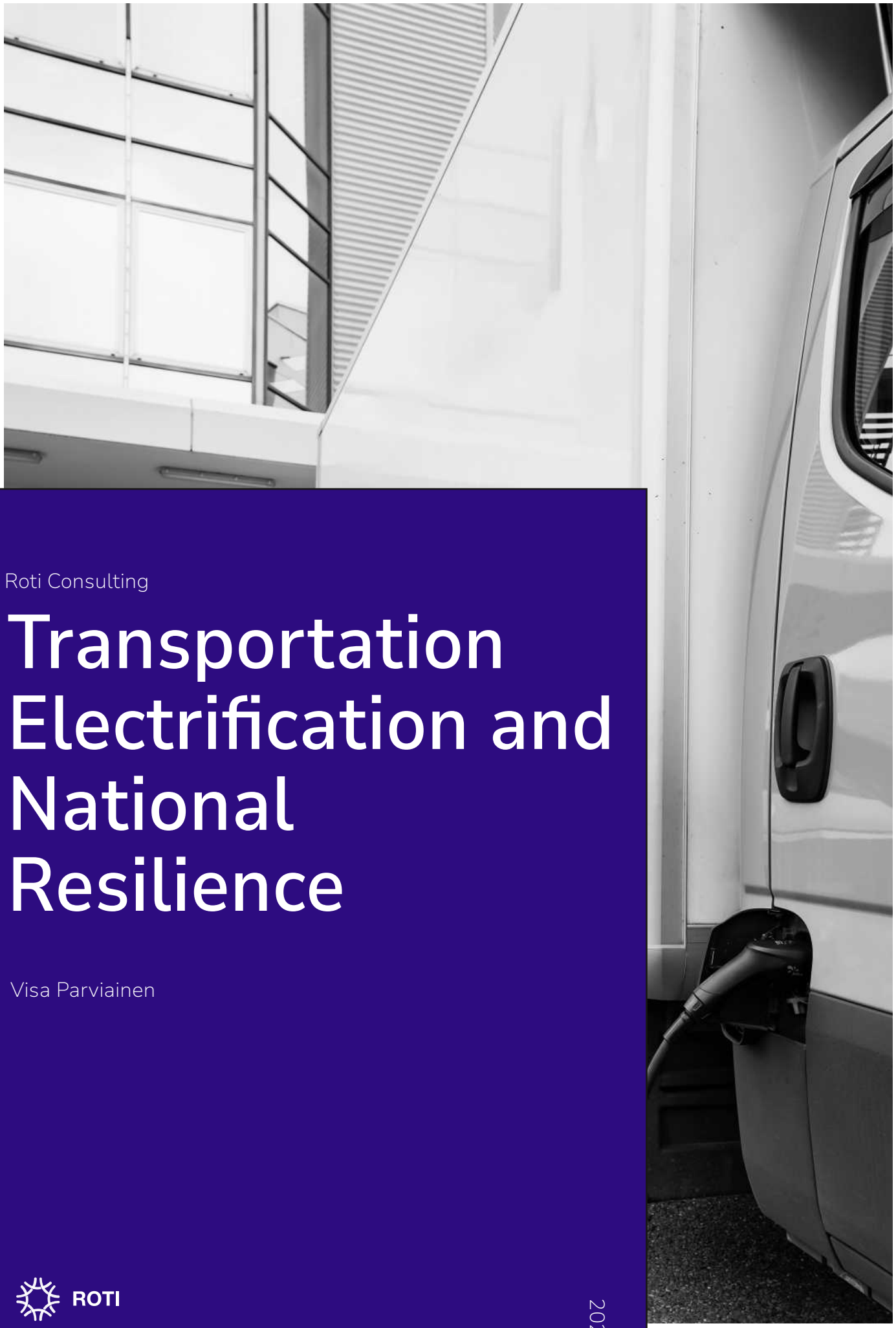

Roti Consulting

Transportation Electrification and National Resilience

Visa Parviainen

ROTI

2024

Table of Contents

Introduction

The rapid electrification of transport is transforming logistics and personal mobility at a pace that few could have predicted just a decade ago. In an increasingly unstable national security environment, it is crucial to evaluate how a shift towards a mostly or completely electrified transport system can enhance or compromise national resilience.

For the purposes of this paper, national resilience refers to a nation's ability to withstand, adapt to, and recover from disruptions to its critical infrastructure and societal functions. In the context of electrified transport, resilience encompasses the robustness of energy systems, the continuity of logistics and mobility networks, and the ability to maintain essential operations during times of crisis—whether due to natural disasters, cyberattacks, or geopolitical instability.

A resilient transport infrastructure must ensure that even under duress, the nation can continue to deliver goods, maintain supply chains, and provide mobility for both citizens, commerce and government services. This requires not only reliable physical and digital systems but also the ability to adapt to and mitigate emerging risks tied to new technologies, such as electric vehicle charging networks and energy management systems. We have intentionally scoped out military, aviation and marine as electrification in these environments will take significantly longer than road transport, with some exceptions addressed below.

Electrified transport offers clear environmental and operational benefits, but it also introduces new dependencies, particularly on the electric grid and digital infrastructure. This white paper explores how the move toward electric vehicles (EVs) affects a nation's ability to maintain critical operations and infrastructure under duress. It aims to assess both the risks and opportunities presented by electrification and outline strategies to mitigate vulnerabilities while maximizing the resilience benefits of an electrified transport system.

For the purposes of this paper, we will focus on the following risk scenarios:

Supply Chain Disruptions

The electrification of transport relies on global supply chains for critical materials like lithium, cobalt, and nickel, as well as specialized components for chargers, batteries and electric drivetrains. Any disruption—whether due to geopolitical tensions, trade restrictions, or logistical challenges—could prevent maintenance, repair and deployment of charging infrastructure or vehicles and over time significantly affect the transport system of a country.

> Critical functions essential to societal security, such as fuel distribution, EV charging networks, and the supply of daily goods, must remain operational during extended power outages.
>
> *Finnish Government TEM/2024/142*

Cyberattacks

As electric vehicle infrastructure becomes increasingly digitized, from smart charging stations to energy management systems, it presents a growing target for cyberattacks. Malicious actors could disrupt charging networks, tamper with energy allocation, or compromise fleet management systems, potentially leading to widespread logistical failures. Cyberattacks on critical transport infrastructure could result in the paralysis of entire fleets, making them vulnerable to ransomware or sabotage, and could have cascading effects across other sectors reliant on transportation. While these concerns also apply to liquid fuel dispensing infrastructure, an a truck with an internal combustion engine (ICE) can be refueled with a 10€ plastic canister but a heavy electric truck has more complex needs.

Actions by Nation-States

Recent conflicts, such as Russia's war on Ukraine, highlight the threat posed by nation-states targeting energy production and distribution infrastructure. As electric transport systems become increasingly integrated into national grids, these networks are exposed to new strategic risks. Direct attacks, such as missile strikes on power stations, or indirect methods like demand manipulation to destabilize energy production balance, could severely impair a nation's logistics, emergency transport, and military readiness. In the context of armed conflict or political instability, the importance of the electrical grid grows as charging infrastructure begins to replace fuel dispensing as a critical component of national security.

In addition to power infrastructure, navigation systems have increasingly been a target of radio jamming attacks. The longer charging time and relative to refueling leads electric vehicles to rely more on connected systems for planning their charging stops, all of these systems rely on global navigation satellite systems which are all too easy to disrupt.

Natural Disasters and Extreme Weather Events

As climate change drives more frequent and severe natural disasters, the physical infrastructure for charging and energy distribution will be under increasing threat. Floods, wildfires, hurricanes, and heatwaves could damage charging stations, cut off power to key regions, or even disable the grid. Ensuring the ability to charge vehicles in these situations, as well as maintaining transport for evacuation and emergency response, is critical for national resilience.

Grid Overload and Energy Supply Disruptions

With the rapid rise in electricity demand due to decarbonization across industries and the introduction of volatile renewable production, national grids could face severe stress, especially during peak times or in areas with inadequate infrastructure. The resilience of energy generation and distribution is crucial to avoid large-scale disruption of electrified transport.

Navigation system interference near Helsinki, December 2024, gpsjam.org

Opportunities

Although we focus on new risks and their mitigation, it's important to recognize that electrification of transport also presents many benefits and opportunities reaching beyond energy independence.

Energy Independence and Security

Electrifying transport reduces reliance on imported oil, a critical factor in enhancing national security. Traditional ICE vehicles depend heavily on a steady supply of fossil fuels, often sourced from geopolitically unstable regions and frequently transported through sea or pipelines which are vulnerable to disruption. By transitioning to electric vehicles powered by domestic energy sources, nations can reduce their vulnerability to external energy supply disruptions.

Additionally, electrification promotes the use of renewable energy sources, such as solar, wind, and hydropower, which are often produced locally. This shift not only strengthens energy independence but also helps decentralize energy generation, making the grid less susceptible to centralized points of failure. Local power generation through renewable resources provides greater flexibility and resilience to energy systems, allowing for the continued operation of transport networks even during broader disruptions.

Enhanced Efficiency and Reliability

Electric vehicles feature simpler drivetrains compared to traditional ICE vehicles, with far fewer moving parts. This simplicity translates into lower maintenance needs, fewer points of failure, and increased reliability for logistics operations and personal mobility. Electric drivetrains, with their reduced mechanical complexity, help streamline supply chains, as fewer specialized parts and services are required to keep fleets operational.

Another key advantage is that electric vehicles can be recharged using basic equipment, such as a portable AC chargers. The onboard chargers built into many EVs allow them to be charged from standard electrical outlets, introducing an element of distribution that enhances resilience, at least for lighter vehicles. This ability to recharge from distributed energy sources—whether at homes, offices, or emergency charging points—offers flexibility that traditional fuel-based systems cannot deliver. This enhances the nation’s ability to maintain mobility in crisis situations when fuel supplies may be disrupted or access to refueling stations or payment systems may be limited.

Future opportunities

The integration of Vehicle-to-Grid (V2G) technology presents a major opportunity

for strengthening national resilience. V2G systems allow electric vehicles to serve as mobile energy storage units, capable of feeding electricity back into the grid during peak demand or emergencies. This ability transforms fleets of EVs into potential energy reserves, providing additional grid stability and flexibility. In addition to supporting the grid, some EVs allow their owner to power their house or equipment, a capability termed Vehicle-to-load (V2L). This ability doesn't affect the grid directly, but mitigates the effects of local outages for non-transport power use.

Further resilience is achieved through the installation of site batteries at EV charging hubs. These batteries can store energy during off-peak hours or from renewable sources, acting as a buffer for the grid during periods of high demand. In the event of grid disruptions, these batteries can ensure continuous charging availability, particularly for critical services and emergency vehicles and support grid balance during normal operation.

Even without the support of V2G/V2L or site batteries, charging infrastructure itself can act as a balancing force for the electrical grid. Chargers can be made to stop charging to prevent a grid overload, giving time for backup production to be brought online. The temporary reduction (or increase) of power consumption to support the power grid is called demand response and is a familiar approach to many power system operators – electric vehicles and their chargers simply provide a new, distributed resource to tap into.

New Risks

Like any new technology that permeates the core of society, electrification of transport also introduces it's share of issues and risks that need to be managed. Some of them are similar to the ones encountered by societies with mostly chemical fuels in transport, others entirely new.

Increased Dependency on the Electric Grid

The electrification of transport introduces the electrical grid as a direct dependency to power both logistics operations and personal mobility. Disruptions to the grid —whether through power outages, cyberattacks, or technical failures—could paralyze transportation networks, affecting everything from supply chains to emergency response capabilities.

Grid overload is another significant risk, especially during peak demand times. Large-scale vehicle charging can place tremendous strain on the grid, potentially leading to further volatility on the power market and additional peak power production. Mitigation of these risks will require the introduction of market mechanisms guiding technical control systems, which will shift demand to follow production instead of the other way around.

Cybersecurity Vulnerabilities

Electrified transport infrastructures introduce a vastly expanded attack surface for potential cyberattacks.

Charging networks, communication protocols, and cloud-based platforms that manage chargers, vehicle fleets and energy demand are all vulnerable to intrusion. As these systems become more interconnected, a successful cyberattack could have far-reaching consequences.

A Ukranian power plant was destroyed in a Russian missile attack in March 2024.

Photo credit DTEK Energy

Charge point management systems (CPMS), Energy Management Systems (EMS), are a particularly sensitive target. Compromising these systems to manipulate energy demand could destabilize local grids or even cause cascading failures if widespread manipulation of energy flows occurs. Moreover, the reliance of public charging networks on digital payment systems and remote authentication adds another layer of vulnerability. Attackers could disrupt payment systems, causing financial losses, or manipulate authentication to restrict access to critical charging infrastructure.

Another growing risk is the potential for adversaries to monitor vehicle movements through compromised networks charging. By hacking into fleet management systems or CPMS systems, hostile actors could track vehicle usage patterns, potentially identifying strategic locations such as storage depots, or logistical hubs.

Supply Chain Vulnerabilities for Critical Materials

The shift to electric vehicles intensifies dependency on global supply chains for critical raw materials and complex components. The production of current generation EV batteries relies heavily on key minerals such as lithium, cobalt, and nickel, much of which are sourced from geopolitically unstable regions. Any disruption to these supply chains — whether from trade restrictions, natural disasters, or political conflicts—could delay the production of EVs and fast-charging infrastructure, leading to widespread operational challenges.

Beyond minerals, the complexity of EV systems and fast-charging stations makes the supply chain more fragile. While slow chargers and basic AC equipment are relatively simple to construct and trivial to maintain, fast DC chargers require advanced components and regular access to spare parts that may be harder to source in times of disruption. Ensuring the availability of local manufacturing or securing alternative supply chains for these critical components will be essential to mitigating the risk of supply chain disruptions.

Operational Risks in Disaster Scenarios

Natural disasters pose a significant risk to electrified transport infrastructure. In the

event of hurricanes, floods, or wildfires, physical damage to charging stations or grid components could disrupt charging availability. While ICE vehicles can rely on pre-existing fuel reserves during a disaster, EVs are dependent on an operational power grid or local charging infrastructure. This creates a vulnerability if charging stations are damaged or power is unavailable during critical moments.

Another concern is the dependency of charging infrastructure on international networking and data services. Charging authentication, billing, and network management often depend on cloud services and data centers located outside the country. Additionally, undersea networking cables could be compromised, leaving charging systems inoperable if there's no backup authentication method. Ensuring the resiliency of these systems —either by decentralizing cloud services or by enabling offline functionality during emergencies—will be critical to maintaining operational continuity during disasters.

Electrification and military

While we don't expect ground vehicles which participate in active combat to migrate to fully-electric drivetrains in significant volumes in the foreseeable future, a significant amount of military logistics rely on commercial logistics services using civilian vehicles. This is doubly true of militaries (eg. Finland) which rely on requisitioned vehicles – effectively turning civilian vehicles into military vehicles during time of war. These operational patterns mean that military planners should have an interest in ensuring EV charging networks remain operational and can be expanded towards the relevant operational areas.

Cybersecurity

As transport electrification scales, the attack surface of this infrastructure—referring to all points where a system can be vulnerable to unauthorized access or attacks—expands dramatically. The shift from traditional fossil fuel systems to electric vehicles introduces new layers of digital and physical infrastructure, each of which presents unique risks.

Components of the Attack Surface

In information security, the attack surface refers to the total number of points in a system where an unauthorized user or malicious actor could attempt to enter, interact with, or manipulate that system. The attack surface includes all vulnerabilities in hardware, software, networks, and human factors that could be exploited to compromise the system's security.

The attack surface of an electrified transport system involves multiple interconnected layers of hardware, software, and communication protocols. Each component of this infrastructure presents potential vulnerabilities, which need to be understood and secured to maintain system resilience. The following key components outline critical points within the attack surface:

Charging Infrastructure

Public and private charging stations serve as primary points of interaction between vehicles and the grid. Their dependence on internet connectivity for operational management, user authentication, and billing creates opportunities for physical tampering and cyberattacks. A compromise at this level can disrupt charging services and propagate issues across the broader network.

Charge point management systems

Charge Point Management Systems (CPMS) are central hubs for managing charging infrastructure. They handle operations such as user authentication (including RFID tags and mobile app controls), energy allocation, and billing. RFID tags, commonly used for vehicle identification at charging stations, are typically checked against the cloud-based records managed by CPMS. If the CPMS or its cloud services are compromised, attackers could manipulate or bypass the authentication process, allowing unauthorized users to access charging resources. Similarly, mobile apps rely on CPMS to deliver control commands for initiating and monitoring charging sessions, adding another vector for potential cyberattacks on user data or service availability.

Grid Management Systems

Distribution System Operators (DSOs) and Transmission System Operators (TSOs) manage the balance and stability of electrical grids at various levels. These systems must now handle the additional energy demands from widespread electric vehicle usage. Attacks on DSO or TSO grid management systems could destabilize local or regional grids, affecting not only EV charging but also broader electricity availability for homes and businesses.

Fleet Management and Telematics Systems


ABB

Terra AC wallbox Authentication and Communication Vulnerabilities

CVE ID: CVE-2023-0863, CVE-2023-0864

Notice

ABB's excemplary vulnerability disclosures are also listed in the CVE database making them easy to monitor.

Fleet management systems and vehicle-specific telematics platforms are increasingly used for monitoring and optimizing logistics operations. Telematics systems track real-time vehicle data, from location to battery health, and relay it to fleet managers. Cyberattacks on telematics platforms or fleet management software could lead to the theft or manipulation of sensitive data, disruption of vehicle operations, or delays in logistics. Compromising these systems may also reveal sensitive routes or schedules, posing a security risk for high-value or critical goods.

Transport Management Systems

Transport management systems or TMS play a critical role in coordinating logistics, optimizing delivery routes, and

ensuring timely transport of goods. As with other centralized systems, TMS is a potential target for cyberattacks. Disruptions to these systems could lead to delays in the transport of essential goods, cascading across supply chains and affecting national resilience in sectors such as healthcare, food distribution, or emergency response.

Communication Protocols

Open Charge Point Protocol (OCPP) and ISO 15118 facilitate communication between EVs, charging stations, and backend systems, such as CPMS. Any vulnerabilities in these protocols (and the protocols below them in the networking stack) could be exploited by attackers to intercept sensitive data, alter energy distribution commands, or block access to charging services. Ensuring the security of these communication protocols is essential to maintaining the integrity of the charging network.

Telecommunications Networks

The telecommunications network is the backbone of all communication between charging infrastructure, fleet management systems, and CPMS. This dependency introduces risks if the telecom network experiences outages or is subject to physical sabotage or cyberattacks. A disruption in telecommunications could effectively sever the connection between EVs and the cloud systems managing charging, billing, and fleet operations, paralyzing the system.

Payment and Authentication Systems

Payment systems and user authentication (often through RFID tags or mobile apps) are essential for accessing charging stations and billing services. RFID tags are typically authenticated against CPMS records, making the cloud-based system a key point of vulnerability. Similarly, mobile apps that control vehicle charging also depend on the CPMS for authorization and monitoring. In the context of payments, EV charging services are heavily dependent on the global payment infrastructure. A functioning payment system requires stable connections to multiple actors, including the acquirer, issuer, Payment Service Provider (PSP), and card schemes (such as Visa or Mastercard). Disruptions in any part of this chain—whether through network outages, cyberattacks, or technical failures—can halt payments, preventing users from charging their vehicles. Given the interconnectedness of this global system, securing each part of the payment chain is crucial for the overall resilience of the charging network.

By examining these key components, it becomes clear how each element contributes to the broader attack surface of electrified transport systems. Each of these components, whether related to charging, fleet management, or communication protocols, must be protected to ensure the continued resilience of national transport networks.

Government and Policy

The resilience of electrified transport infrastructure depends on coordinated efforts between government and private sector stakeholders. Governments must establish the necessary policy frameworks, regulations, and incentives, while the private sector is responsible for implementing secure, reliable infrastructure and services. Both play crucial roles in ensuring that the benefits of electrified transport can be realized while minimizing risks.

Policy Recommendations

Governments are uniquely positioned to establish the resilience of electrified transport systems through well-structured policies, regulations, and targeted investments. These areas are critical to securing and strengthening electrified transport infrastructure

Governments should introduce explicit requirements for the resilience of charging networks and related infrastructure through public funding programs and regulation. Key areas include:

Offline Authentication Options

Policies should mandate offline authentication capabilities for charging stations, ensuring they can continue to operate during network disruptions or cyber incidents.

Uptime Requirements

For publicly funded charging infrastructure, regulations should include minimum uptime standards, ensuring that these services remain functional during crises, especially for logistics and emergency services.

Local Spare Parts Availability

To minimize downtime, governments should require operators of publicly funded charging infrastructure to maintain a local supply of critical spare parts. This ensures that repairs can be executed quickly, supporting operational continuity.

Signage requirements

Charging hubs along major roads should be indicated with signage, which include the number and type of available plugs (especially CCS and MCS) to ensure vehicles can find chargers even when navigation systems are inoperable

Roadside signage indicating alternative fueling stations next to a highway, Seoul Korea, 2024

Manual battery preconditioning

Vehicles should allow drivers to manually turn on battery preconditioning prior to arrival. Current approaches rely on the availability of GPS navigation and sometimes only work with a small subset of chargers.

Enforce component level right-to-repair

Being able to repair a charger power module from a DC charger by replacing a faulty fan or a vehicle battery by replacing an individual cell ensures that a small fault doesn't render the asset a total loss when module level spares become scarce.

Grid Modernization and Decentralization

To support the growing demand for electricity from electric vehicles, governments should incentivize investments in grid upgrades, including:

Time-of-Use Power Markets

Implementing or expanding time-based pricing models, such as day-ahead markets, enables consumers to shift energy usage to off-peak times, reducing strain on the grid.

Demand Response Markets

Markets like the Frequency Containment Reserve for Disturbances (FCR-D), existing in the Nordics, allow distributed energy resources (such as EVs and batteries) to participate in grid stabilization efforts. Enabling EVs and energy storage systems to join these markets promotes greater grid flexibility and resilience.

Renewable Integration and Storage Incentives

Governments should provide incentives for integrating renewable energy sources and energy storage at critical infrastructure points, such as major EV charging hubs. This setup can bolster grid stability, reduce dependency on fossil fuels, and maintain charging availability during peak demand or grid instability.

Cybersecurity Standards

Establishing cybersecurity frameworks specifically tailored for electrified transport systems is essential to mitigate unique security risks:

Adopt or Reference Standards

Governments should encourage compliance with existing frameworks, such as the NIST Cybersecurity Framework and ISO/IEC 27001, to protect critical systems like Charge Point Management Systems (CPMS) and grid management platforms

Regulations for Regular Audits

To maintain high security, government policies should require regular cybersecurity audits for operators of electrified transport infrastructure, ensuring ongoing adherence to best practices.

Specific Security Extensions and Protocols: Require standards with enhanced security protocols, such as the OCPP 1.6 security extensions in addition to network level security measures.

Private sector resilience

The private sector, encompassing logistics companies, transport operators, and Charge Point Operators (CPOs), plays a critical role in implementing robust infrastructure and maintaining operational resilience. While governments set the regulatory framework, it is the private sector's responsibility to ensure that these guidelines are translated into actionable measures.

This section breaks down the roles of Transport Companies and CPOs, as both have unique responsibilities, but it should be noted that it's not uncommon for a transport company to also maintain their own charging infrastructure at least to an extent in which case the CPO responsibilities also apply to them.

Transport Companies

Transport companies, particularly those relying on electrified fleets, must be prepared to operate in challenging environments where network connectivity or GPS services may be disrupted. To ensure resilience, transport companies should implement the following practices:

Establish Processes for Operating Without Networks or GNSS

Transport operators should develop and maintain processes to function offline, including distributing physical lists of charging locations and providing drivers with offline authentication methods for charging. This will enable continued operations even when navigation systems are inoperable.

Regularly Test Offline Capabilities

Companies should conduct regular drills to simulate network outages, ensuring that drivers are well-trained to locate charging stations, navigate routes, and authenticate charging sessions without relying on online services.

Maintain Spare Part Availability

To minimize downtime, transport companies should stock critical spare parts for their vehicles. This ensures that repairs can be performed swiftly, particularly during emergencies when supply chains may be disrupted.

Demand Information Security Certifications from Suppliers

Transport companies should require their hardware, software, and service providers to have up-to-date information security certifications (e.g., ISO 27001, IEC 62443). This ensures that suppliers meet stringent cybersecurity standards, reducing the risk of vulnerabilities within the fleet's ecosystem.

Charge Point Operators

Charge Point Operators are responsible for maintaining the infrastructure that powers electrified transport. As operators of critical infrastructure, CPOs must take proactive steps to ensure service

continuity and secure their networks against threats:

Support Offline Authentication

CPOs should mandate support for offline authentication from their backend and charger providers. This includes enabling OCPP 1.6 features, such as whitelisting RFID tags or vehicles, to allow charging even during network outages. If offline authentication is not feasible, chargers should be configured to offer free charging when disconnected from the network to maintain service availability.

Robust Signage at Charging Hubs

Proper signage indicating the presence of charging stations along major routes is essential. This includes displaying the number and type of plugs available (e.g., CCS, MCS) to ensure that drivers can find suitable chargers even without GPS.

Invest in Cybersecurity and Acquire Certifications

CPOs must acquire cybersecurity certifications (e.g., ISO 27001, IEC 62443) and maintain a stringent security posture.

Maintain Redundant Network Connections

Ensuring that charging stations have multiple redundant network connections is crucial for resilience. Ideally, this includes a combination of satellite and cable-based internet connections to avoid single points of failure.

Localize OCPP Backend Operations

CPOs should ensure that their OCPP backends are located as close to the operational area as possible. In the event of prolonged network issues, CPOs should have contingency plans to deploy backend instances in local data centers to ensure service continuity.

Conclusion

Electrification of transport presents an opportunity, but also raises new concerns. Fortunately, the types of challenges presented by the transition are mostly mitigated by familiar structures and processes – good grid design and cybersecurity practices will get us far. The remaining issues of dependance on out-of-country parts and services also apply to many other domains, but are often not sufficiently addressed; In the case of critical infrastructure they must be.

Roti consulting provides services focused in technology evaluations and electromobility.

roticonsulting.com

visa@roticonsulting.com

ROTI