frijlink (WSP)

Conclusions and recommendations

Introduction: the energy transition and the Dutch national charging infrastructure agenda

The energy transition is a major challenge facing the Netherlands along with the rest of the world. This energy transition means that many carbon containing energy sources, such as petrol, coal, oil and gas will be replaced by electricity:

- road transport will be powered by electricity;
- homes and businesses will be heated by electric heat pumps and waste heat;
- industrial processes and hydrogen production will be powered by electricity.

The electricity needed for this is increasingly generated by sun and wind. These energy sources are sustainable but not always predictable and they are located in the entire electrical grid. In the future, local electricity storage by means of batteries, among other things, will also come into the picture.

The climate agreement of June 2019 sets out the measures to be taken by the Netherlands. These include that electric passenger cars will become competitive around 2025, the charging infrastructure for electric vehicles will be further rolled out (including any network modifications) and that by 2030 all new cars will be zero-emission. The Dutch National Charging Infrastructure Agenda is a long-term policy agenda based on this.

Cybersecurity of charge points

In this study we investigated the cybersecurity of the charging infrastructure. The target year was 2030. According to current expectations, there will not be 270,000 but 1.8 million charge points in the Netherlands by 2030 and this number will still increase further in 2030. The total peak capacity demanded by charge points will then be twenty times higher than it is today. The Netherlands is currently leading the world in the rollout of electric vehicles. In this way, the Netherlands can fulfil an important role in guaranteeing the preconditions for good and safe transport.

In addition to the possibility of using the charging infrastructure to provide flexibility when the stability of the electricity network so requires, there is also the downside, namely that sudden failures or disruptions in charging patterns can have a very large impact on the mobility of the Netherlands and the stability of the electricity network.

We have identified four scenarios in which a typical cyberattack would result in substantial disruption. Each scenario will develop in its own way and will have a different impact on society. The four scenarios are:

Scenario 1. Smart Attack by State Actor

This scenario assumes that smart charging has largely been introduced in the Netherlands. In this scenario, the back office system of a Charge Point Operator is attacked and, through manipulation of the smart charging possibilities, the charge points controlled by this back office system are deployed to throw the electrical grid of the Netherlands out of balance and to cause a blackout that could last several days. It is expected that this will be possible in the Netherlands from some time after the year 2025.

Scenario 2. Major Attack of a State Actor

In this scenario, a central information system is attacked, whereby the balance of the electrical grid is communicated via status information or via prices, after which the charging of connected charge points can suddenly be stopped. If the sudden drop in capacity exceeds 3,000 MW, there is a real risk of a national blackout in the Netherlands. This scenario is expected to be possible from around 2027 onwards.

Smart charging makes it possible to connect more charge points to the networks than without smart charging. This increases the load on the networks and makes them more susceptible to blackouts. Disruptions can also occur at the regional level with a smaller amount of power lost in a geographically concentrated area. Disruptions will also occur more quickly in regions where the networks are already under pressure.

On a national level, we expect that a blackout resulting from a successful attack on a single large Charge Point Operator will not be possible until several years after 2030. By that time, the increased peak capacity of charging stations and electric cars will also make such an attack more easily successful.

The impacts of scenarios 1 and 2 are very serious and similar. Mobility will be severely affected. Deliveries and freight services are disrupted and emergency services are severely hampered. A blackout of the electrical grid could completely disrupt public life; internet, mobile telephony, TV and all services dependent on electricity would also be disrupted, possibly leading to riots and deaths.

Scenario 3: Ordinary cyberattack

In this scenario, the back office system of a Charge Point Operator is for example attacked by ransomware, a script kiddie or anti-durability terrorists, among others. This causes the Charge Point Operator's back office system to fail and the managed charging stations may be down for days or weeks. This can result in customers of that particular Charge Point Operator being unable to charge. Depending on the customers of the Charge Point Operator, this could mean that emergency services or essential logistics services are partially out of action, or that many people in a particular city or region are unable to go to work because their car cannot be charged.

Scenario 4: Privacy attack

In this scenario, the customer data of loading sessions is stolen and published or misused in some other way. This may be done by state actors or criminal organizations. The aim is to make money or undermine trust. There is no direct effect on mobility or the electrical grid, but it can undermine confidence in the national charging infrastructure and thus the further growth of electric transport.

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.

The risks will also increase over time; in addition to the increasing use of charge points, unexpected chain and cascade effects are to be expected, and the peak capacities of electric vehicles and charge points will continue to rise. Although in this study we have confined ourselves to the Netherlands, the effects will probably be greater because charge point operators operate charge points in several countries, mobility also crosses borders and the electrical grid is linked at European level. Disruptions at lower grid levels can also have an impact on higher grid levels, especially if they occur in areas where the grids are already under pressure.

The scenarios show that the cyber risk lies primarily in the back office systems of Charge Point Operators and Smart Charging Service Providers. There is currently no legislation or regulations on the cybersecurity of these back office systems. There are guidelines for charge points from ElaadNL/ENCS which, because they are requested in public tenders, provide a clear standard for the charge points themselves, but only partly for the back office systems. Incidentally, the standards drawn up by ElaadNL/ENCS are mainly used in tenders for public charge points and hardly ever in purchases of private charge points (which account for 2/3 of the market).

The lack of legislation and regulations is explained by respondents as charge points being a new development that is mainly seen in the consumer sphere. But because charge points are almost all controlled by a back office system, the impact of such a system can be many times greater than that of a large electricity generator. A large electricity generator does however have standards and supervision from laws and regulations in the field of cybersecurity.

It is therefore highly desirable that adequate cybersecurity of the systems of the national charging infrastructure is guaranteed by legislation and regulations. Since the electricity network is linked at European level, it should also be put on the agenda at a European level that adequate security of the vital systems surrounding the charging infrastructure will be guaranteed.

There are currently several existing legislative and regulatory frameworks in the Netherlands that could form a starting point for achieving the necessary legislation. It is desirable that a situation is eventually achieved in which major parties in the Dutch charging infrastructure not only have a duty of care to guarantee the cybersecurity of the systems under their management, but are also being supervised in this respect and are required to report incidents.

It is also desirable that a segmentation of back office systems is implemented, so that the impact can be limited in the event of a successful cyberattack. This will bring it more in line with the standards keeping the balance in the power grid, which require that no disruption shall occur when a single element fails.

Contents

CHAPTER 1

Introduction

1.1 Introduction

The following assignment was formulated for Berenschot:

Provide the cybersecurity task force of the National Infrastructure Agenda security working group with an insight into what the risks and impact are when the cybersecurity of the charging infrastructure is not properly set up.

In any case, risks and impact for the following stakeholders must be indicated:

- *TSO*
- *DSOs*
- *CPOs*
- *EMSPs*
- *EV drivers*
- *Society*

This research addresses this assignment.

1.2 Reading guide

In chapter 2, 'Background and methodology', we discuss how we conducted the study. In chapter 3 we discuss the structure of the charging infrastructure and the expected developments and forecasts in terms of numbers. In chapter 4 we discuss the importance of balance in the electrical grid. In chapter 5 we discuss cybersecurity of charging points, including regulation. In Section 6 we identify four typical cyberattack scenarios and their impact on mobility, the electricity supply and society. The appendices cover the interviews, and a list of abbreviations.

In this report we have tried to make the sometimes technical aspects of electricity and cybersecurity understandable for readers without the relevant specific technical background. Where possible, references have been made to the relevant written sources.

CHAPTER 2

Background and methodology

2.1 The challenge

Whereas there are currently around 270,000 charge points, this is expected to rise to 1.8 million by 2030. This is an infrastructure in which many parties are active with ICT systems working together. As a result, multiple cyberattack surfaces are possible for attack or disruption. The impact of a (targeted) disruption of the infrastructure can be very great. Both upstream (to the DSOs and TSOs) and downstream (via electric cars to mobility and to the shutdown of substantial parts of national transport to the disruption of other vital sectors).

Investigating the risks and impact of cybersecurity on the charging infrastructure is a task that has several dimensions. We believe that a good analysis of the potential risks and impact of cybersecurity is essential to raise awareness and to identify potential problems relating to electric driving and the charging infrastructure in good time. Insights from various fields of knowledge are needed to create an integrated picture. This could include knowledge of cybersecurity, the market and the ICT infrastructure surrounding charge points, as well as the social consequences of power failures, transport and other vital sectors. In addition, an open eye must be kept for developments that have a limited impact today but could pose a substantial threat in a few years' time. Forecasts towards 2030 are leading in this respect. The future cannot be predicted, but where possible and necessary we make well-founded assumptions in order to provide quantitative estimates.

In this report, we outline the risks and impact for the various stakeholders and also provide advice and tools to further develop the insights obtained into recommendations and standards.

2.2 Starting points for this research

- The situation in 2030 is taken as a starting point. This means, among other things, 1.8 million instead of 270,000 charge points, concentration, but also new entrants in all submarkets.
- The current situation without additional standards, regulations and measures between now and 2030 is assumed.
- The starting point is a further developed smart grid along the lines of ECISS.
- The development of the market for charge points is based on current forecasts.
- For the control limits, the current norms of the TSO and DSOs are used.
- The report is based on the currently known attack surfaces and modi operandi of cyber actors.
- For probabilities of cyberattacks and possibilities of attack surfaces, expert judgement is assumed. In this, it is assumed - in accordance with current reality - that despite guidelines such as those of ElaadNL/ENCS, opportunities for cyber-intrusion still remain. Moreover, the aforementioned ElaadNL/ENCS guidelines are only applied to public tenders, while private home and work charging points represent a larger volume.
- Cyberattacks are active, deliberate attacks on an ICT system[1].

2.3 Methodology

For this research, we conducted a document study and interviewed experts. The purpose of the document study was to get a better idea of the current knowledge on cybersecurity of charge points. The documents and information for the study were obtained through desk research from public sources or sent by interview partners. We spoke with scientific experts from technical universities in the field of charging infrastructure and power grids and experts with relevant functions working at CPOs, eMSPs, TSOs, DSOs, and charging point suppliers, among others. In addition, we spoke to representatives of the research organizations ElaadNL and ENCS.

Finally, there was also a meeting at which we talked to experts Marko Kruithof and Vincent Frijlink about the possible cyber risks that we identified on the basis of the document study and interviews. During the session, the risks were further explored and a number of additions were made to the risks that had been formulated up to that point.

The report was compiled on the basis of the document study, the information obtained from the interviews and the input from the expert meeting. Where possible, reference is made to the sources of information.

CHAPTER 3

National charging infrastructure

Before we look at the cyber risks of the national charging infrastructure, we will first examine its structure. In doing so, we look primarily at the technical structure and connections. Ownership may differ: a charge point may be owned by a private individual, but will often be technically controlled by a CPO who will also provide back office systems and apps, especially if smart charging becomes the norm in 2030.

3.1 Simplified build-up of charging infrastructure

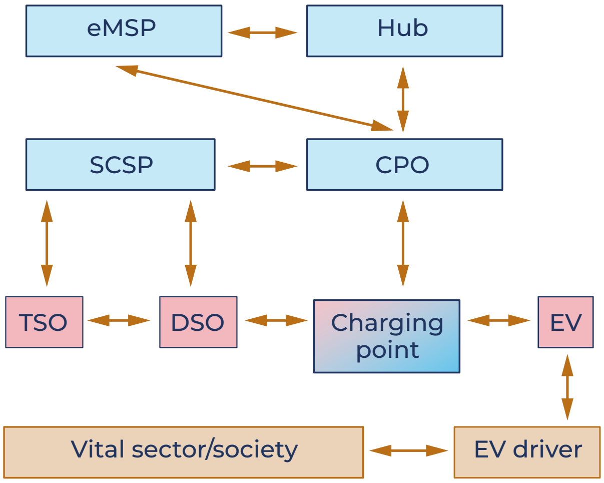


Figure 1: **Simplified charging infrastructure structure.**

The above diagram can be read as an introduction to the charging infrastructure. A more complete diagram is shown in section 5.2(System overview charging infrastructure).

The points of leverage for cybersecurity are mainly in the blue areas: the charging point itself and the ICT infrastructure of the Smart Charging Service Providers (SCSPs), the Charging Point Operators (CPOs) and the e-Mobility Service Providers (eMSPs). These consist of both various applications and their links, implemented with OCPI for example. The number is currently large, for example there are already about 50 eMSPs for all the Dutch charge points. An important point of contact is also the Smart Charging Service Providers (SCSPs).

SCSPs control the set-up and operation of the so-called ‘smart grid’, in which the purchase and return of electricity between the charge points and the electrical grid is controlled, also based on peaks and troughs in the consumption in the electrical grid itself. Hubs are also known as Roaming Service Platform (RSP) and take care of the mainly financial settlement of charging sessions between CPOs and eMSPs.

The red areas show the supply of electricity, from the high-voltage grid managed by TenneT TSO, via the medium and low-voltage grids managed by the DSOs, to the physical load point. Cyber disruptions at the load point via the CPO or eMSP, or in the future via the SCSP, have the potential to cause major disruptions at the DSOs and TSO. The extent and speed of the disruption are essential. Disruptions in these areas are also associated with a potentially major impact on society. This is discussed in more detail in Section 6.

The orange areas are relevant in determining the direct impact: the effect on the EV driver and on society, with the emphasis on vital sectors. Disruption of only these areas can also have a major impact on society. More on the impact analysis can be found in section 6.

3.2 The expected growth of EVs and charging infrastructure towards 2030

We have made analyses based on data from sources including ElaadNL. Figure 2 shows the forecast demand for electricity from mobility in the year 2030, for passenger vehicles, public transport and freight. The current demand is approximately 2,000 GWh for mobility[2] (including trains). In 2030, demand for electricity for mobility will be almost 11,000 GWh (about 9% of total national consumption) in the medium scenario (excluding trains)[3]. It can be seen that - besides passenger transport - delivery vans and freight transport will also have a substantial demand for electricity in 2030. The electricity demand of public transport buses will then be close to maximum, but will account for a relatively small share of the mobility sector.

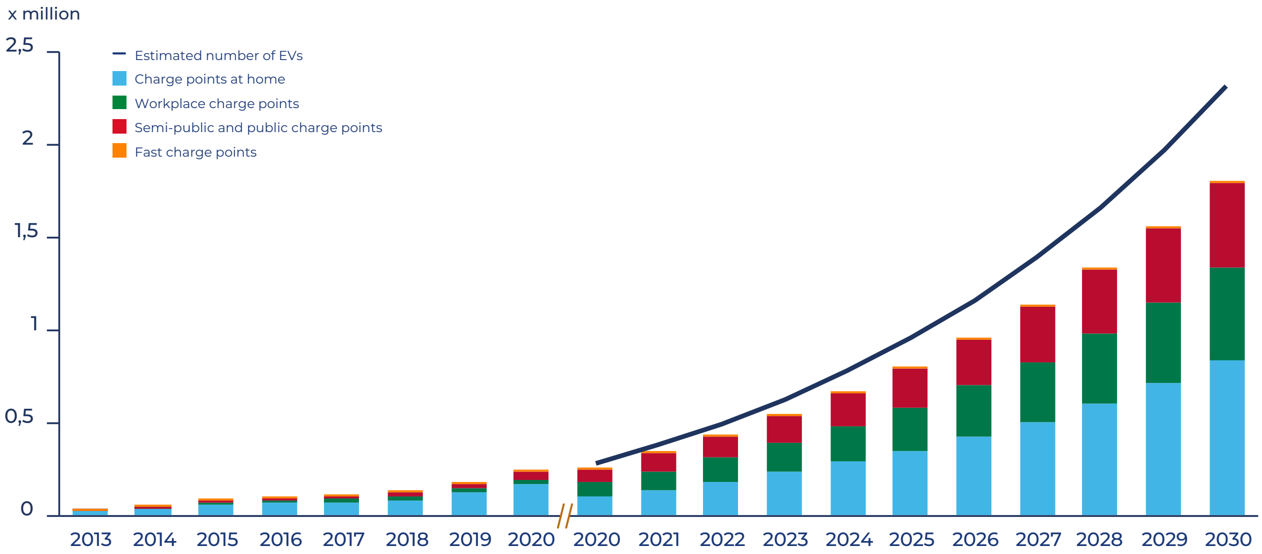


Figure 3: **Number of electric passenger cars and charge points. Historical development up to and including 2020: RVO 2021. Forecast 2020-2030: ElaadNL outlook 2021.**

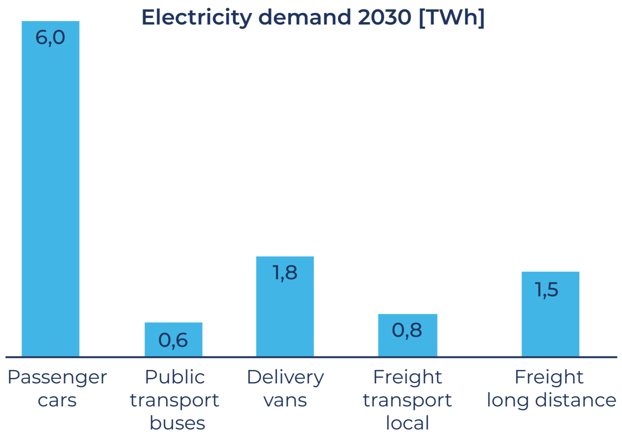


Figure 2: **Forecast of electricity demand per modality in 2030 based on forecasts from the various ElaadNL outlooks for the medium-growth scenario and a constant electricity consumption per type of vehicle.**

3.2.1 The development of electric passenger cars

The policy of the Dutch government is that by 2030 only emission-free passenger cars will be sold[4]. Similar goals are being set internationally: President Biden has stated that by 2030 half of new cars in the USA must be electric[5].

It is expected that there will be 1.8 million charge points[6] in the Netherlands in 2030, and an expectation of approximately 2.3 million EVs. Figure 3 shows the prognosis for the number of electric passenger cars and various charge points by 2030. The historical data do not exactly match the forecast, as can be seen from the differences between the two 2020 points. The number of home charge points has been historically represented on the basis of the percentage of EV drivers who indicated that they were charging at home in 2020, which gives an estimated 169,000 private charge points[7]. This while only about 30% of households have their own driveway, and about 47-59% of kilometers are charged at home (numbers vary between the 2020 and 2021 surveys)[7,8]. On top of that, 16-23% are charged at home at a public charging station. Presumably, the percentage of private charging points will decrease in the future, as those with their own driveway now seems overrepresented.

Figure 3 shows the historical development up to and including 2020 and the prognosis for 2030. It can be seen that in 2030 the number of charge points is forecast at 1.8 million, and the number of EVs at about 2.3 million.

Figure 4 shows how the connections to charge points are distributed on a weekday, divided among the various types of charge points[11]. In terms of kWh, this picture would look different because there are not the same number of all types of charge points. During the week, the need for charging is greatest. At home, charging is mainly carried out at around 18:00 hours. In time, smart charging (and an SCSP) will be required to prevent overloading of the low-voltage grid at this time.

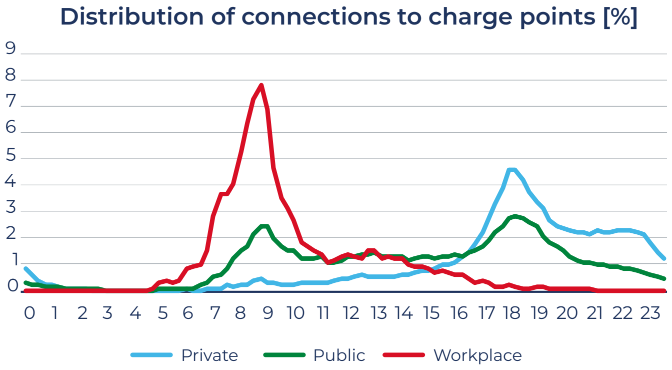


Figure 4: **Number of connections (in percentages!) per different types of charge points. The vast majority (~75%) of the demand is met by home charging points. The peak in the number of new connections is around 6 pm. In absolute terms, the need for charging is greatest in the evening, as most of the charging demand is met by the private profile.**

Although only about 30% of households have their own driveway, in the year 2021 no less than 59% of the need for charging is met at home (privately), of which 8% via a socket outlet and 51% via a home charging point. In 2020, the figure was 47% (of which 7% was via a socket outlet and 40% via a home charging point). The corona pandemic plays a role in the large differences between the figures for 2020 and 2021. The morning peak is at public charge points near the workplace. The evening peak is currently mainly at home charge points, but in the future this peak will increasingly be at public charge points.

The total charging demand for passenger cars in 2030 is expected to be 6,000 GWh12. The expected development of peak demand [9] is shown in Figure 5, which indicates that peak demand in 2030 will be around 2,000 MW.

All these forecasts do not yet take account of smart charging. Smart charging will become necessary in the future to cushion peaks, but it will also pose an additional vulnerability if it is disrupted by a cyberattack. The vulnerability is often greatest during a peak. A large part of the peak demand in the evening is met by private charge points. As shown in Figure 4 also a peak in the morning. Most of this peak is at work stations. An estimate based on the available data is that peak demand in the morning will be approximately 35% of the peak demand in the evening. This means that peak demand in the morning in 2030 is expected to be around 700 MW. The main difference with the evening peak is that most of this will be charged at public charge points.

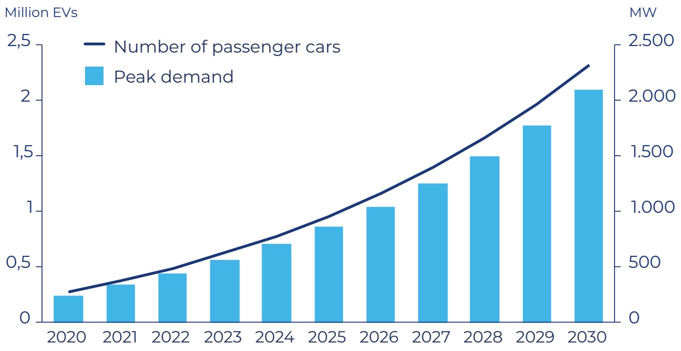


Figure 5: **Development of peak demand together with the number of passenger car EVs. The peak demand occurs at the beginning of the evening around 19:00h.**

3.2.2 The development of vans and freight transport

In addition to the growth in passenger cars, the demand for electricity from delivery vans and freight transport will also grow strongly. Figure 6 that - without smart charging - the peak demand for electricity from delivery vans is expected to grow to 3,300 MW in 2030. The peak demand of delivery vans and freight transport will be more or less simultaneous with the evening peak for electric passenger cars. This is based on an estimate by ElaadNL[13], extrapolated from the growth in the number of electric delivery vans to 2030. Although the number of delivery vans and freight transport is considerably smaller than the number of passenger vehicles, peak demand is high. This is because the consumption of delivery vans is relatively high and peak demand is concentrated more in the evening. With smart charging, peak demand can be reduced to 40% of peak demand without smart charging, or 1,300 MW. Of this total, 50% is expected to use private and public charge points at home and the remainder at the company's own charge points.

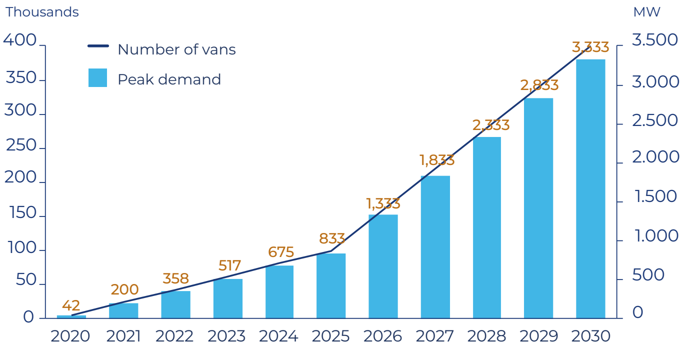


Figure 6: **Projected growth of electric delivery vans 13and associated peak demand, without smart charging and without major increase in capacity of charge points (interpolation between 2020, 2025, and 2030).**

Electric freight transport (excluding delivery vans) is also expected to grow strongly[3]. The charging profile will be different from that of cars and delivery vans, and there will be more charging in between using fast chargers. For freight transport charging points we assume an average of a 50 kW connection (for an 'ordinary' charging point) to an average of 650 kW for a fast charger (at service stations or special truck rapid charging locations)[3]. The peak capacity expected for freight transport in 2030 is around 800 MW, rising sharply to 2,900 MW by 20353.

3.2.3 Development of peak power and coupled power of passenger cars and vans

If we combine the development of the expected peak demanded capacity in the previous two sections, we arrive at the following totals. These totals cover the expected peak demanded capacity in the year 2020, the reference year 2030 and the year 2025. On top of this comes the capacity for freight transport, as stated in the ElaadNL forecasts. This leads to the following table.

Year	Passenger car peak power (MW)	Van peak power (MW)	Freight peak power (MW)	Total peak power (MW)
2020	250	40		290
2025	860	830	90	1800
2030	2.100	3.300	840	6.300

Table 1: **Total peak power per year**

This total peak capacity of 6,300 MW in 2030 is just under a third of the current maximum national capacity of about 21,000 MW.

In terms of power (amount of energy per second), there are considerable differences between existing charge points. For a single-phase connection, a typical home charge point is around 3.7 kW, and for a typical 3x25A three-phase connection, due to electrical engineering requirements, it is 11 kW. These are the capacities most people are currently charging at. Most sessions charge at around 3.7 kW[10].

In 2018 this was the case in more than 70% of cases, and in 2020 it was still the case in around 35% of charging sessions at public charging points. At public charging points, 11 kW is currently the most common, accounting for around 30% of charging sessions in 2020. All new electric car models have a 3-phase charger on board. Previously, this was sometimes a single-phase charger, but this appears to have been abandoned. Only 5% of the sessions take place at higher power, but also 5% at lower power.

At the moment, 11 kW charge points are the most popular option. The forecast for the number of charge points in 2030 in the latest ElaadNL outlook[11] is 1.8 million. With an average maximum capacity of 11 kW[12] per charge point, this means a installed capacity of 18,700 MW in 2030. This does not mean that this capacity will be used for charging simultaneously, because not every charge point will be occupied and not every plugged-in car will have a maximum charging requirement.

A closer study of the data from some of the public charge points in the Randstad area and the northwest of the Netherlands[13] shows that an average of 14-20 kWh is charged per session. In 2020 (at the time of the corona pandemic) 70 GWh were charged by 280,000 EV drivers, at 11,000 public charge points during 4.3 million sessions. Per EV driver, this means an average of 15 sessions at a specific charge point of ~16 kWh per year. On average, over 6,000 kWh were charged per charge point. In 2019, the average capacity per public charge point was 5.1 kW. That will have increased a bit since then, due to more 3-phase charging (which gives 11 kW). At 7 kW, that means a charging session takes over 2 hours. In 80% of cases, a car is at a charge point for 6 hours, and on average 8 hours for all charging sessions, including the peaks at the bottom and top. At charging points at work, charging time is 5.5 hours for 80% of cases, with an average of 6.6 hours. At home, cars are connected the longest, with 10.3 hours for 80% of cases, and an average of 12 hours. Of these, about 25% are expected to be actively used. 75% of miles are charged at home. That percentage is expected to decline in the future, as the overrepresentation of households with their own driveway is expected to decrease. There are significant differences between regions. Use of a charge point varies from 4,881 kWh/year in SGZH (18 municipalities in the province of Zuid-Holland) to 8,356 kWh/year in Utrecht.

The capacity of passenger car batteries that are connected at any one time can be derived from the charging profiles and the degree of utilization. The utilization rate of charge points (the degree to which a charge point actually charges an EV) varies considerably, but is between 25-40% for public and private charging infrastructure. The utilization rate will be higher on average during peak demand. The utilization rate during evening peak demand is not exactly known. Assuming that peak utilization is somewhat higher than average, we estimate it to be 50%. The peak capacity demanded is then around 2,000 MW. Including those cars that are not actively charging, the total connected capacity of passenger cars will then be about 4,000 MW.

In addition, there is the coupled capacity of delivery vans, which we have also estimated on the basis of peak demand, assuming it to be 150% of peak demand. In the evening, vans' peak demand is estimated at 3,300 MW. Assuming an additional capacity of 150%, this gives a connected capacity of 5,000 MW for vans. For passenger cars and delivery vans together, this would then be 4,000+5,000 = 9,000 MW. These have the same evening demand profile. On the same assumptions, as early as 2025 an aggregate coupled capacity of 3,000 MW for cars and delivery vans will be reached, which is equal to the control limit of the European grid.

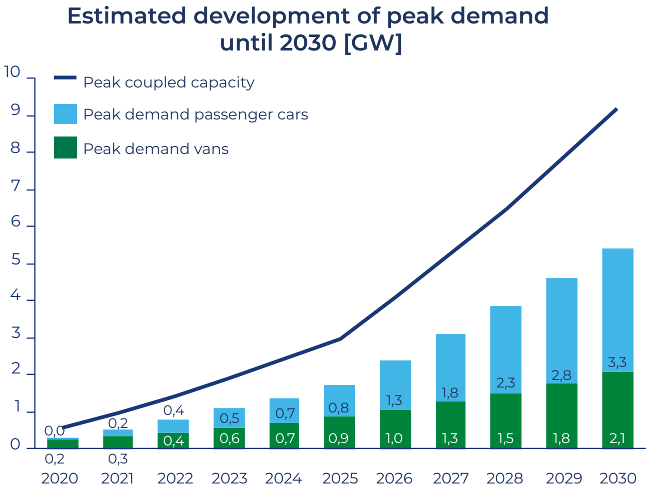


Figure 7: **Estimated development of coupled capacity of cars and vans during evening peak hours (for vans, only filled in with known forecasts).**

For the possible impact and risk of a type 2 cyberattack (see Chapter 6), the peak demand is particularly important because this shows how large the immediate quick-impact capability is if a cyberattack takes place during peak hours.

3.2.4 Different connection types

The table below shows that there is a variety of connection types per grid operator. The table shows the small-user connections, but does not include the large-user connections (3x80A and larger). The proportions between the various connection types also vary between grid managers.

The connections for the first three rows (1x25A, 3x25A and 1x35A) are basic tariff connections, above them consumers have to pay more for the fixed annual network costs. This is why only 3.4% of consumers choose another, usually heavier connection. With 1x35A a maximum of 8 KW can be supplied, with 3x25A a maximum of 17 kW. It can be seen that with this tariff structure, a 22 kW charging capacity is possible for very few consumers.

Bottlenecks are expected in the connections to industrial estates, particularly for transport companies with several electric trucks. Some delivery vans charge at private charge points. Demand for public charging points for delivery vans is expected to increase, particularly in the Randstad, due to the lack of private property or driveways with charging facilities. The number of charging points will grow rapidly from 2025 onwards. Although delivery vans drive many kilometres and will need to charge relatively often, the number of required charging points is still limited compared to passenger cars.

AConnection type	Min. duration 50kwh	Enexis	Liander	Stedin	Total	Fraction
1*25A	13 uur	531.906	1.126.192	152.151	**1.810.249**	**21,9%**
3*25A	4½ uur	823.655	1.097.822	323.397	**2.244.874**	**27,2%**
1*35A	7 uur	1.088.888	1.215.387	1.617.748	**3.922.023**	**47,5%**
Rest		191.586	20.866	69.990	**282.442**	**3,4%**
Totaal		**2.636.035**	**3.460.267**	**2.163.286**	**8.259.588**	**100%**

Figure 8: **Distribution of connection types by grid operator.**

3.2.5 Increasing charging capacities and smart charging

Charge points move towards a situation where home charge points can generally handle a maximum of 11 kW[14]. For charging points on the road, a development is visible whereby the capacities for fast charging are based on direct current (DC) and are becoming increasingly higher, in the short term up to 350 kW for passenger cars[15]. The CharIN consortium (which also developed the widely used CCS plug in Europe) is now working on a charging point and plug for trucks with a capacity of 4,500 kW[16].

Entso-e, the association of TSOs in Europe, calls for rapid action to roll out charge points with the option of smart charging so that they do not need to be replaced later. From the perspective of the European electrical grid, it is desirable that the purchase and redelivery of electricity can be coordinated with the balance of the grid and the production of electricity by sun and wind. Smart charging can therefore play a role in maintaining the balance of the electrical grid, and is therefore extremely important for the energy transition. Before the 'smart grid' can get off the ground, however, a number of hurdles still have to be taken:

- It must be made clear how the benefits of smart charging can also reach the EV driver[17].
- The European standard for charging: the combined charging system standard (CCS) will have to be further developed, including the publication of ISO standard 15118-20, so that full Vehicle to Grid smart charging is possible and can be built into EVs, charge points and SCSPs. It is expected that this can be realized in or after the year 2025[18] [19]. Around this time, the application of smart charging will become increasingly essential to enable charging infrastructure within the current infrastructure of the TSO and DSOs without significant reinforcement.
- The conditions under which the various data required for a smart grid are exchanged must become clear. Not only the technical standards, but also the ownership and value of the data, as well as its privacy and security.

> *"As EVs will be increasingly integrated in the energy system, security from cyberattacks will also represent a key issue, so as to avoid data being intentionally manipulated to generate negative impacts on the system balance. Moreover, control systems of EV-charging should be designed in such a manner that data failure or manipulation does not lead to a substantial change in system balance (cyber-resilience) and emergency situations are properly managed (e. g. restoration after black-outs). "*
> ENTSO-E Position Paper - Electric Vehicle Integration into Power Grids, 31 March 2021.

It is clear that smart charging will be necessary to have a stable electrical grid in Europe even in 2030. In a position paper by European TSOs: Entso-e states that TSOs have an important role to play here and that an uncontrolled charging process will present 'significant challenges' to the electricity network[20]. And that through smart charging, the peak in the evening between 16:00 and 22:00 can be reduced and postponed to the night and afternoon, when prices are also lower[21].

Of course, smart charging also requires SCSP parties to make the charge points 'smart' and take account of the balance in the grid. Several parties are preparing to play the role of SCSP in the future: car manufacturers, energy suppliers, CPOs and eMSPs. Time will tell which parties will fulfil the SCSP role and in what combination.

3.3 Global expectations

3.3.1 Peak load of EVs

The International Energy Agency expects that in the year 2030 9.6% of the peak load in the evening in the European Union will come from the charging of electric cars in the sustainable development scenario, which assumes uncontrolled charging[22]. (In the Netherlands, this percentage will be higher in 2030 and around 30% because the adoption of electric driving in the Netherlands is higher than the average in Europe).

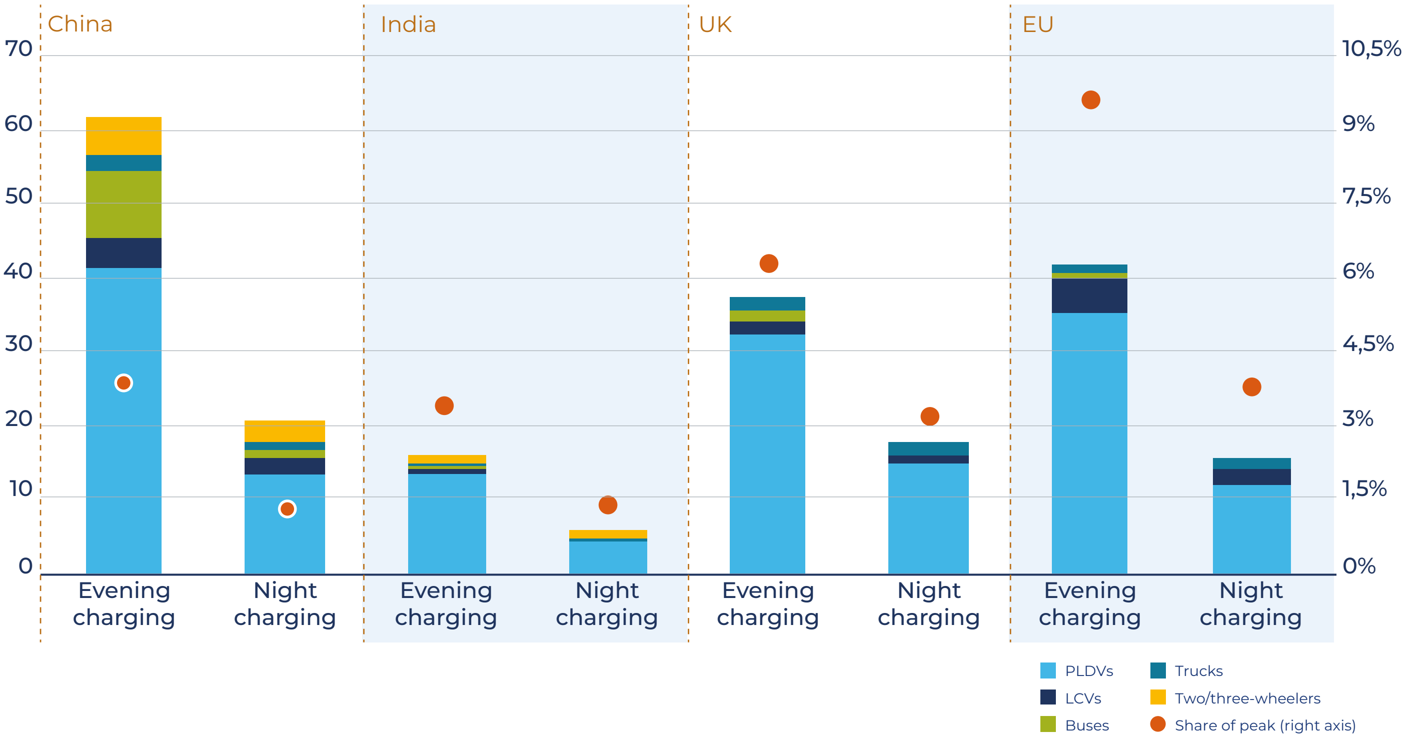


Figure 9: **Load imposed by EVs on each continent in 2030, with percentage of peak load (orange spheres).**

3.3.2 Batteries

The batteries used in electric cars will also being developed further. This also has an impact on the cost, since the battery accounts for[23] about 35-45% of the cost of an electric car. Between 2010 and 2020 batteries have become almost 90% cheaper[24]. In addition, new technologies are constantly being developed, leading to larger batteries with lower costs, higher performance and less use of scarce metals[25]. In addition, at the top end of the market already the first 30% of the battery can be fast charged with direct current and a capacity of 250 KW[26]. It is expected that by 2030 the development of current Li-ion technology will have reached an end point, with EVs being able to travel an average of 350-400 km on a single 70-80 kWh battery charge.

3.3.3 Number of private charge points per country

The number of charging points in the Netherlands is relatively high: in 2019 it was 4% of the number of private charging points worldwide [27]. The number is based on an estimate, given the percentage of EV drivers who indicated they could charge at home 8.

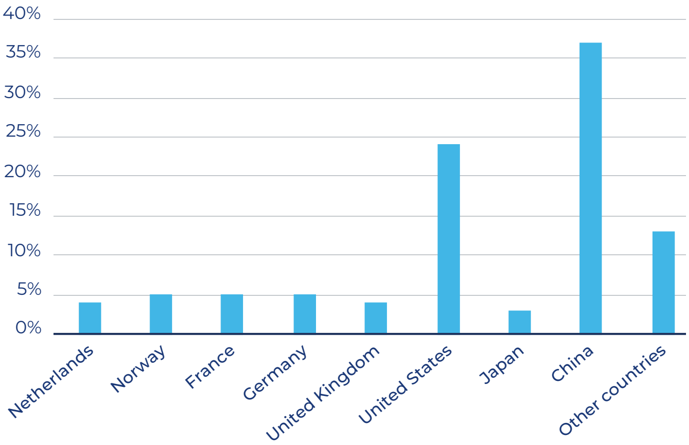


Figure 10: **EV slow charging points by country in 2019.**

3.3.4 Public charging stations

The Netherlands has a relatively large number of public charge points: 8% of the number of public slow charge points worldwide. [28]

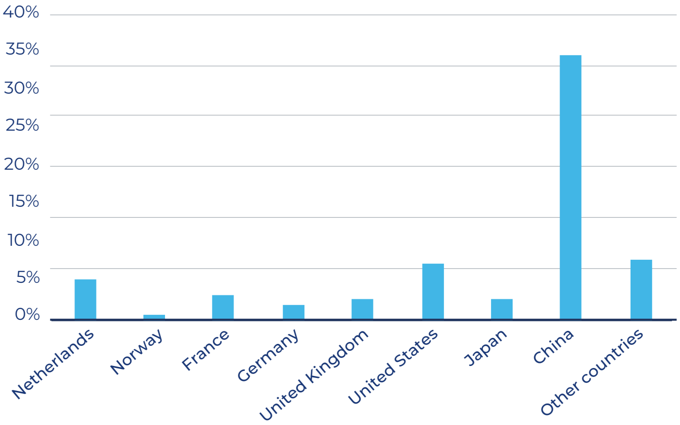


Figure 11: **Public slow charging stations by country in 2019.**

3.3.5 Rapid charging stations

The Netherlands, on the other hand, has relatively few fast charging stations[29]: their importance is expected to increase by the year 2030, especially given the possibilities of modern EVs to charge with a capacity of around or above 250 kW[30]. Extrapolation of expectations shows a fivefold increase in the number of fast chargers by 2030. The fast chargers are mainly installed by car manufacturers, independent and fuel operators, and restaurants and car dealers[31].

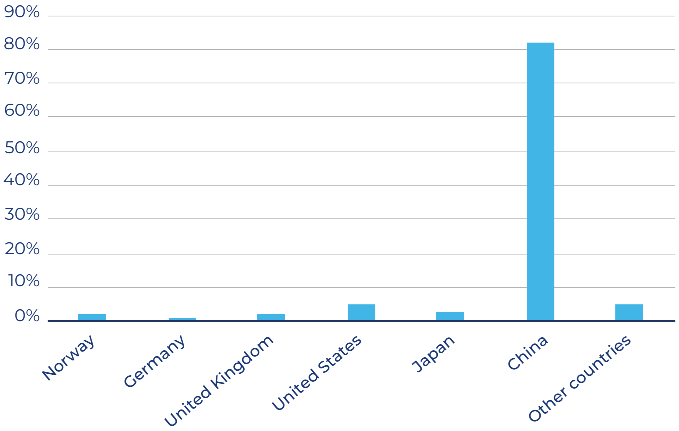


Figure 12: **Public fast charging points by country in 2019.**

3.3.6 Charging point providers and CPOs

There are a limited number of CPOs and charging station manufacturers active in the Netherlands.

Larger charging pole manufacturers include:

- Alfen
- ChargePoint (USA)
- Ecotap
- Enovates (software and hardware for charge points)
- EV Hub
- EVBox (part of the French energy company Engie)
- Ratio
- Schneider
- Webasto

Larger CPOs include [32]:

- Allego
- BP with Volkswagen
- Eneco e-Mobility
- Engie
- FastNed
- Shell Recharge (incl. Newmotion and Ubricity)
- Vattenfall

CHAPTER 4

Electrical grid stability

In order to calculate how important an unplanned disruption of the national charging infrastructure is for the electrical grid (due to a cyberattack, for example), we discuss the control limits of the electrical grid in this section.

4.1 Introduction: the balance in the electrical grid

The Dutch (and European) electrical grid must be permanently ‘in balance’ to ensure uninterrupted supply. In balance’ means that at any given moment the same amount of electricity is being supplied as is being used. This is no easy task: for example, nowadays the peak is in the evening before going to bed and there is a dip in the middle of the day. As a result, in the Netherlands both consumption and production vary between 5,000 and 21,000 MW[33] in a day.

In the Netherlands this balance is monitored by TSO TenneT which ensures that the same amount of electricity is produced as is consumed at any time of the day, by means of various types of quarter-hourly contracts with electricity producers. TSO TenneT does this by paying close attention to the frequency of the electrical grid. If the electrical grid is in balance, the frequency is exactly 50 Hz: the current moves back and forth 50 times per second. If the frequency drops below 50 Hz, then there is not enough power being supplied (the generators cannot keep up the pace), and if the frequency rises above 50 Hz, too much power is being produced.

Technically, the Dutch electrical grid is connected to the countries around us to form the European electrical grid. If too much or too little electricity is produced in the Netherlands, electricity can be exported to or imported from other countries. All the TSOs in Europe jointly monitor the balance in their connected and synchronous electrical grids. The TSOs in Europe have united for this purpose in the Entso-e organisation, which makes precise agreements on the obligations of all TSO members in legal documents.

4.2 Control limits for the purpose of this investigation

In order to interpret the impact of disruptions to the Dutch charging infrastructure caused by cyberattacks, we have also looked at the chain effects upstream: the impact on the Dutch electrical grid.

The International Energy Agency expects that about 9.6% of the peak load in the evening will be due to the charging of electric cars in the year 2030 in Europe.[34] Using this figure as a benchmark, the expectation is that such a proportion can be handled well in 2030 if we look at regular consumption during the day. But if we look at the peak capacity we calculated ourselves (6,300 MW in 2030), this could be around a third of the Netherlands’ total peak capacity. The difference can be explained by relatively more electric cars in the Netherlands than in Europe as a whole. This shows that the challenge for the National Charging Infrastructure is significant.

If we also look at the possible impact of cyberattacks, we must also look at possible disruptions in a period of seconds and minutes. Here are three examples to illustrate this.

1. The first example concerns the limitations resulting from the limited transmission capacity of the European grid. The recent separation of the European electricity network on 8 January 2021 shows that a failure can spread in just 43 seconds from the initial failure of a power line in Croatia to the separation of the European electrical network into two parts.[35] This shows that the failure of a single power line can increase the load on the adjacent power lines, which then also fail, etc. After the separation, there was a power shortage of 6,300 MW in the northwestern section and a power surplus of 6,300 MW in the southwestern section. By switching off major consumers in Italy and France and disconnecting a power station in Turkey, among other things, the impact was limited and the two sections could be reconnected after an hour.

   This example shows that transport capacity can also be a limiting factor. This applies on a European scale, but also within the Netherlands. TenneT can solve transmission problems in the high voltage grid in the Netherlands by means of so-called ‘congestion management’, for example by reducing the supply of electricity in one part of the country and increasing it elsewhere, thus reducing the demand for transmission capacity.

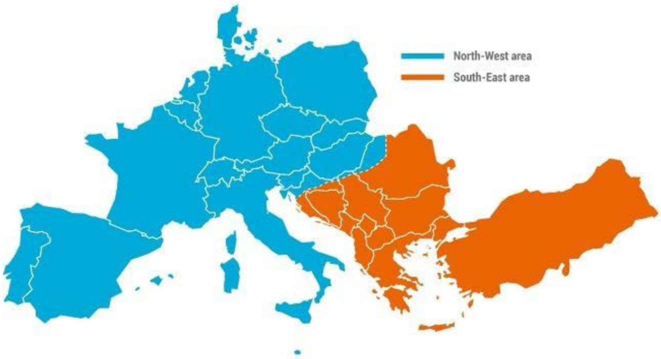


Figure 13: **Splitting the European electricity network into two parts on 8 January 2021.**

2. A second example of the speed at which an outage can occur is the outage of electricity on 9 August 2019 around Little Barford in England. Following a lightning strike to a transmission line, a cascade of generator and wind turbine outages followed until a minimum frequency of 48.8 Hz was reached after 76 seconds at a 1,700 MW outage. As planned in such situations, power was then cut off to customers, leaving 1.1 million customers without power. This helped bring the frequency back to 50 Hz after five minutes, but customers were without power for between 15 and 45 minutes.[36]
3. The ability of state actors to attack a power grid is demonstrated in the example of the attacks on DSOs in Ukraine on 23 December 2015. In a coordinated and long-prepared cyberattack, three DSOs were attacked, and the control of the power grid using the SCADA control systems was taken over by the attackers. As a result, thirty 35kV and 100kV substations were shut down for 3 hours, leaving 225,000 customers without electricity.[37, 38]

In this study we will therefore focus primarily on the potential impact of cyber disruptions on rapid disruptions in electricity demand (or supply) from charging points on the electrical grid, as these can have the greatest potential impact by far.

4.3 Management of rapid disruptions in the power grid

The Dutch TSO TenneT has three types of pre-contracted, rapidly available capacity at its disposal to deal with rapid disruptions in the electrical grid in the Netherlands[39]:

1. The Frequency Containment Reserve (FCR). This reserve is automatically activated within a few seconds and must be able to deliver full power in 30 seconds and hold for 15 minutes. With a deviation of 0.2 Hz from 50 Hz this is used to its maximum.
2. The FCR of the Netherlands is purchased together with the TSOs of Austria, Belgium, Germany, western Denmark, France, Slovenia, and Switzerland in a daily auction for the next day. The FCR of the Netherlands has to be delivered within the Netherlands, with a maximum for the power to be delivered across the border. The FCR of the Dutch TSO: TenneT is set at 114 MW for the year 2021.

   The Automatic Frequency Restoration Reserve (aFRR). This can be activated by the TSO and must be able to deliver the contracted power within 15 minutes with a 7% increase per minute. The aFRR of the Dutch TSO TenneT has been set at 290 MW both upward and downward for the second half of the year 2021.
3. TenneT also has access to the 'Manual Frequency Restoration Reserves directly activated' (mFRRda). This has been set at 1015 MW upward and 760 MW downward for the second half of 2021. These reserves can be called up manually in the event of incidents.

However, the Netherlands is also part of the European electricity network which is managed by the TSOs that are members of the European association ENTSO-e. The frequency is kept as close as possible to 50 Hz: an excess of more than 0.2 Hz is considered critical.[40] The power available in practice is determined per 15 minutes and varies per day.

TSO TenneT assumes a maximum reference incident of 3,000 MW, both downwards and upwards.[41]

If we consider this, we should actually also consider the effect of a simultaneous cyber disruption in Europe, because systems of CPOs, eMSPs and SCSPs are often cross-border. A cyber incident will also be able to manifest itself across borders.

The Netherlands' electricity demand is expected to be around 140,000 GWh in 2030, an increase of approximately 30% compared to 20202. As energy generation becomes more sustainable, the variety of ways in which electricity can be generated will increase. For example, the capacity of offshore wind energy is expected to have risen to 20,000 MW by 2030.[42]

Another limitation lies in the number of international cross-border connections from the Netherlands: this involves a total of approximately nine interconnectors with a total capacity of about 21,000 MW.[43] The load on these interconnectors vary. Sometimes the sum of the capacity of a transfer between two countries exceeds 3,000 MW.[44]

4.4 A fragile and under-resourced distribution network

As a result of the energy transition, the electrical grid will become both more important and more unstable. This is because both supply and consumption will become more decentralised with less influence from the national TSO. If there are 1.8 million charge points in 2030 and people connect their cars to the charge point when they return home and demand power, consumption at peak times in the evening around 6 p.m. will increase in the future. The challenge for balancing the electrical grid is also increasing because the supply of electricity is also increasingly dependent on renewable sources that are weather dependent. For example, it is expected that by 2030 the total capacity of wind energy in the Netherlands, at 18,300 MW, will be close to the country's peak electrical consumption.[45] But of course there will also be days without wind and little sun and electricity still needs to be supplied.

The current size of the electricity distribution network is nowhere near enough to make the energy transition possible. This is already leading to bottlenecks, scarcity and a situation where consumers will have to wait longer for their charging stations to be connected[46]. The DSO Alliander reports that in 2050 the demand for electricity will be 2.5 to 6 times higher than the current capacity available[47]. In a city like Amsterdam, this will largely be due to a sharp increase in the number of charge points, combined with the supply of power from solar panels and additional demand for power from new companies and data centres, for example. This can be partly solved by also using cables that are currently kept 'in reserve' in case of a failure in another cable, but this also means that a cable failure will lead much faster to a disruption in the energy supply to citizens and businesses.

The probability of an outage occurring is increased if transmission capacity previously held in reserve for use in the event of an outage is used for regular transmission. On 2 July 2020, the Dutch Authority for the Financial Markets decided that TSO TenneT was permitted to do so for a part of its grid in the north of the Netherlands: the failure reserve may be used for the regular transmission of sustainable electricity in the interests of energy transition[48]. Consequently, the 'N-1 redundancy' no longer applies to this part of the grid.

The supply of energy is also shifting from large generators to a variety of decentralised generation of different types of renewable energy, the capacity of which can vary greatly. In the Netherlands, these are mainly

- solar panels; and
- wind turbines.

The consumption of electricity is increased as fossil energy sources are replaced by electrical energy for:

- industry;
- heating;
- transportation.

These three additional needs for electrical energy are different during the day but can be reasonably predicted under normal circumstances. Of course, they make the dependency on electricity even greater than it already was. If smart charging becomes necessary to stay within the capacity of the electricity network, this creates an extra vulnerability if the smart charging is switched off or no longer works properly.

Additional measures may also be required to ensure grid stability if electricity is generated almost entirely from renewable sources. This may involve reactive power. We will not consider this issue in more detail in this study.

In addition, cyber risks are magnified by the fact that a multitude of consumer devices are connected via the Internet to a back-office system that can switch these devices on and off and thereby create a substantial power demand or supply.

Think for example of the following consumer IoT devices:

- charge points;
- smart thermostats and Home Energy Management Systems (such as TOON);
- heat pumps;
- solar panels;
- washing machines;
- Furnaces; and
- batteries for local electricity storage.

4.5 Impact of the charging infrastructure on the electricity networks

The increase in controllable and relatively flexible demand capacity provides great opportunities to help keep networks stable in the future. If, for example, smart charging is applied, peak demand will be reduced and the demand for electricity will be spread over a longer period. This will allow more power to be connected to the electrical grids. However, this smart and controllable capacity also has a downside: when the controllable capacity is suddenly deployed in a way that is contrary to what is required to maintain the grid balance. If smart charging is assumed in the future and suddenly does not work, the peak demand in the evening will be much higher than it would be with smart charging. If the networks are no longer able to cope with this and are much fuller than can be anticipated with such a peak demand, this could lead to disruptions. In the analysis below, we look at the capacity that the electrical grid can typically handle and how the growth of the charging infrastructure relates to this.

4.5.1 National to international

The high-voltage grid is operating at 380 kV and can transmit typically 2,000-2,500 MW of power. We mentioned earlier that TenneT, as part of Entso-e, is working on the assumption that a maximum of 3,000 MW of emergency capacity can be switched on and off quickly. This capacity must be able to be brought on and off quickly to safeguard the grid balance. When the charging infrastructure has been configured to remain within the technical limits of the electrical grid in a few years' time using smart charging, a sudden increase or decrease in the charging capacity or the disabling of smart charging in the event of a cyberattack could cause a blackout at the national or even international level.

According to our prognosis, if smart charging is not applied and only a sudden interruption in the actual demand for electricity by charging cars and delivery vans occurs, a peak demand of 3,000 MW will be reached around 2027. The simultaneous stopping of all charging infrastructure could then cause instability on the grid. If supply from only one CPO fails, it is only a percentage of that which is served by that CPO. The threat of a national blackout due to failure of one CPO is not likely to occur until after 2030.

With smart charging of cars and delivery vans and operation of all CPOs simultaneously, the 3,000 MW capacity may be reached earlier, i.e., when the total capacity connected at any one time reaches 3,000 MW. In Section 3.2.5 we reasoned that this capacity will be reached as early as 2025. By having all vehicles deliver back to the grid at the same time, the entire connected capacity can be called upon to meet a sudden demand. By having all vehicles charge simultaneously, this same capacity can used for sudden generation of a demand. According to our forecasts, the threat to national grid stability from smart control of all passenger cars and delivery vans will therefore already be around 2025. Heavier freight transport will contribute to the load but has not been considered separately because it is also expected to have a different loading pattern.

Expectations regarding the potential for smart charging are set for 2025 or beyond. The maximum connected volume is therefore expected to be 3,000 MW by then. It is important to think about the cybersecurity aspects before that moment, so that it is impossible to control everything simultaneously via a single 'button'. At grid operators, segmentation of control power is standard build in, to provide a similar security. Increasing power demand from smart infrastructure in addition to load points, such as smart home energy systems, washing machines, ovens, or heat pumps, make it especially urgent to think about cybersecurity standards.

Regional and local

Transmission grids at 150 kV have a transmission capacity of typically 250-400 MW. Below the transmission grids are the medium-voltage distribution grids, which distribute the voltage to the lower grid areas. The distribution grids have voltage levels of 10 - 20 - 50 kV, and below these are low-voltage grids at 400/230 V. Transformer stations link the different voltage levels of the grids. A household with a 3x25 amp connection has a maximum total capacity of 17 kW. The capacity of the transformer substations between the medium-voltage and low-voltage levels is around 0.2-1 MW, and around 100 MW from medium-voltage to the 150-kV network. The transformers between the transmission grid (380 kV) and an interconnected grid usually have a capacity exceeding 500 MW.

At present, several places in the Netherlands are already experiencing congestion at the lower grid levels. Figure 10 and Figure 14-15 illustrate this with an example of the Liander grid areas, where the grid operator is already experiencing bottlenecks in the ability to connect customers, both for demand and supply. The biggest bottlenecks are produced as the result of the growth in the supply of renewable electricity, which is being introduced at low grid levels and for which the grids were not designed. Grid upgrades take a long time and require planning, making it impossible to connect customers everywhere. In the event of disruptions on heavily utilised network areas, problems will arise sooner than when ample capacity is available.

Smart management, such as smart charging, can reduce peak loads and thus create space to realize more connections. The downside is that this increases the pressure on the networks.

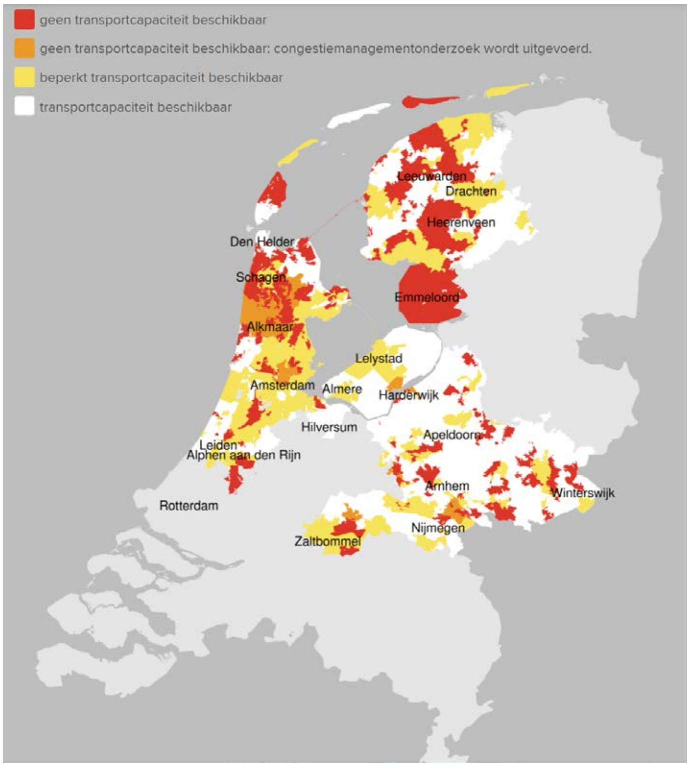

geen transportcapaciteit beschikbaar
geen transportcapaciteit beschikbaar: congestiemanagementonderzoek wordt uitgevoerd.
beperkt transportcapaciteit beschikbaar
transportcapaciteit beschikbaar
Leeuwarden
Drachten
Heerenveen
Den Helder
Schagen
Emmeloord
Alkmaar
Lelystad
Amsterdam
Almere
Harderwijk
Hilversum
Apeldoorn
Leiden
Alphen aan den Rijn
Arnhem
Winterswijk
Rotterdam
Nijmegen
Zaltbommel

Figure 14: **Overview of availability of transport capacity for extra large-scale consumption. (Source: Liander)**

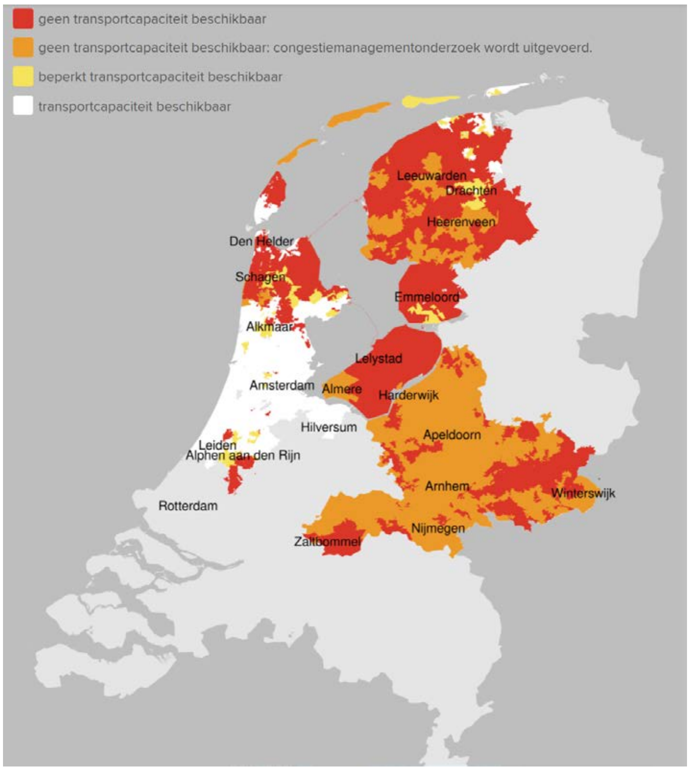

geen transportcapaciteit beschikbaar
geen transportcapaciteit beschikbaar: congestiemanagementonderzoek wordt uitgevoerd.
beperkt transportcapaciteit beschikbaar
transportcapaciteit beschikbaar
Leeuwarden
Drachten
Heerenveen
Den Helder
Schagen
Emmeloord
Alkmaar
Lelystad
Amsterdam
Almere
Harderwijk
Hilversum
Apeldoorn
Leiden
Alphen aan den Rijn
Arnhem
Winterswijk
Rotterdam
Nijmegen
Zaltbommel

Figure 15: **Overview of transport capacity available for Liander's additional large-scale consumption. (Source: Liander)**

Sudden changes in the load capacity of EVs, whether due to a sudden reduction or an increase, can have an impact on the regional grids earlier than is the case for the 380-kV grid. The distribution of grids and connections varies widely throughout the country. Consequently, some regions will be more sensitive to disruptions than others. If the capacity is only just sufficient for the current situation, a disruption will occur more easily. The system is already under pressure.

To illustrate: 100 MW, which is roughly the capacity of a substation connecting the distribution network to the 150 kV network, has room for 9,000 11 kW charging points if they are consumed simultaneously, provided that there is no other demand for electricity at the substation. At smaller stations, of 20 MW, there is only room for less than 2,000 charging points. If that number of charging sockets is exceeded, the boundaries of a substation are already reached. In addition, the impact depends on whether a disruption occurs once or repeatedly. The moment a 25-100 MW region is actively disrupted, security of supply problems can already arise at a regional level.

Current concessions for public charging stations exceed 1,000 charging stations, or the capacity of smaller stations. In 2018, there was a concession for 4,500 public charging points, divided between two provinces and 43 municipalities[49]. A cooperation between Rotterdam and 30 other South Holland municipalities aims to increase the number of public charging points by 7,000 in the next 5 years. In the municipality of Utrecht, a concession will see 1,600 public charge points installed over the next 4 years. It depends on the size of the area and the configuration of the networks when the actual limits of transport or transformers are reached. As soon as smart charging becomes necessary to guarantee connection, you can assume that problems will arise in the event of a sudden failure of the smart charging facility.

HOOFDSTUK 5

Cybersecurity of charge points

In this chapter we will discuss the cybersecurity of charge points.

5.1 Introduction

In doing so, we look at the following in turn:

- A system overview charging infrastructure: what elements can be are seen from a cybersecurity perspective in the charging infrastructure?
- The regulations and standards in the current situation: What laws and regulations currently exist for charging infrastructure?
- The vulnerability in charging infrastructure : we discuss in general terms some of the background to the vulnerability of national charging infrastructure, and give some examples.
- Finally, we provide a brief overview of the typical phases in a cyberattack.

5.2 System overview charging infrastructure

In the diagram below, we provide a simplified overview of the elements of the charging infrastructure indicating what the main cyberattack areas are.

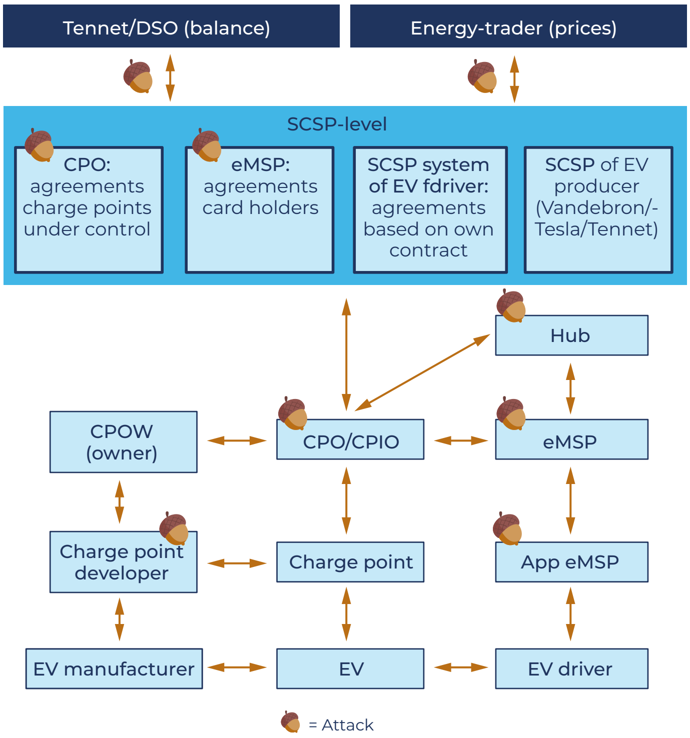

Tennet/DSO (balance)
Energy-trader (prices)
SCSP-level
CPO: agreements charge points under control
eMSP: agreements card holders
SCSP system of EV fdriver: agreements based on own contract
SCSP of EV producer (Vandebron/-Tesla/Tennet)
Hub
CPOW (owner)
CPO/CPIO
eMSP
Charge point developer
Charge point
App eMSP
EV manufacturer
EV
EV driver
= Attack

Figure 16: **Simplified overview of charging infrastructure with cyberattack areas.**

A brief explanation of each element is given below.

- EV = Electric Vehicle: this is the electric car which needs to be recharged. An attack on one car is annoying but only a threat to the system if other elements can be attacked as well.
- **EV driver:** the driver of the car.
- **EV manufacturer:** also the EV manufacturer can become an attack surface and thus, for example, through an infected update, cause an EV to become infected with malware.
- Charging point: A charge point can charge one or more EVs. A cyberattack on this is only dangerous if other elements can be attacked from here.
- The charge point developer may constitute a cyberattack surface: if the software updates[50] contain malware, many charge points may be infected. This may also make the 'generic' software included in the charge point software a cyberattack surface.
- The CPO/CPIO (Charge Point (Infrastructure) Operator) usually has a back office system that manages many charge points. This is an important area of attack.
- The CPOW (Charge Point Owner) can be a private individual, a municipality, a parking garage owner, etc. Often they have no data exchange with charge points and therefore have no cyberattack surface [51].
- The eMSP (eMobility Service Provider) provides cards, sometimes an App and financial services, so that EV drivers can charge at public charging points and later receive a bill for doing so. They are a cyberattack surface because they know names and charging data of customers, which are privacy sensitive.
- The App of the eMSP can have a function as identification and also to influence charging and see charging data. This makes it a cyberattack surface for charging behaviour and for privacy.
- The roaming Hub transmits from the eMSP to the CPO which cards are valid, and from the CPO to the eMSP which charges have been performed. Since no direct personal data is exchanged here, it is a limited cyberattack surface.
- The SCSP level can still be completed in several ways in the future. Often from an already existing party in the charging infrastructure. Most of them form a cyberattack surface because by means of control signals, charging can be reduced or - in the future – charge points will be able to also discharge via V2G (vehicle to grid).
- TenneT and DSO know the balance at national and lower level. The provision of information to the SCSP level is a cyberattack area as manipulation of this can (suddenly) change the loading behaviour of many CPOs.
- Energy trading with prices is a player we expect to emerge in a smart grid and based on contracts per day per 15 minutes can offer prices to EV drivers, eMSPs and CPOs. Manipulation of this data could lead to a sudden change in charging behavior and thus create a cyberattack surface.

For the actual power demand it is important to realize that many elements in this scheme can reduce the demanded power. This starts with the EV: the charge status of the battery and limitations in the charging software can cause the charging to be lower than the maximum. The charging station itself can limit the power to be delivered, especially if the charging station can deliver less than the maximum, due to e.g. limitations from the electricity connection or limitations from multiple charging sessions. The CPO/CPIO can limit the charging speed of the connected charge points, e.g. from considerations of purchase prices or limitations from the maximum capacity of multiple charge points. The SCSP can, based on many considerations, including current price and balance, give the connected CPOs and charge points a signal to charge less. TenneT and the energy trader with prices provide the SCSP with information on the basis of which it can steer for charging less than the maximum.

5.3 Regulations and standards in the current situation

Currently, there are actually no legal standards or regulations for the cybersecurity of charge points and the underlying infrastructure.

However, there are a number of rules and standards or starting points for developing these in the future. We mention the following:

5.3.1 Security requirements for procuring EV charging stations of ENCS and ElaadNL

The ***'Security requirements for procuring EV charging stations' of ENCS and ElaadNL*** [52]. Although not formally enforced, since 2017 it is widely prescribed in public tenders for concessions for public charging stations in Dutch municipalities and provinces [53]. As a result, CPOs and charge point manufacturers consider this standard as a de facto standard they should be able to comply with.

These requirements include cybersecurity requirements with respect to the charge point itself:

a. Authentication and authorization for users and systems.
b. Cryptographic keys.
c. Opening and logging of security events.
d. Remote firmware updating.
e. Limiting vulnerabilities with hardening.
f. Protection of communications over a WAN.
g. Development process of the software of the charge point.

It is easier for charge point manufacturers to bring one or a few types of charge points onto the market. Because they have to comply with these security requirements and the Netherlands is currently a major market for charge points, this is seen as a standard.

This does not mean that all the charge points offered on the market fully comply. Tests of the actual characteristics will sometimes show that adjustments are required. It is unclear whether these requirements are always fully applied to private charge points, which make up the largest share. Some suppliers may also opt for a lower level of cybersecurity in the management or the actual supply, because this is easier to manage and therefore saves costs, for example.

In addition, this standard does set security requirements for the charge point itself, but only indirectly and to a limited extent for the back office system ('CSMS') that manages and controls the charge point.

There are still many charge points using the lower version 1.6 of the OCCP protocol, where the connection can be secured by means of user name and password only, without certificates on the side of the charge point and the back office system.

5.3.2 NIS directive and Wbni

Charging points are currently not part of the vital infrastructure and therefore do not fall under the Wbni: the Network and Information Systems Security Act[54]. Providers that fall under this Act must take appropriate technical and organisational measures to secure their ICT systems and also have a duty to report. If charge points or their back office systems were to be designated as vital, they would have to comply with the associated duty of care, notification and supervision. The Wbni is a Dutch interpretation of the 'NIS directive' of the European Union [55]and may be amended in the coming years.

5.3.3 National Cybersecurity Agenda

The National Cybersecurity Agenda (NCSA) was released in 2018 and[56] includes 7 ambitions. This NCSA was evaluated in 2021 and presented to the House of Representatives by the Minister of Justice and Security on 11 June 2021. On 28 June 2021, the Minister of Justice and Security presented the Cybersecurity Assessment Netherlands to the Lower House of Parliament and, at the same time, informed the House of Representatives of the progress of the Dutch Cybersecurity Agenda. Based on the recommendations from the assessment, important learning points can be identified. A decision on the follow-up to the National Cybersecurity Strategy will have to be taken by the next cabinet.

5.3.4 EU cybersecurity certification framework

At the European level, the 'EU cybersecurity certification framework' is being developed. This must provide a basis for 'EU-wide certification schemes'. Such a certification scheme includes which categories of products or services are described by it, which cybersecurity requirements such as standards or technical specifications exist, how evaluation takes place and the intended level of security that is achieved with it[57]. It involves ENISA, the EU Cybersecurity Agency, which has been given a number of mandates in the area of cybersecurity [58]under the EU Cybersecurity Act. Such a scheme could in the future potentially form the basis of an EU-wide cybersecurity standard for load points.

5.3.5 CE Standards

In addition, there are CE standards, which relate to the electrical requirements of the charge point, just as they apply to toasters or other electrical appliances. Charging points are often assembled from components which meet CE standards, but these are mainly electrical and physical safety standards.

5.3.6 Radio Equipment Directive

The Radio Equipment Directive is an EU directive and has applied to radio equipment sold within the EU since 2017. It could cover, among other things, the communication, privacy and fraud prevention of charging stations with the back office system of a CPO.

5.3.7 Framework guideline on sector-specific rules for cybersecurity aspects of cross-border electricity flows

It is also possible that charge points or the back office systems of CPOs, for instance, could become part of the 'Framework guideline on sector-specific rules for cybersecurity aspects of cross-border electricity flows' of ACER, the European Union Agency for the Cooperation of Energy Regulators. They do not form an explicit part of it, but could become part of it in the future. It is possible that they will then form part of the entities in Table 1, such as an 'electricity digital market platform' or 'critical service provider' to which the rules of this framework will apply[59]. This framework was presented to the European Commission in July 2021 and will be elaborated into a proposal for a network code within 12 months.

5.3.8 Energy Performance of Buildings Directive

The EU Directive 2018/844 of 30 May 2018 amending Directive 2010/31/EU on the energy performance of buildings and Directive 2012/27/EU on energy efficiency sets out requirements on charging points in Article 8. This includes a requirement that in buildings with more than 10 parking spaces, infrastructure for cables shall be provided for at least one in five parking spaces in buildings not suitable for habitation and for each parking space in buildings suitable for habitation. However, no functional or security requirements are attached.

5.3.9 Other directives and regulations

In addition, there are various other directives and regulations from the European Union that have common ground with regard to charge points, but these contain usually limited or no cybersecurity provisions[60]:

- Trans-European Network for Transport (TEN-T) Regulation review;
- Alternative Fuels Infrastructure Directive (published in 2021; it will have the status of 'Regulation');
- CO2 Emissions for cars and vans performance standards;
- Clean vehicles directive;
- Sustainable and smart mobility strategy;
- Renewable energy directive II 2018/2001/EU (new version expected in 2021);
- Energy Efficiency Directive (EU) 2018/2002 ;
- The European Green Deal ;
- 2030 Climate target.

5.3.10 Rules to charge points from the United Kingdom

In the United Kingdom, work is being done on securing the smart charging system. Perhaps this can also inspire developments within the EU. It has been recognised in the UK that cyber risks exist and that hacking into the control systems of charge points threaten the stability of the electricity system if large numbers of charge points can be manipulated simultaneously[61]. There are 90-100 suppliers operating in the UK, these have had 800 models of charge points approved and the top three charge point manufacturers have seen market share drop from 95% in 2014 to 70% in 2020. The following policy choices were made [62]:

a. All private charge points must be 'smart', which means that they must also be able to feed back into the home or the grid, without making V2G compulsory at this stage.
b. All charge points should default during set-up to not charge during peak times (8:00am to 11:00am and 4:00pm to 10:00pm on weekdays).
c. All charging points should have an arbitrary delay to start charging (so that, for example, not all charging points start charging at 22:00 exactly, as this would create another sudden peak load).
d. All charging points must in any case already comply with the minimum requirements of the Internet Of Things cybersecurity standard ETSI EN 303 645 [1]. These requirements will apply from autumn 2022.

5.4 Vulnerability in charging infrastructure

The purpose of this study is to investigate the cybersecurity aspects of the national charging infrastructure in 2030.

5.4.1 Increasing importance of cybersecurity

Various bodies are pointing out the increasing importance of cybersecurity.

The Cybersecurity Assessment Netherlands 2021 (CSBN 2021) drawn up by the National Coordinator for Counterterrorism and Security (NCTV) in collaboration with the National Cybersecurity Centre (NCSC) states that the cyber threat is continuing to develop, with the threat from state actors increasingly blending in with the threat from cybercriminals. In addition, ransomware has become a solid revenue model for cyber criminals. Preparatory acts of sabotage pose a risk to national security.

In July 2021, Angeline van Dijk, director of the Radiocommunications Agency, also warned that the transition to a sustainable energy supply could make the Dutch electricity network more vulnerable to hackers. In particular, solar panels and charge points were mentioned. There is a particular problem if the software used to control these is attacked[63]. The Telecom Agency's report entitled 'Cybersecurity risks for the electricity network in the light of energy transition' notes:

- that efforts are being made to prevent overcharging with smart charging by imposing requirements, but that it is difficult to impose requirements on consumers;
- that a large-scale hack of charge points, their back office or the car manufacturer is given a very high ranking mainly because of the average probability and high social impact; and
- that the producer is too small to fall under the current supervision regime, so that there is no insight into cybersecurity risks[64].

[1] This standard provides a basis of rules for consumer Internet of Things devices, but expects further elaboration in other standards.

5.4.2 Analysis of ICT cyberattacks at charge points

In elaborating the sensitivity analysis, we distinguish two different aspects: lateral vulnerability and chain effects. We will examine both aspects.

5.4.3 Lateral vulnerability

Lateral cyber vulnerability occurs when a particular part of a software network has been compromised, so that other parts of this software network can then be easily attacked as well. An example was a part of the NotPetya malware, which spread the malware independently to other computers in the same network. For charge points, lateral vulnerability can manifest itself if, for example, an SCSP is technically in the same network as the CPO's with which the SCSP communicates.

5.4.4 Examples lateral vulnerability loading points.

It recently became clear that the cybersecurity of charge points leaves much to be desired. Several types of charge points could be hacked by researchers. Some charge points were actually not secure in design because they made use of techniques that cannot be made secure. The researchers were able to take over a charge point, gain access to the Wi-Fi network, or gain access to the back office system by using the API[65]. Or by updating the firmware. They were not the smallest either: one supplier had 2.9 million devices under management. Some vendors reacted quickly and others only after a journalist inquired[66]. This research also states that by breaking into back office systems and switching many charge points on and off alternately, the electrical grid can be destabilised, which can lead to blackouts67.

Of course, the vulnerability of charging infrastructure to cyberattacks would be significantly reduced if a charging point were not connected to a CPO's back office system at all. We do not expect that to take place substantially for the following reasons:

- The trend is that devices are increasingly being linked to back office systems via the Internet.
- To make smart charging possible (as many parties desire), a charge point will have to be linked to a back office system that knows the current balancing and demand situation and prices of the electrical grid.

5.4.4 Vertical vulnerability: Chain effects and social impact of power failure

Chain effects occur when failure of one component leads to failure of another component. This can happen for instance when the failure of an eMSP hinders the use of a CPO. But also upstream: sudden up- or down switching by CPOs can cause problems for the TSO or DSO. And also downstream: failure of load points will result in a loss of transport, causing problems for various (vital) sectors. For example, see the traffic jams in the port of Rotterdam after the failure of the Maersk container terminal or the limited supply by petrol stations after the ransomware attack on Colonial Pipeline in May 2021.

Social costs in case of failure of charge points are comprised of the following factors:

- Loss of business
- Loss of mobility (partly this can be 'made up' later, but partly not)
- Breakdown of emergency services
- Stuck lifts
- Failure of 112 emergency lines
- Failure of refrigerators
- Failure of heating
- Human lives

In this study we do not perform an extensive Social Cost Benefit Analysis of possible power outages, but we do provide some key figures based on a few historical situations.

A study in 2003 estimated the social costs of a daytime disruption in the Dutch conglomeration 'Randstad' at € 72 million per hour[67]. These costs are many times the costs of the electricity not supplied, which amounted to only € 1.6 million[68]. Differences between sectors were pronounced, with the magnitude of lost leisure time for households comparable to the production losses of businesses. Within this, damages in the services sector were higher than in industry.

An increasing share of the energy demand is becoming dependent on electricity. Examples include mobility, heat supply and service activities. During the power outage in Amsterdam in 2017, 360,000 households were without electricity from 4:00 a.m. onwards, train traffic was halted, the district heating system failed and 20,000 households were without heating. By 9:00 a.m. the power failure had been resolved, but it took longer to get the heating systems up and running again and to bring water for district heating to the right temperature. The economic damage was estimated at 20-30 million euros.

Future effects will also weigh more heavily on services that depend on electricity, such as the mobility of emergency services, in the event of longer interruptions. If the fire brigade, police or ambulance services can no longer turn out because of flat batteries, emergency assistance cannot be provided where needed. The costs of longer power cuts will rise accordingly.

Unexpected and unintended cascading effects can also make the impact of a failure in mobility and electricity supply larger than initially foreseen. For example: if (part of) a hospital runs out of heating despite emergency provisions, the fire brigade is called out. But after helping to move patients, the battery of the fire truck may be depleted, making it impossible to drive to a fire. Et cetera.

In chapter 3.2an estimate was made of the amount of power that can be controlled via charge points at different times of the day.

5.5 Phases of cyberattack

A cyberattack proceeds in phases. These phases broadly consist of [69]:

- **Initial Access**
  The initial access can take place by trying passwords, sending a phishing mail with an infected document containing malware, attacking an improperly patched website with a known vulnerability, etc. The result is that the hacker is ‘inside’.

- **Consolidation and preparation**
  The hacker obtains more and more privileges, moves ‘laterally’ through the network, hides himself and makes sure he can gain access in multiple ways. However, the hacker usually cannot gain access to other networks if they are segregated from the network he is already in.

- **Impact on target: the strike**
  The hacker strikes. He gets data out of the network, encrypts data using ransomware, destroys backups and systems, etc. In the case of charge points, for example, the hacker can update a charge point with infected firmware, causing smart charging to stop working, enabling the hacker to take over control of the system, and so may require a mechanic to visit each charge point to repair it, etcetera.

CHAPTER 6

Impact associated with cybersecurity risk of charging infrastructure

6.1 Introduction

This chapter examines the social impact and chain effects of four different scenarios for a cyberattack. These were identified with the help of experts, and grouped in this chapter so that four generic scenarios could be identified. For each scenario, we analyse the impact.

In accordance with the basic principles, these are deliberate attacks. From the perspective of general information security it is of course also possible to imagine other disruptions, such as failures of the internet, electricity or telephone; poorly functioning software or smart charging algorithms, etc.

6.2 Overview of scenarios

We identified the following four scenarios. Each scenario is based on a typical cyber threat. For each cyberattack, the cyberattack with the highest impact is described as a typical attack. Of course, variations on the four described attack scenarios with less impact can be imagined: think of an attack on a smaller player, an attack not during peak hours, a less well-executed attack, et cetera.

For each scenario, we indicate: the main cyber threats we have identified, with motivation, the method with the actor, the attack surface or function used, and the main additional measures.

For each scenario, we indicate the impact, as well as a calculation of the year when this scenario will exceed the control limits.

6.3 Scenario 1: **Smart Attack by State Actor**

Scenario	Motivation	Method with actor	Attack surface/function	Important measures
1	Disruption NL society	APT (Advanced Persistent Threat)	Backoffice large CPO's (using OCCP and OCPI protocols if needed)	- segmentation & protection software development - Authentication and Authorization - Hardening CPOs and SCSPs - Intrusion detection, patching, logging

In an attack according to scenario 1, the back office of a large CPO is hacked. From there, all connected charge points are used to attack the electrical grid. The possibilities of smart charging are exploited. This scenario also reveals that if smart charging is used to reduce peak demand, this also introduces an additional vulnerability if smart charging is deliberately deployed by a malicious party seeking to destabilize the electricity network. To a lesser extent, this also applies to the second and third scenarios.

Actor	State Actor
Motivation	Disruption of the Dutch society
Approach	Attack on one or more back office systems of load points. In particular, back office systems of a CPO or SCSP. This involves the manipulation of the possibilities of smart charging
Impact TSO	Possibly a blackout and separation of the Netherlands from the European network, and possibly a blackout of Europe, especially if the CPO is also active in several other countries
Impact DSO	Local disruptions and blackouts, also stemming from TSO
Impact CPO	Disrupted operation of attacked CPO, in case of a failure of the electricity network of course also failure of the charging infrastructure of other CPOs
Impact eMSP	None.
Impact of national charging infrastructure	Failure of national charging infrastructure. Fatalities are also to be expected when electric emergency vehicles are no longer deployable: ambulances, police, etc.
Impact mobility Netherlands	Mobility outage during blackout after EV batteries run out.
Possibly achieved in which year	From 2025 onwards. Assuming an attack on one CPO.

6.4 Scenario 2: **Large Attack by State Actor**

Scenario	Motivation	Method with actor	Attack surface/function	Important measures
2	Disruption Dutch society	APT	Communication between TenneT and electricity market parties with SCSPs	- Encryption of communication control signals and market prices. - Two-sided authentication, segmentation, security authorization
2	Disruption NL society	APT	Backoffice large CPO's or EV manufacturer, also OCCP and OCPI protocols Non bi-directional TLS Trojan spread via upgrade of charging station software	- Authentication and authorization - hardening CPOs and SCSPs - Intrusion detection, patching, logging

In the event of an attack based on scenario 2, either a) the TenneT control signal containing the grid balance or the prices based on this balance is hacked, or b) a very central SCSP is hacked. From there, all controlled charge points are used for an attack on the electrical grid. This involves a sudden interruption of charging via charge points. This is expected to disrupt the grid balance if the suddenly switched-off capacity is greater than 3,000 MW.

We have taken 3,000 MW as a control limit because 3,000 MW is considered the normative reference incident for frequency interference in the European Entso-e context. In the Netherlands, an incident of 1,300 MW is regarded as one that the TSO itself can remedy, but because the Dutch grid is linked to the European one, an incident of up to 3,000 MW is not expected to cause any real problem. An incident above 3,000 MW might of course also be handled, depending on the circumstances at the time (e.g. several generators operating at low load). In this report, we have assumed existing and known control limits.

Such an attack is of course also possible on a single large CPO, but as only the charge points of that particular CPO will be affected, the effect will be smaller. For example, if a CPO is attacked that controls 20% of the charging points in the Netherlands, it will only be 20% of the peak capacity. Assuming a peak capacity for personal EVs of 2,000 MW and a peak capacity for vans of 3,000 MW In the year 2030, the effect will be only 20% of 5,000 MW which equals 1,000 MW. It may then depend on the location whether this leads to immediate problems at regional or national level, or whether it can be absorbed by the grid. Especially in urban areas, the load on the electricity network is closer to the maximum load and therefore the vulnerability is higher. Only after 2030 may such an attack on one CPO lead to a blackout.

Actor	State Actor
Motivation	Disruption of society
Approach	Attack on one or more back office systems charge points. Mainly CPO, SCSP or TSO control. To the extent that more than 3000 MW in the Netherlands are disconnected.
Impact TSO	Possibly a blackout of the Netherlands and disconnection of the Netherlands from the European network.
Impact DSO	Local disruptions and blackouts, also from TSO
Impact eMSP	None
Impact of national charging infrastructure	Failure of national charging infrastructure
Impact mobility Netherlands	Fatalities are also to be expected when electric emergency vehicles are no longer deployable: ambulances, police, etc.
Achieved in which year	After 2027 if a connection to TenneT or to a central SCSP is attacked, Probably after 2030 if a single large CPO is attacked

The larger the blackout, the longer it will usually last. For a nationwide blackout, the consequences are significant. The duration will be approximately 8 hours. If the scale is even larger than national it may take even longer. Above 8 hours, it is unknown what the consequences will be. Certainly if we take into account the increasing dependence on electricity for the provision of mobility, but also heating, telecommunications and IT.

6.5 Scenario 3: **'Ordinary cyberattack'**

Scenario	Motivation	Method with actor	Attack surface/function	Important measures
3	financial gain	Criminal organization with ransomware	Technical system under SCSP or CPO system	Good backup not directly accessible from back office Intrusion detection Adequate authentication
3	For example, anti-establishment terrorists	DDOS	Access servers CPOs, eMSPs. Supply chain attack through infection of generic software used by CPO.	DDOS car wash setup by CPO and eMSP
3	Just trying	Unpredictable or script kiddie	Website, API of CPO	Basics in order: authorization, authentication, patches
3	Social disruption smaller scale	Prisoner transport, ME, police, fire department, ambulance	Change of geographic information, CDRs	Ditto.
3	Energy price on the stock exchange influenced by traders or state actors	Major hacking and taking positions in advance	Technical system under SCSP or CPO system	Ditto.
3	Financial gain	Skimming of cash flows, medium-sized actor	Hub, big bang or little bit	Control of money flows, authentication of correct information exchanged.
3	None; bad luck	APT	Escaped Trojan with zero-day	Segmentation.

Actor	Various actors: script kiddie, terrorist, criminal organization
Motivation	Making money or trying out or making a point.
Approach	Attack on one back office systems charging points. So that one CPO fails.
Impact CPO	Failure of back office system of one CPO. Financial damage (because a mechanic has to be sent to each charge point) and image damage.
Impact eMSP	Probably limited; possible financial damage.
Impact DSO and TSO	Local disruptions and brownouts or blackouts, including from TSO
Impact on national charging infrastructure	Failure of charging stations of one CPO. Possibly live again after a few days. However, if the firmware of the charge points has also been compromised as a result of the cyberattack, it may take weeks before all charge points have been visited and manually restored. If certain essential services or a geographical area are heavily dependent on the affected CPO, this could cause substantial disruption.
Impact mobility Netherlands	Reduced availability of public charge points. A number of private customers can no longer charge at home. When it comes to charging points with a high charging speed: economic damage to charging stations and companies that depend on fast chargers during the day, such as delivery vans, supplying supermarkets.

6.6 Scenario 4: **Privacy attack**

Scenario	Motivation	Method with actor	Attack surface/function	Important measures
4	Damage to confidence in charging infrastructure or financial gain or espionage/ prepared attack, espionage between parties	Criminal organisation or APT with semi-political objectives	Stealing CDRs (loading data with privacy information)	• eMSPs : encryption database CDR's, • Authentication, authorization • Segmentation • Message Encryption

Actor	Especially criminal organizations, or State Actors with semi-political goals.
Motivation	Making money or undermining trust in mobility infrastructure.
Approach	Especially stealing charge data or cardholder data.
Impact CPO	Failure of back office system of one CPO.
Impact eMSP	Customer data on the street. Declining confidence.
Impact TSO	None
Impact DSO	None
Impact on national charging infrastructure	Reduction in confidence; this also leads to a delay in energy transition.
Impact mobility Netherlands	None

6.7 Costs of a blackout in the Netherlands

As described above in this chapter, there are several cyberattacks that carry the risk of possibly leading to a blackout. A blackout in the Netherlands is usually defined as a situation in which more than 50% of the electricity supply has failed. Fortunately, this has not occurred in the Netherlands to date. For this reason, there are no experiences or statistics available.

The bigger the blackout, the longer it will last. We have assumed a 24-hour blackout. In 2003 the cost of a daytime blackout in the Randstad conglomerate was estimated at around 72 million euros per hour[69]. The time of day is one of the factors determining the costs and where they are incurred. A daytime power failure results in production losses at companies, it may be difficult to get home, and the impact is especially great in the service sector.

Actual costs and damages may of course differ from those roughly calculated below, due in part to:

- a shorter duration of the blackout due to the TSO's and DSOs' ability to resolve the disruption sooner than in one day;
- a longer duration of the blackout due to unforeseen cascading effects;
- A longer duration of the blackout because cyberattacks continue during the recovery work;
- the costs for the Netherlands as a whole may be higher, because the dependency on electricity in 2030 will be much greater than was known in 2003 when the loss of €72 million was calculated.
- This is how we come to estimate the cost of a 24-hour blackout in the Netherlands as shown in Table 2.

Factor	amount	unit
Cost of damage 1 hour no electricity Randstad	72	Million Euros
Duration of disturbance in hours	24	Hours
Total damage during Blackout	1,728	Million Euros
Conversion factor from Randstad to the Netherlands	2,2	
Total damage Netherlands during blackout	3,736	Million Euros

Table 2: **Estimated costs of a nationwide blackout of 24 hours in the Netherlands.**

A cyberattack in the Netherlands may also have an effect in other countries. Either because the cyberattack also affects loading points in other countries, because the party under attack is active in several countries and/or because a failure in the electricity supply in the Netherlands also affects other European countries.

Appendix

APPENDIX 1

Interviews

Interviews were conducted with experts working for the following parties.

- Allego
- Radiocommunications Agency
- ElaadNL
- ENCS
- eViolin
- Engie
- Enovates
- MultiTankcard
- Stedin
- TenneT
- Transport and Logistics Netherlands
- Delft University of Technology
- TU Eindhoven

APPENDIX 2

List of Abbreviations

aFRR	Automatic Frequency Restoration Reserve. This is the ‘regulating power’. It is controlled by TenneT TSO and, once activated, can be fully deployed within 15 minutes.
CPO	Charge Point Operator
DDoS	distributed-denial-of-service
ENCS	European Network for Cybersecurity. A non-profit member organization that brings together critical infrastructure owners and security experts to deploy secure European critical energy grids70.
ENTSO-E	European Network of Transmission System Operators for Electricity. Since 1 July 2009 responsible for all operational tasks of the TSOs in Europe.
eMSP	e-Mobility Service Provider
EV	Electric Vehicle
mFRR	Manual Frequency Restoration Reserve. This is the ‘Reserve Power’ (mFRRsa) and ‘Emergency Power’ (mFRRda). This power can be deployed by TSO in the event of a prolonged imbalance in the electrical grid in order to ‘free up’ the aFRR so that it can be used again if necessary.
OCPI	Open Charge Point Interface
OCPP	Open Charge Point Protocol
SCSP	Smart Charging Service Provider
SCADA	Supervisory Control And Data Acquisition
FCR	Frequency Containment Reserve. This is the ‘Primary Reserve Power’. This power can be called upon within seconds and delivers the full contracted power within 30 seconds.

APPENDIX 3

References

Endnotes

1 This definition is intentionally limited in scope. It is also different from the definitions in the Cybersecurity Dictionary of the Cybersecurity Alliance (www.cybersecurityalliantie.nl/documenten/publicaties/2019/09/30/cybersecurity-woordenboek). Therein, “Attack” is described as “Action in which someone intentionally attempts to disable or circumvent security in order to get into a digital system” and “Cyber attack” is described as: “A targeted attack in or through cyberspace. Targets may include individuals, groups, companies and organisations, governments, other countries”.

2 Climate and Energy Outlook, PBL, 2020.

3 Elaad.nl outlook ‘Truckers get on power’, 2020. Online: www.elaad.nl/uploads/files/20Q3_Elaad_Outlook_E-trucks_internationale_logistiek.pdf.

4 Climate Agreement, The Hague, 28 June 2019, p.50. Recharging economies: The EV battery manufacturing outlook for Europe, McKinsey, p.3, May 2019.

5 ‘Half of New Cars in US to be Electric by 2E030’, NRC, 6 August 2021.

6 See also the Climate Agreement, The Hague, 28 June 2019. In it, the number of expected charging points is estimated at 1.7 million in 2030 (in the latest ElaadNL forecast it is 1.8 million).

7 Yearly review Electric driving on the road, RVO, 2020

8 The national EV and driver survey - Experiences and opinions of users. RVO, 2021.

9 Using electric vehicles as flexible resource in power systems: A case study in the Netherlands. A. Beltramo, A. Julea, N. Refa, Y. Drossinos, C. Thiel, and S. Quoilin. IEEE, 2017.

10 Elaad.nl Open datasets for electric mobility research, update April 2020.

11 ElaanNL outlook ‘Electric driving in rapids’, 1 November 2021. Online: www.elaad.nl/uploads/files/2021Q3_Elaad_Outlook_Personenautos_2050.pdf.

12 ElaadNL outlook ‘Electric on demand’, 2020. Online: www.elaad.nl/uploads/files/20Q2_ElaadNL_Outlook_E-bestelvoertuigen_V1.0.pdf

13 Trends in Charging Infrastructure Use, EV Data, September 3, 2021, www.evdata.irias.nl/data?lang=nl.

14 Electric Vehicle integration into power grids, Entso-e position paper, entso-e, 31 March 2021.

15 Electric Vehicle integration into power grids, Entso-e position paper, entso-e, 31 March 2021, p.19.

16 Megawatt Charging System (MCS), Charin, May 8, 2021, www.charin.global/technology/mcs/.

17 Electric Vehicle integration into power grids, Entso-e position paper, entso-e, 31 March 2021, p.28 & p.29

18 The road to two-way CCS electric car charging, Bryce Gaton, July 21, 2021, Online: www.thedriven.io/2020/07/21/the-road-to-bidirectional-ccs-electric-car-charging/

19 www.charin.global/news/vehicle-to-grid-v2g-charin-bundles-200-companies-that-make-the-energy-system-and-electric-cars-co2-friendlier-and-cheaper/.

20 Electric Vehicle integration into power grids, Entso-e position paper, entso-e, 31 March 2021.

21 Electric Vehicle integration into power grids, Entso-e position paper, entso-e, 31 March 2021, p.29.

22 IEA, Contribution of electric vehicles to hourly peak demand by country and region in the evening and night charging cases in the Sustainable Development Scenario, 2030, IEA, Paris www.iea.org/data-and-statistics/charts/contribution-of-electric-vehicles-to-hourly-peak-demand-by-country-and-region-in-the-evening-and-night-charging-cases-in-the-sustainable-development-scenario-2030.

23 Recharging economies: The EV-battey manufacturing outlook for Europe, McKinsey, p.3, May 2019.

24 Electric driving gets cheaperand cheaper, nu.nl, 14 August 2021.

25 Tesla’s 4680 battery cell is ‘brilliant’ according to industry experts, Iqtidar Ali, October 4, 2020, www.evannex.com/blogs/news/ tesla-s-4680-cell-is-a-stroke-of-genius-sandy-munro.

26 Tesla Model S Plaid fast charging result amaze: analysis, Mark Kane, July 28, 2021, www.insideevs.com/news/515641/tesla-models-plaid-charging-analysis/.

27 IEA, Private electric vehicle slow chargers by country, 2019, IEA, Paris www.iea.org/data-and-statistics/charts/private-electric-vehicle-slow-chargers-by-country-2019.

28 IEA, Publicly accessible electric vehicle slow chargers by country, 2019, IEA, Paris www.iea.org/data-and-statistics/charts/publicly-accessible-electric-vehicle-slow-chargers-by-country-2019.

29 IEA, Publicly accessible electric vehicle fast chargers by country, 2019, IEA, Paris www.iea.org/data-and-statistics/charts/publicly-accessible-electric-vehicle-fast-chargers-by-country-2019.

30 www.insideevs.com/news/515641/tesla-models-plaid-charging-analysis/

31 Snel, sneller, snelst, The development of fast chargers in the Netherlands until 2025. Extrapolation of the middle scenario comes to 8500 quick chargers in 2030.

32 See e.g. Dans om de laadpaalmarkt nog net begin, NRC, 20 April 2021.

33 www.tennet.eu/nl/elektriciteitsmarkt/data-dashboard/belasting/.

34 IEA, Contribution of electric vehicles to hourly peak demand by country and region in the evening and night charging cases in the Sustainable Development Scenario, 2030, IEA, Paris www.iea.org/data-and-statistics/charts/contribution-of-electric-vehicles-to-hourly-peak-demand-by-country-and-region-in-the-evening-and-night-charging-cases-in-the-sustainable-development-scenario-2030.

35 System separation in the Continental Europe Synchronous Area on 8 January 2021 - 2nd update, Entso-e, 26 January 2021, www.entsoe.eu/news/2021/01/26/system-separation-in-the-continental-europe-synchronous-area-on-8-january-2021-2nd-update/. Start of events at 14:04:25.9 and separation of network completed at 14:05:08.6.

36 Technical Report on the events on 9 August 2019, ESO, 6 September 2019, ‘National Grid ESO LFDD 09/08/2019 Incident Report’, 37 pages, retrieved 23 june 2021 from www.nationalgrideso.com.

37 Can Cyber Attacks cause a blackout? b, A. Stefanov, TU Delft, 31 March 2021.

38 Analysis of the cyber attack on the Ukrainian power grid, Defense use case, E-ISAC, March 16, 2016,

39 Dutch ancillary sevices, Tennet, retrieved from www.tennet.eu/electricity-market/dutch-acillary-services.html on 18 August 2021.

40 The biggest flare-up in over a decade, www.hoogspanningsnet.com/tag/netfrequentie/. Retrieved June 15, 2021.

41 Dutch Ancillary Services, Tennet, “This means that an outage of 1000 MW anywhere in the synchronous area, should result in a Dutch FCR contribution of 37 MW. Since reference incident is 3000 MW in total” www.tennet.eu/electricity-market/dutch-ancillary-services/

42 www.tennet.eu/electricity-market/transparency-pages/ ; “By 2030, the originally planned capacity of 15 gigawatts of offshore wind energy will increase to 20 GW.”

43 www.tennet.eu/our-grid/international-connections/about-international-connections/ retrieved on 23 june 2021.

44 E.g. On 15 August 2021, the total import through interconnectors from Germany to the Netherlands was 3598 MW between 03:15 and 03:30.

45 Review of wind generation within adequacy calculations and capacity markets for different power systems, L. Söder et al, Renewable and sustainable energy reviews 119 (2020) 109540, 22 November 2019.

46 www.liander.nl/nieuws/2021/06/24/knelpunten-op-het-elektriciteitsnet-amsterdam

47 Alliander: ‘City is fast heading for a power infarction’, Het Parool, 3 August 2019, www.parool.nl/nieuws/netwerkbedrijf-alliander-stad-is-hard-op-weg-naar-een-stroominfarct~b74c497c/.

48 Kenmerk ACM/UIT/534445, Zaaknummer ACM/19/036613, Besluit van de Autoriteit Consument en Markt op grond van artikel 37a van de Elektriciteitswet 1998, betreffende de ontheffiefingsaanvraag TenneT codebepalingen enkel storingserve, Autoriteit Consument en Markt, 2 juli 2020.

49 Gelderland and Overijssel use joint purchasing power for procurement of public charging points, Piano expertise centre for procurement, 2019.

50 This does not take place at all CPOs because updates sometimes fail and cause malfunctions that require a trip by a technician, which increases costs.

51 However, a cyber attack on electricity meters or Home Electricity Management Systems could ensure that the control signals these give off in the case of smart charging are compromised, as a result of which (also) the charge points could exhibit undesirable behaviour.

52 Security Requirements for procuring EV charging stations (www.encs.eu/encs-document/security-requirements-for-procuring-ev-charging-stations/, EV-301-2019, version 2.0, December 24, 2019.

53 ElaadNL: Niewe Eisen voor cybersecurity voor laadpalen het eerste toegepast. December 1, 2016. www.elaad.nl/nieuwe-eisen-voor-cybersecurity-laadpalen-voor-het-eerst-toegepast/.

54 Replying to Parliamentary Questions by Renco Dijkstra (VVD) about the message ‘Electric cars more expensive to maintain than fuel cars’, 22 January 2021, letter from the State Secretary for Infrastructure and Water Management S. van Veldhoven - Ven der Meer to the Speaker of the Lower House of the States General.

55 DIRECTIVE (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, European Union, 19 July 2016.

56 www.ncsc.nl/documenten/publicaties/2019/mei/01/nederlandse-cybersecurity-agenda.

57 ‘The EU cybersecurity framework’, Euopse commission, www.digital-strategy.ec.europa.eu/en/policies/cybersecurity-certification-framework, retrieved 2 August 2021.

58 The EU Cybersecurity Act, European Commission, www.digital-strategy.ec.europa.eu/en/policies/cybersecurity-act, retrieved 2 August 2021.12

59 ‘Framework guideline on sector-specific rules for cybersecurity aspects of cross-border electricity flows. ACER, 22 July 2021.

60 Electric Vehicle integration into power grids, Entso-e position paper, entso-e, 31 March 2021.

61 The Electric Vehicles (Smart Charge Ponts) Regulations 2021, Impact Assessment, 2021,

62 Smart Charging Consultation - Government Response, UK Government, July 2021.

63 Hackers can sabotage power grid via solar panel and charging station’, NOS, 12 July 2021.

64 Riskid Cybersecurity risks for the electricity network in the light of the energy transition, Radiocommunications Agency, 2021, p.77 and p.119.

65 Smart car chargers. Plug-n-play for hackers?, PenTestPartners, August 2021, www.pentestpartners.com/security-blog/smart-car-chargers-plug-n-play-for-hackers/.

66 Home car chargers owners urged to install updates, Dan Simons, BBC Click, 3 August 2021, www.bbc.com/news/technology-58011014.

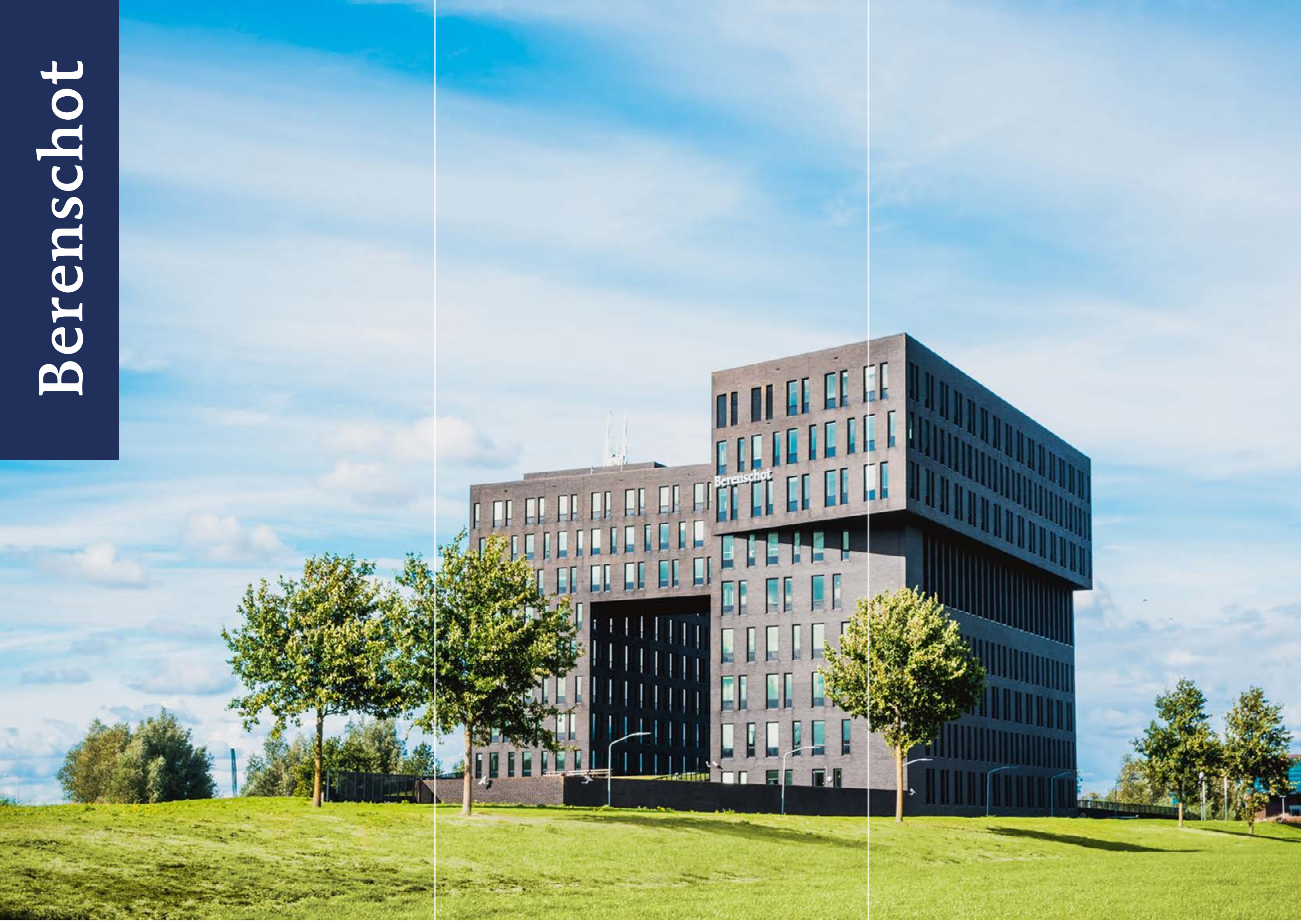
67 “Gansch the radar work stands still.” The Costs of Power Outages, C. Bijvoet, m. de Nooij, C. Koopmans, SEO, UvA, 2003, p.67.

68 At the DSO Enexis, for a regular consumer connection, no compensation is charged for the first 4 hours, for the next 4 hours 35 Euros, and for every 4 hours thereafter 20 Euros. This 20 euros per 4 hours translates into 8 cents per minute. www.enexis.nl/consument/storingen-en-onderhoud/storingen/compensatievergoeding-na-storing. This amount is not equal to the social damage.

69 Lifecycle of a ransomware incident, CertNZ, 2021.

70 ENCS and ElaadNL, Security Requirements for procuring EV charging stations (www.encs.eu/encs-document/security-requirements-for-procuring-ev-charging-stations/).

Berenschot



'WIJ ZIJN BERENSCHOT, GRONDLEGGER VAN VOORUITGANG'

Wij zien een Nederland dat altijd in ontwikkeling is. Zowel sociaal als organisatorisch verandert er veel. Al meer dan 80 jaar volgen wij deze ontwikkelingen op de voet en werken we aan een vooruitstrevende samenleving. Daarbij staan we voor duurzaam advies en de implementatie hiervan. Altijd gericht op vooruitgang én echt iets kunnen betekenen voor mensen, organisaties en de maatschappij.

Alles wat we doen, is onderzocht, onderbouwd en vanuit meerdere invalshoeken bekeken. In ons advies zijn we hard op de inhoud, maar houden rekening met de menselijke maat. Onze adviseurs doen er alles aan om complexe vraagstukken om te zetten naar praktische oplossingen waar u iets mee kan. Wij geven advies en bieden digitale oplossingen waarbij we ons focussen op:

- Toekomst van werk en organisatie
- Energietransitie
- Toekomst van zorg
- Transformatie van openbaar bestuur

Berenschot Groep B.V.

Van Deventerlaan 31-51, 3528 AG Utrecht

Postbus 8039, 3503 RA Utrecht

030 2 916 916

www.berenschot.nl