Building a cyber-resilient eMobility ecosystem

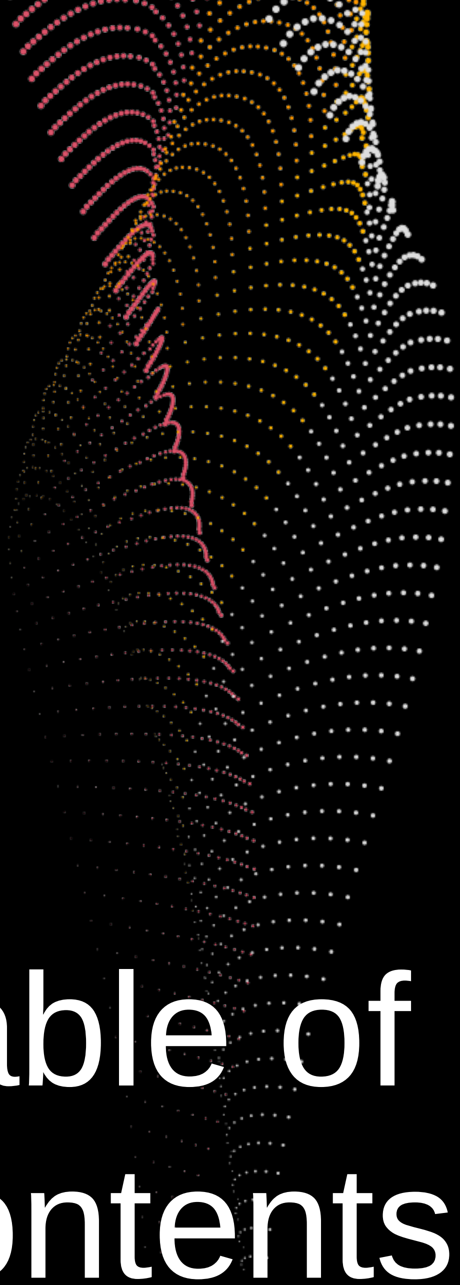
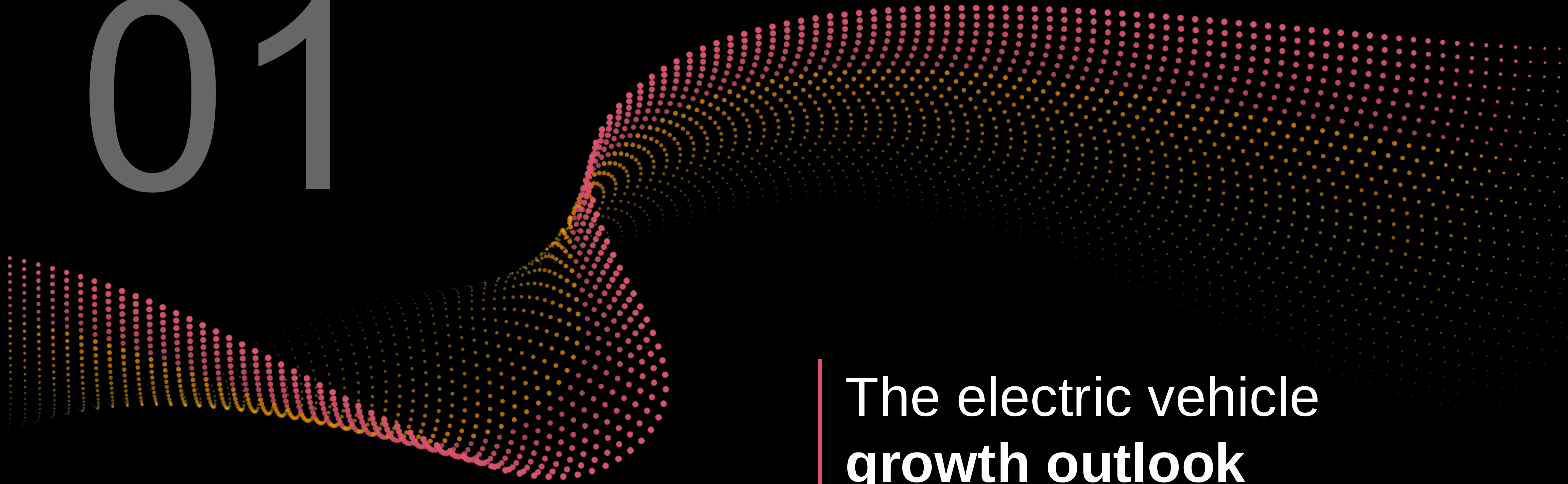


Table of contents

01



The electric vehicle **growth outlook**

01 The electric vehicle growth outlook

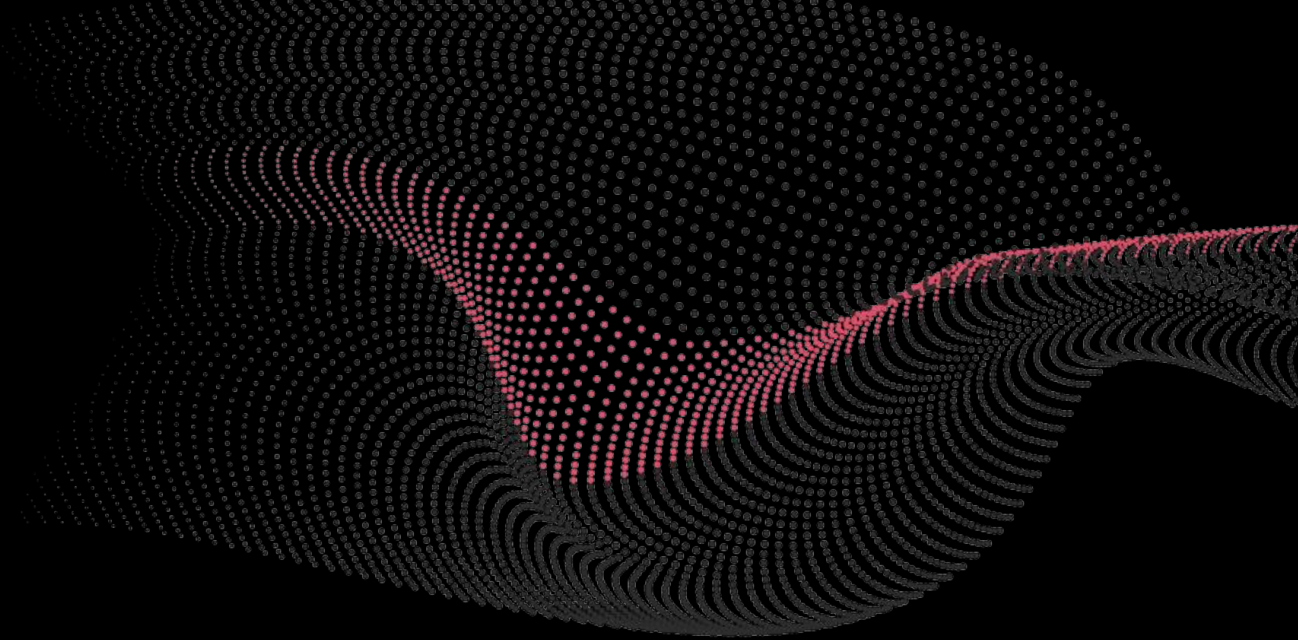
Decarbonising road transport is essential and electric vehicles (EVs) offer a promising solution with zero tailpipe emissions, reducing fossil fuel dependence, improving air quality and fostering innovation and growth in the green energy sector.

The adoption of electric vehicles is accelerating globally, with nearly 14 million new electric vehicles registered in 2023 alone[1]. Key countries, such as China, Europe and the United States accounted for nearly 95% of global EV sales[1]. In the Gulf Cooperation Council (GCC) region, the UAE is leading in EV adoption and charging infrastructure development, followed by Saudi Arabia[2,3]. PwC Middle East forecasts that by 2035, new EV sales will represent 25% of the UAE market and 64% in Saudi Arabia[2,3].

EV Sales by 2035:

UAE
25%
Saudi Arabia
64%

However, as EV uptake across the GCC continues to grow, the increasing connectivity and complexity of the broader eMobility ecosystem raises cybersecurity challenges that impact a range of stakeholders – from manufacturers and payment processors to power grid operators, charging infrastructure providers and electric vehicle owners.



This paper explores the electric vehicle ecosystem and its cybersecurity imperatives, highlighting the key threats and offering actionable recommendations to eMobility stakeholders.

02

An integrated **ecosystem**

02 An integrated ecosystem

Electric Vehicles are not standalone; it is part of a broader ecosystem that encompasses multiple industries within different sectors

Charging infrastructure:

Charge Point Operators (CPOs) manage public EV charging stations, while eMobility Service Providers (eMSPs) handle payment and access. Clearing houses connect CPOs and EMSPs, ensuring seamless charging across networks.

Electricity sector:

Charging stations are connected to the grid, while private stations connect locally. Grid operators assess capacity to ensure compliance with impact standards.

Public sector:

The public sector supports eMobility by setting regulations, providing incentives, investing in infrastructure, funding research and promoting public awareness.

Payment terminals:

They enable secure transactions for electric vehicle charging through mobile apps, RFID cards and digital wallets

Battery industry:

The battery, accounting for up to 40% of an electric vehicle’s cost, is managed by a battery management system to ensure performance, safety, longevity and end-of-life management.

Energy management:

Energy Management Systems (EMS) optimise charging based on renewable energy availability. Bidirectional charging allows electric vehicles to return power to another source (detailed beneath).

Insurance companies:

They offer tailored policies, embedding insurance in vehicle purchases and partnering with mobility services to provide integrated coverage.

02 An integrated ecosystem

The electric vehicle ecosystem encompasses a range of convergent technologies:

Vehicle connectivity:

All new vehicles are internet-connected, letting users access features via an application on a smartphone. 5G enables real-time communication between EVs, charging stations, infrastructure and the EMS (if applicable) supporting autonomous driving, charging and traffic management. These novel features rely on AI, IoT, sensors and real-time data to improve mobility and efficiency.

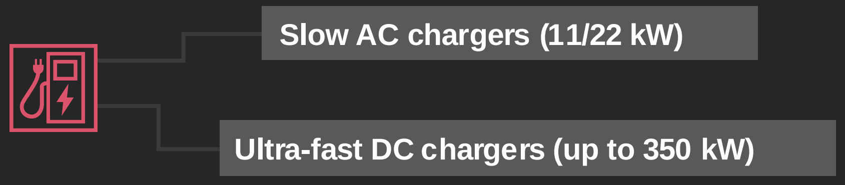
Smart charging and bidirectional charging:

Smart and bidirectional charging allow electric vehicles to draw power from the grid and return energy, supporting grid stability and home power needs. This vehicle-to-X technology (X being Grid, Home, Building, Load or Vehicle) optimises charging based on demand and renewable energy availability, reducing grid strain, lowering costs and promoting sustainability.

Multiple payment mechanisms:

Secure transactions for electric vehicle charging, vehicle data management and peer-to-peer energy trading are facilitated via multiple payment methods, allowing users to initiate payments for electric vehicle-related services via point-of-sale terminal machines, mobile wallets, direct bank applications, RFID cards and QR codes to enhance transparency and efficiency in this market.

Charging infrastructure is divided into private (home, work and depot charging for fleets) and public. It includes slow AC chargers (11/22 kW) to ultra-fast DC chargers (up to 350 kW) with standardised communication and plug systems.



Slow AC chargers (11/22 kW)

Ultra-fast DC chargers (up to 350 kW)

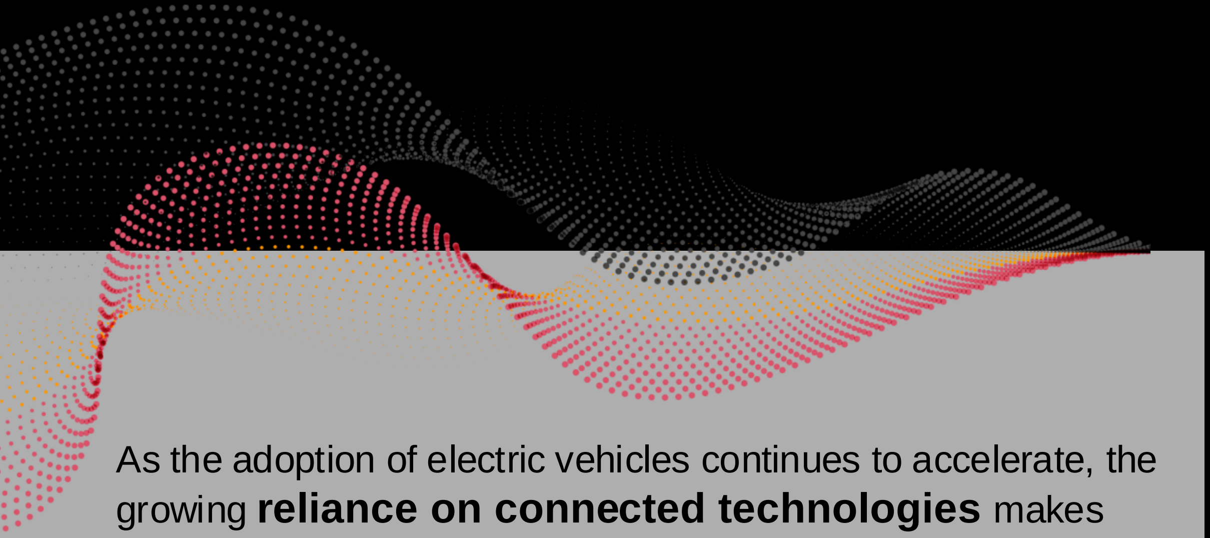
	EVs	CPs
US	71.9m	2.18m
China	247.5m	9.81m
Germany	19.9m	0.63m
KSA	800k	180k
UAE	110.5k	45k

Figure 1: Electric vehicles and charging points forecast for selected countries

03

Cybersecurity imperatives for the **eMobility transition**

03 Cybersecurity imperatives for the eMobility transition



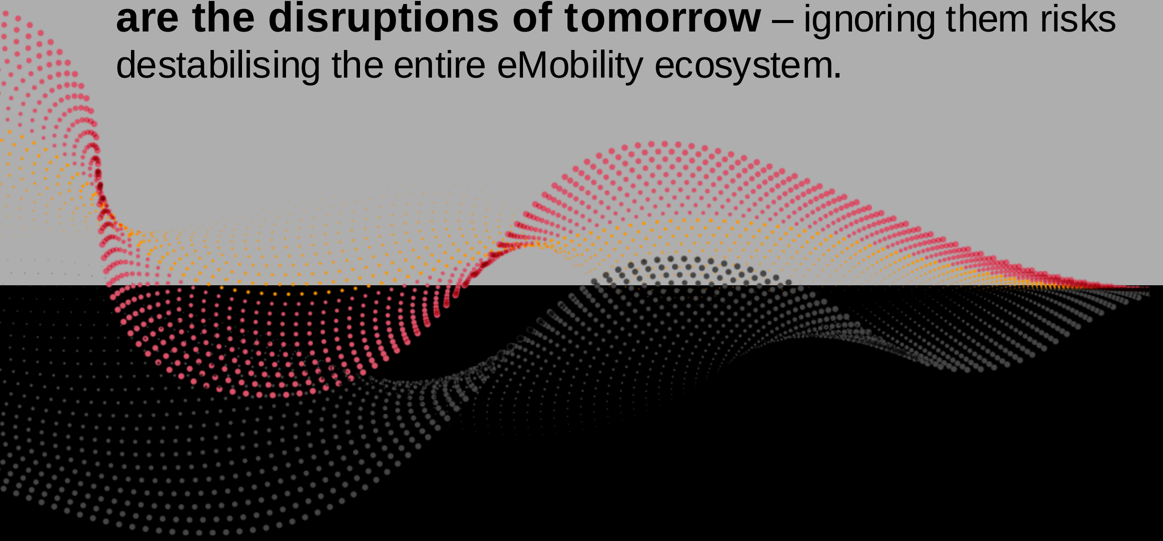
As the adoption of electric vehicles continues to accelerate, the growing **reliance on connected technologies** makes them increasingly vulnerable to cyberattacks…

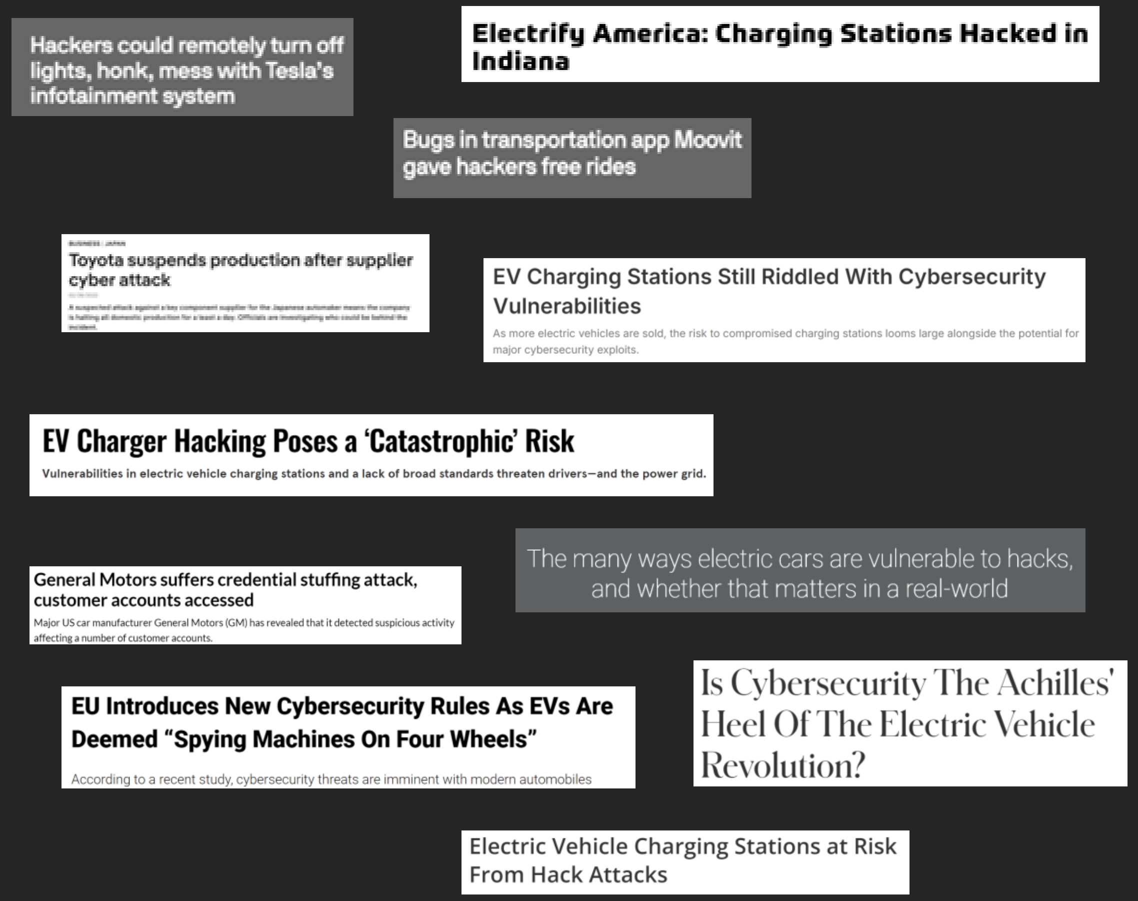
Cyberattacks on energy systems are an increasing global threat[4], as critical infrastructure becomes more interconnected and dependent on digital networks. These attacks can disrupt power generation and distribution, with far-reaching consequences. As energy networks grow more complex, the risk of cyber threats escalates worldwide

03 Cybersecurity imperatives for the eMobility transition

This rising threat extends to the electric vehicle ecosystem. Recent reports highlight that cyberattacks targeting electric vehicles and their supporting infrastructure are no longer just a theoretical concern, but a growing reality. Several high-profile incidents, as seen in (Figure 2), have already demonstrated the vulnerabilities of electric vehicles and charging networks to malicious actors, making them a potential entry point for wider disruptions in the energy grid.

… In an interconnected world, **the vulnerabilities of today are the disruptions of tomorrow** – ignoring them risks destabilising the entire eMobility ecosystem.





Hackers could remotely turn off lights, honk, mess with Tesla's infotainment system

Electrify America: Charging Stations Hacked in Indiana

Bugs in transportation app Moovit gave hackers free rides

BUSINESS | JAPAN

Toyota suspends production after supplier cyber attack

[illegible]

A suspected attack against a key component supplier for the Japanese automaker means the company is halting all domestic production for at least a day. Officials are investigating who could be behind the incident.

EV Charging Stations Still Riddled With Cybersecurity Vulnerabilities

As more electric vehicles are sold, the risk to compromised charging stations looms large alongside the potential for major cybersecurity exploits.

EV Charger Hacking Poses a 'Catastrophic' Risk

Vulnerabilities in electric vehicle charging stations and a lack of broad standards threaten drivers—and the power grid.

General Motors suffers credential stuffing attack, customer accounts accessed

Major US car manufacturer General Motors (GM) has revealed that it detected suspicious activity affecting a number of customer accounts.

The many ways electric cars are vulnerable to hacks, and whether that matters in a real-world

EU Introduces New Cybersecurity Rules As EVs Are Deemed "Spying Machines On Four Wheels"

According to a recent study, cybersecurity threats are imminent with modern automobiles

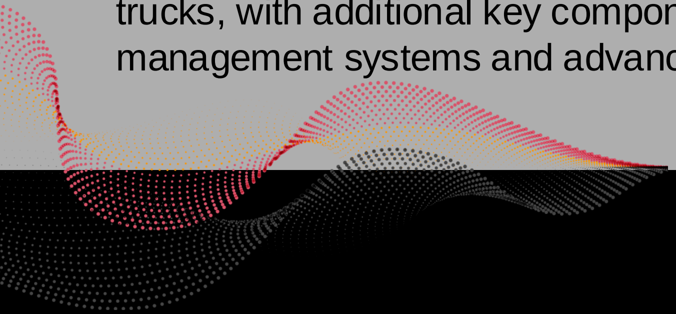
Is Cybersecurity The Achilles' Heel Of The Electric Vehicle Revolution?

Electric Vehicle Charging Stations at Risk From Hack Attacks

Figure 2: Examples of recent incidents highlighting the vulnerabilities of the eMobility ecosystem to cyberattacks and malicious actors

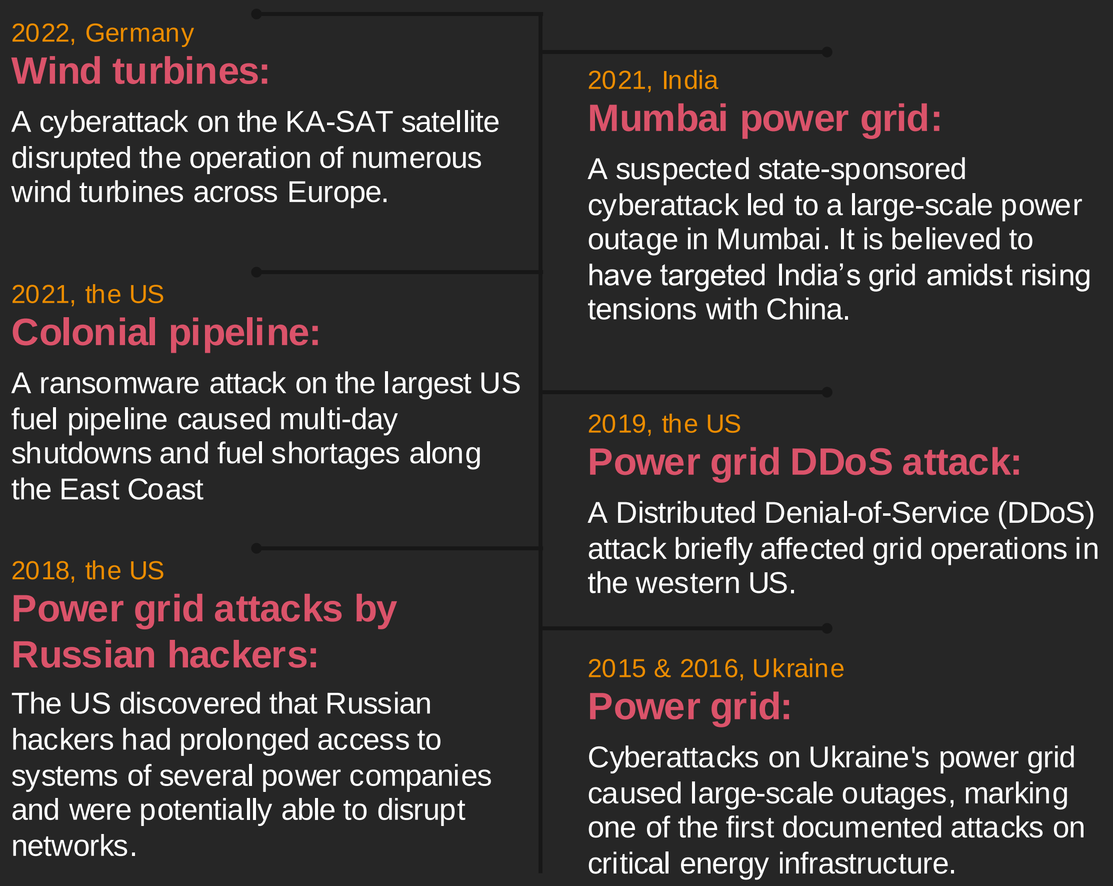
03 Cybersecurity imperatives for the eMobility transition

EVs, including those operated by batteries (BEVs) and Plug-in Hybrid (PEHVs)[5], use electric motors and batteries charged by the power grid. They range from two-wheelers to e-buses and trucks, with additional key components like power electronics, management systems and advanced software interfaces.



Although the grid has not yet faced a cyberattack specifically targeting electric vehicles or their equipment, the risk remains imminent. As adversaries increasingly target critical energy infrastructure, cyberattacks – ranging from ransomware to state-sponsored disruptions – exploit vulnerabilities in our interconnected systems. These attacks could lead to power outages, fuel shortages and significant economic damage, compromising grid reliability and national security. Such disruptions can result in millions of euros in operational costs to restore power, with blackout-related expenses.

Therefore, grids can serve as points of compromise to target EV infrastructure, and Figure 3 (below) highlights multiple instances where grids were the subject of cybersecurity attacks.



2022, Germany

Wind turbines:

A cyberattack on the KA-SAT satellite disrupted the operation of numerous wind turbines across Europe.

2021, the US

Colonial pipeline:

A ransomware attack on the largest US fuel pipeline caused multi-day shutdowns and fuel shortages along the East Coast

2018, the US

Power grid attacks by Russian hackers:

The US discovered that Russian hackers had prolonged access to systems of several power companies and were potentially able to disrupt networks.

2021, India

Mumbai power grid:

A suspected state-sponsored cyberattack led to a large-scale power outage in Mumbai. It is believed to have targeted India's grid amidst rising tensions with China.

2019, the US

Power grid DDoS attack:

A Distributed Denial-of-Service (DDoS) attack briefly affected grid operations in the western US.

2015 & 2016, Ukraine

Power grid:

Cyberattacks on Ukraine's power grid caused large-scale outages, marking one of the first documented attacks on critical energy infrastructure.

Figure 3: There have been several high-profile cyberattacks on power infrastructure over the past decade

[5] Fuel Cell Electric Vehicles (FCEVs) are also EVs, where the energy is stored as hydrogen in a high-pressure tank. However, these vehicles are not connected to the public power grid, which is why they are not considered in this white paper.

04

Securing the eMobility **value chain**

04 Securing the eMobility value chain

Multiple potential attack vectors could disrupt the entire electric vehicle value chain…

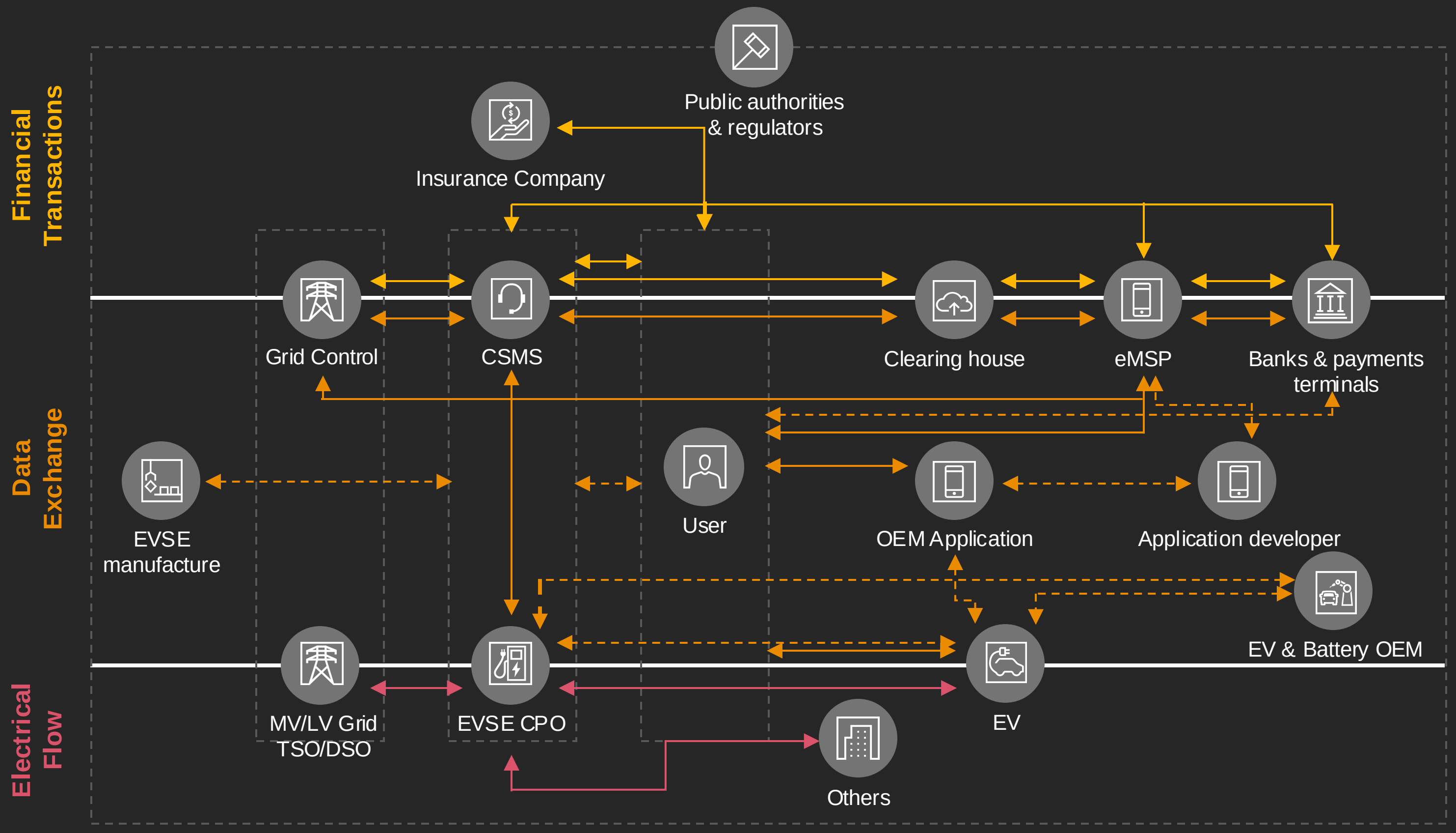
The eMobility value chain is a complex, interconnected ecosystem involving multiple stakeholders from various sectors, making it highly susceptible to cyber threats. The integration of advanced wireless and cloud technologies enhances the capabilities and convenience of EVs but also introduces significant cybersecurity challenges. The decentralised, distributed and interconnected nature of EV systems creates numerous attack vectors, necessitating heightened vigilance and a proactive cybersecurity approach.

Key vulnerabilities in the eMobility value chain include widespread internet connectivity, reliance on mobile apps and inconsistent security protocols. The diversity of components and actors further complicates security efforts and limited physical security measures increase the risk of attacks.

04 Securing the eMobility value chain

The energy sector remains a prime target in the cyber threat landscape[6], given the complexity of the operating environments and the potential impacts. Electrification of the mobility ecosystem significantly increases the attack surface – the number of possible points where an unauthorised user can access a system[7] – as seen in Figure 4 (below).

Securing EV infrastructure is not only vital for public safety but also essential for protecting vehicle owners and the broader community.



*Other: Buildings, Houses, Vehicles, Loads, etc.

- ↔ Electrical Flow
- ↔ Data Exchange
- ⇠ ⇢ Temporarily Data Exchange
- ↔ Financial Exchange

Figure 4: A simplified overview of the various transactions between stakeholders, all of which are vulnerable to cyberattacks.

05

The future of eMobility: **Cybersecurity driving innovation**

05 The future of eMobility: Cybersecurity driving innovation

With EVs becoming smarter and cyber threats more advanced, the eMobility sector is accelerating towards a future where cybersecurity is the new horsepower.

The EV transition is driven by convergent technologies that are transforming industries and accelerating the shift to sustainable transportation. Key priorities include enhancing the cybersecurity of eMobility infrastructure; integrating AI to predict and mitigate cyber risks; and addressing emerging threats to operational technology in sectors such as transportation and energy.

Consumer concerns and preferences:

Around 60% of electric vehicle owners in the US express concerns over the cybersecurity of their vehicles and charging systems[12]. Middle Eastern consumers are particularly focused on the security of connected systems in electric vehicles, preferring vehicles that integrate advanced cybersecurity features to ensure safe charging and vehicle operation. Given the rising temperatures in a desert climate, manufacturers are enhancing battery cooling systems, but cybersecurity measures for such systems is becoming increasingly critical[13,14,15].

Rapid global growth of the EV cybersecurity market:

The global market for automotive cybersecurity is projected to grow at a compound annual growth rate (CAGR) of 18.5%, reaching approximately US$6 billion by 2028. This growth is fueled by the increasing adoption of connected EVs and their reliance on software, making them attractive targets for cyberattacks[8,9].

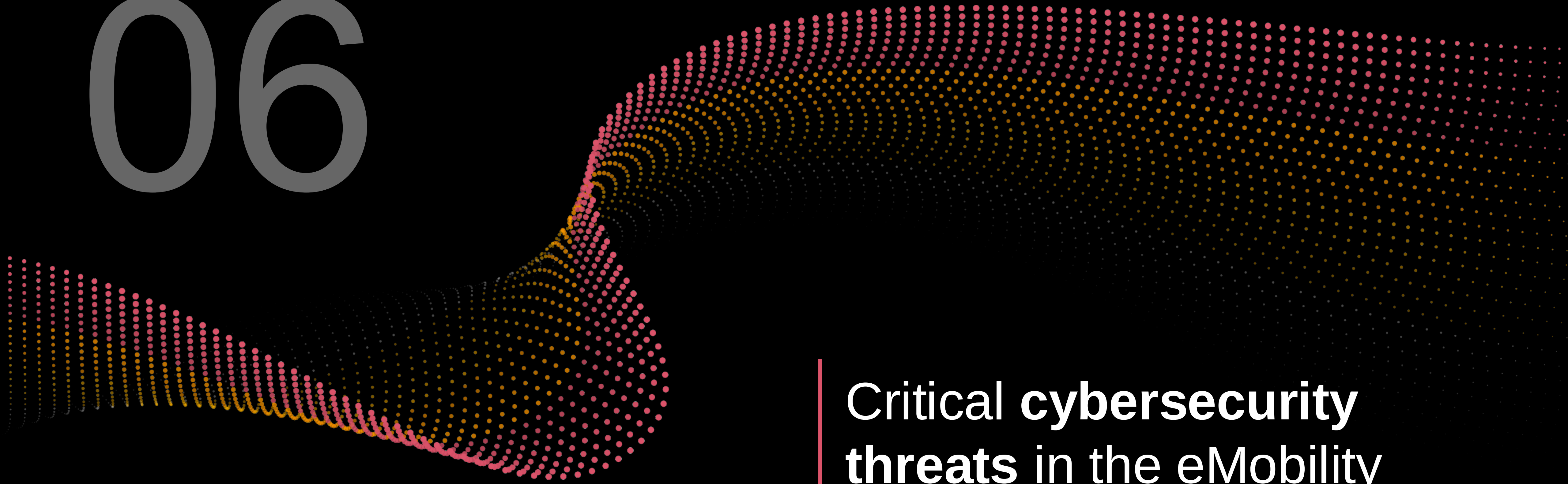
Regulatory enhancements and compliance:

The United Nations Economic Commission for Europe (UNECE) cybersecurity standards, including UN R 155 and UN R 156[10], became mandatory in July 2024. Regional governments are bolstering their cybersecurity frameworks to align with these global standards while addressing local challenges. This includes the adoption of AI-driven cybersecurity solutions to secure data and prevent sophisticated threats in emerging spaces like eMobility[11].

Increased cybersecurity investment:

Spending on cybersecurity solutions in the region is forecasted to grow by over 10% year-on-year, reaching US$6.2 billion in 2024. This growth is driven by the increasing adoption of digital technologies and smart infrastructure in sectors like electromobility[16].

06



Critical **cybersecurity threats** in the eMobility sector

06 Critical cybersecurity threats in the eMobility sector

The eMobility sector faces critical cybersecurity threats that could disrupt operations, compromise safety and expose data, making robust security essential.

With the increasing connectivity and complexity of electric vehicles and their infrastructure, ensuring robust cybersecurity measures is more critical than ever. Below, Figure 5 explores some of the most pressing cybersecurity threats in the eMobility sector, along with examples to illustrate the potential risks and impacts.

Threat	Description	Examples	Impact level
Ransomware attacks	Significant threat with attacks nearly doubling in recent years. Targets critical infrastructure, including charging stations and vehicle control systems	A ransomware attack targeting a network of EV charging stations or an attack that locks down vehicle control systems in a fleet of electric buses.	5
Remote vehicle manipulation	Hackers can gain control over critical vehicle functions such as braking, steering and acceleration, posing significant safety risks.	Hackers can gain control over critical vehicle functions such as braking, steering and acceleration, posing significant safety risks.	5
Data breaches and leaks	Targets sensitive data, including user credentials, employee information and intellectual property. Used for financial gain or other malicious activities.	Targets sensitive data, including user credentials, employee information and intellectual property. Used for financial gain or other malicious activities.	4
Supply chain vulnerabilities	The eMobility sector relies on a complex supply chain. A breach in any part can have widespread implications.	The eMobility sector relies on a complex supply chain. A breach in any part can have widespread implications.	4
Denial-of-Service (DoS) attack	Disrupts vehicle systems or charging infrastructure, rendering them inoperable and causing significant inconvenience.	A DoS attack can disable a city's network of EV charging stations or disrupt fleet management by targeting vehicle communication systems.	4

06 Critical cybersecurity threats in the eMobility sector

Threat	Description	Examples	Impact level
Legacy systems	Older systems not designed with cybersecurity in mind may be more vulnerable to attacks. Upgrading these systems is costly and complex.	An older fleet of electric buses with outdated software being hacked or legacy charging stations with outdated security protocols being targeted.	3
Spoofing attacks	Attackers present false information to vehicles, potentially leading to incorrect navigation or other critical errors.	A spoofing attack misleading a vehicle's GPS system or false data being fed to autonomous vehicles may cause unsafe driving decisions.	3
Regulatory compliance	Keeping up with evolving cybersecurity regulations and standards is challenging. Non-compliance can result in legal penalties and loss of consumer trust.	An EV manufacturer facing fines for not adhering to new cybersecurity regulations or failure to comply with data protection laws resulting in financial penalties.	3
Payment method security	As eMobility services increasingly rely on digital payment methods, securing these transactions is crucial to prevent fraud and theft.	A cyberattack on a charging network's payment system could lead to unauthorised transactions and financial losses. Alternatively, hackers could place fake QR code stickers on charging stations to scam users.	3
Consumer awareness	Many consumers are not fully aware of the cybersecurity risks associated with connected and autonomous vehicles.	Consumers not updating their vehicle's software, leaving it vulnerable to cyber threats or lack of awareness about phishing scams leading to compromised vehicle security.	2

Figure 5: The eMobility ecosystem faces a wide range of critical threats

06 Critical cybersecurity threats in the eMobility sector

Addressing these threats and issues requires a multifaceted approach, including robust cybersecurity frameworks, continuous monitoring and collaboration across the industry.

Severe risks are facing eMobility stakeholders, as these threats can target multiple areas and lead to significant consequences across all levels.

06 Critical cybersecurity threats in the eMobility sector

After identifying the current threats and challenges in the eMobility sector, it is crucial to assess the specific risks these threats pose to stakeholders. These risks can have a significant effect on financial stability, operational efficiency and consumer trust. Below, we outline the key cybersecurity risks in the eMobility sector, offering context for each to underscore their potential impact.

Financial loss

due to ransomware attacks demanding payments and fraud from intercepted payment information

1

Technical vulnerabilities

in legacy systems and supply chain components that can be exploited by hackers

2

Operational disruptions

from denial-of-service attacks that can disable charging stations and vehicle systems

3

Safety hazards

arising from remote vehicle manipulation may lead to potential accidents and unsafe driving conditions

4

Regulatory non-compliance

leading to legal penalties and costly recalls if cybersecurity standards are not met

5

Reputational damage

due to data breaches and security incidents that erode consumer trust

6

Consumer trust issues

from lack of awareness and education about cybersecurity risks, making users more vulnerable

7

Data privacy violations

resulting from data breaches that expose sensitive personal and company information

8

Service outages

due to attacks on charging infrastructure and vehicle systems, causing inconvenience and loss of service

9

Identity theft and fraud

from intercepted payment information and data breaches, leading to financial and personal data misuse

10

Given the potential for severe consequences across all levels, it is crucial to prioritise and address these cybersecurity risks with the highest level of importance. Stakeholders must implement comprehensive cybersecurity strategies to safeguard against these threats and ensure the continued growth and safety of the eMobility sector.

07

Recommendations for eMobility stakeholders

07 Recommendations for eMobility stakeholders

Ensuring cybersecurity within the eMobility sector requires co-ordinated efforts from different parties:

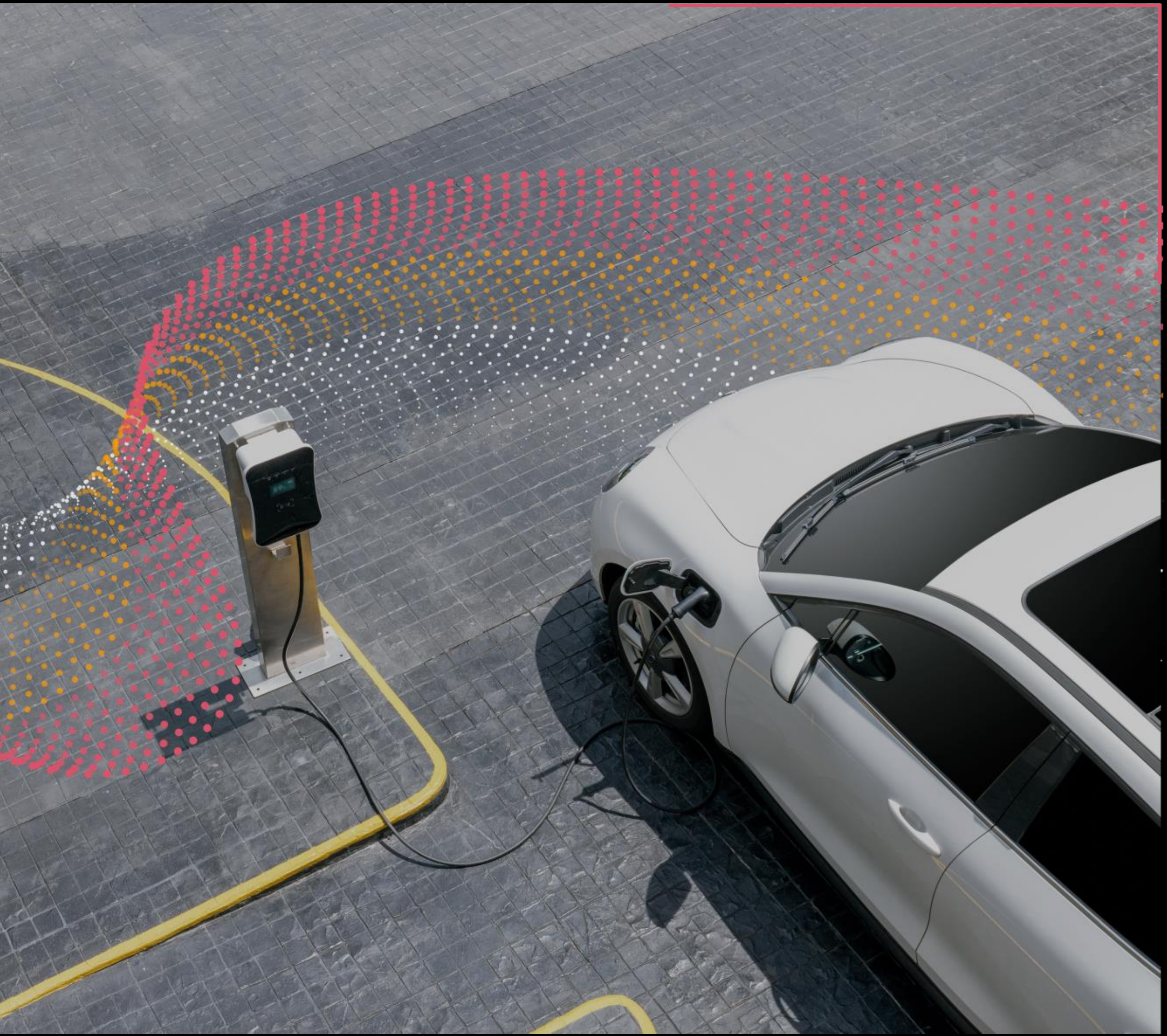
1 | Government and regulatory bodies

- Develop and enforce comprehensive cybersecurity standards, guidelines and policies for the overall EV supply chain.
- Educate EV owners and operators about best practices to enhance overall security.

2 | Utility companies

- Segment the network to protect electric vehicle charging infrastructure from other critical systems.
- Invest in real-time monitoring systems to quickly identify and respond to suspicious activities.
- Incorporate technologies to predict and prevent potential issues within the grid.

07 Recommendations for eMobility stakeholders



3 Banks and payment terminals

- Ensure all payment processing systems are compliant with Europay, Mastercard, and Visa (EMV) standards to enhance security.
- Implement advanced algorithms to monitor and identify suspicious transactions related to EV charging and payments.
- Enhance user experience with features like one-click payments, contactless options and e-wallet integration

4 EV owners

- Keep the vehicle's software up to date to protect against vulnerabilities.
- Prefer trusted and secure charging stations, avoiding those without visible security measures such as dynamic QR codes and authentication systems.
- Protect personal data by enabling privacy settings in vehicle infotainment systems and apps.

07 Recommendations for eMobility stakeholders

5 Insurance companies

- Create and maintain plans to quickly address and mitigate the impact of cyber incidents.
- Collaborate with Original Equipment Manufacturers (OEMs) and Charging
- Point Operators (CPOs) to simplify the claims process for incidents involving EVs and charging stations.

6 EV original equipment manufacturers

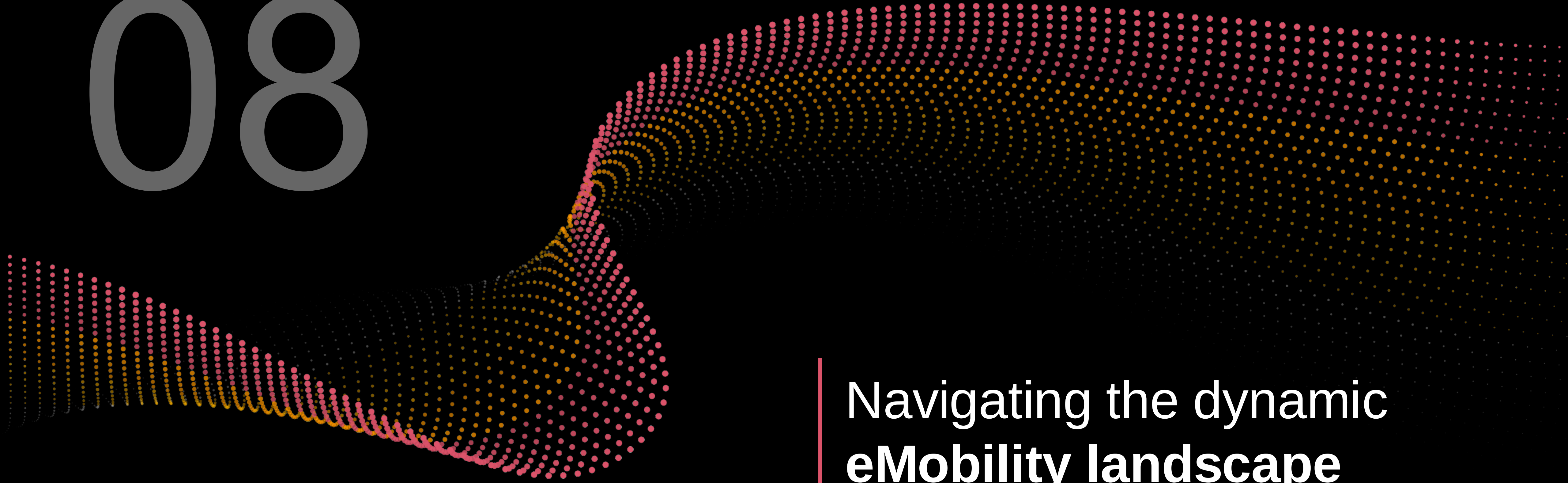
- Work with ecosystem members to design, test and implement robust cybersecurity protocols and standards.
- Continuously identify and mitigate potential threats to ensure vehicle and infrastructure security.
- Coordinate with giga factories to maintain battery security under the Extended Producer Responsibility policy approach, which assigns producers responsibility for the end of life of products[17].
- Incorporate endpoint protection, encryption and secure OTA updates, aligning with UN Economic Commission for Europe cybersecurity standards such as R155 and 156[18].
- Provide comprehensive security training to dealerships and service centres to enhance overall vehicle security.

07 Recommendations for eMobility stakeholders

7 | Charging point operators and eMobility service providers

- Use strong encryption protocols to secure data between charging stations and backend systems.
- Ensure only authorised personnel can access critical systems and data through robust access control mechanisms.
- Engage with EVSE manufacturers for timely security updates on technical components and software.
- Implement tokenisation, EMV compliance and payment card industry data security standards[19] to enhance transaction security.
- Introduce demand-response mechanisms and dynamic pricing, offering real-time monitoring and alerts for station availability and security.

08



Navigating the dynamic **eMobility landscape**

08 Navigating the dynamic eMobility landscape

The eMobility ecosystem is rapidly evolving, with significant adoption of Electric Vehicles (EVs) in the UAE and Saudi Arabia. The sector encompasses an intricate web of industries such as charging infrastructure, battery production, energy management, the public sector and payment systems. Emerging technologies like 5G, IoT, AI and smart charging are driving innovation but also increasing cybersecurity vulnerabilities.

Cyberattacks on the EV ecosystem pose significant risks, including financial losses, operational disruptions, regulatory penalties and safety hazards. These threats target stakeholders including EV manufacturers, charging operators, utilities and consumers. The industry faces regulatory pressure, growing consumer concerns and evolving attack vectors like ransomware, data breaches and vehicle manipulation.

Stakeholders should think about different domains when it comes to the eMobility ecosystem, including:

1. Rapid electric vehicle adoption requires extensive investment in charging infrastructure, particularly in countries like the UAE and Saudi Arabia.
2. Transitioning to renewable energy-powered charging infrastructure to reduce dependence on fossil fuels, enhance grid resilience and promote sustainability is increasingly becoming a necessity.
3. Collaborative efforts across industries and government bodies are essential to meet ambitious targets pertaining to the eMobility ecosystem.
4. The eMobility ecosystem's reliance on connectivity and digital infrastructure increases its susceptibility to cyber threats. Stakeholders must focus on securing each component of the value chain, from charging stations to vehicle systems.
5. Cybersecurity must move beyond compliance to a proactive, strategic priority, involving routine audits, penetration testing and employee training to ensure a robust, secure and reliable eMobility ecosystem.

08 Navigating the dynamic eMobility landscape

6

Emerging technologies such as bidirectional charging and AI-driven energy management promise efficiency but demand robust security protocols. Compliance with the latest global and regional cybersecurity standards is vital for business continuity and consumer trust.

7

Cyberattacks can cause large-scale disruptions, financial losses and safety issues. It is imperative that consumers be educated and that payment systems are secured for fostering trust in the ecosystem.

8

Collaboration between companies in the EV ecosystem, from manufacturers to service providers, is required to develop secure, seamless and integrated solutions.

9

Players like charging point operators and utility companies must align on standards, infrastructure scalability and energy management to meet future eMobility demand.

10

Governments must think about standardisation and enforcement of eMobility cybersecurity policy frameworks to address unique regional eMobility challenges. Partnerships could also be established with private entities to accelerate EV infrastructure development and ensure its security.

Contact us

Heiko Seitz

Partner
Global and ME eMobility Leader
Heiko.Seitz@pwc.com

Raddad Ayoub

Partner
Raddad.Ayoub@pwc.com

Dr. Jonas Wussow

Manager
Jonas.w.Wussow@pwc.com

Dr. Bassem Haidar

Manager
Bassem.Haidar@pwc.com

Ahmad Shah

Manager
Ahmad.Shah@pwc.com

References

[1] IEA (2023), **Global EV outlook 2023 Trends in electric cars**, https://www.iea.org/reports/global-ev-outlook-2024/trends-in-electric-cars

[2] PwC Middle East (2024), **KSA eMobility Outlook**, https://www.pwc.com/m1/en/publications/documents/2024/emobility-outlook-2024-ksa-edition.pdf

[3] PwC Middle East (2024), **UAE eMobility Outlook**, https://www.pwc.com/m1/en/publications/documents/2024/emobility-outlook-2024-uae-edition.pdf

[4] Ferris, N., Van Renssen, S., & Ferris, N. (2021, February 17). **Cybersecurity threats escalate in the energy sector**. Energy Monitor. https://www.energymonitor.ai/digitalisation/cybersecurity-threats-escalate-in-the-energy-sector/?utm_source=chatgpt.com&cf-view

[6] PwC Threat Intelligence (2024), **Under The Lens - The Energy Sector**, https://www.pwc.de/de/energiewirtschaft/under-the-lens-the-energy-sector.pdf

[7] https://www.cloudflare.com/learning/security/what-is-an-attack-surface/

[8] https://www.marketsandmarkets.com/Market-Reports/cyber-security-automotive-industry-market-170885898.html

[9] https://www.statista.com/outlook/mmo/electric-vehicles/worldwide

[10] https://www.appluslaboratories.com/global/en/news/publications/new-cybersecurity-regulations-vehicles-unece-wp29

[11] https://unece.org/sustainable-development/press/un-regulations-cybersecurity-and-software-updates-pave-way-mass-roll

[12] Aljohani, T., Almutairi A. (2024), **A comprehensive survey of cyberattacks on EVs: Research domains, attacks, defensive mechanisms, and verification methods** https://www.sciencedirect.com/science/article/pii/S221491472400151X /

https://www.thehindu.com/sci-tech/technology/are-uss-cybersecurity-concerns-over-chinese-evs-justified/article68745519.ece#:~:text=An%20attack%20on%20an%20EV's,ripple%20effect%20of%20security%20vulnerabilities.

[13] The Hindu (2024), **Are U.S.'s cybersecurity concerns over Chinese EVs justified?,** https://www.thehindu.com/sci-tech/technology/are-uss-cybersecurity-concerns-over-chinese-evs-justified/article68745519.ece

[14] Alotaibi, S. A., Alghamdi, M. A., & Alzahrani, A. H. (2024). **The impact of electric vehicle adoption on urban air quality in Riyadh**. Journal of Transport & Health, 24(4), 151-162. https://doi.org/10.1016/j.jth.2024.10015

[15] Brighente, A., Conti, M., Donadel, D., Poovendran, R., Turrin, F., & Zhou, J. (2023). **Electric Vehicles Security and Privacy: Challenges, Solutions, and Future Needs**. IEEE Transactions on Intelligent Transportation Systems. https://doi.org/10.48550/arXiv.2301.04587

[16] IT Security Spending in the Middle East and Africa to See Double-Digit Growth in 2024, According to Latest IDC Forecast, https://www.idc.com/getdoc.jsp?containerId=prMETA51977024#:~:text=Johannesburg%20%E2%80%93%20Spending%20on%20security%20products,International%20Data%20Corporation%20(IDc).

[17] https://epr.sustainablepackaging.org/

[18] https://www.appluslaboratories.com/global/en/news/publications/new-cybersecurity-regulations-vehicles-unece-wp29

[19] https://www.pcisecuritystandards.org/standards/