White Paper
of Charging Interface Initiative e.V.

Cable Theft at Charging Stations

2026-09-15

Charging Interface Initiative (CharIN) e.V.
EUREF-Campus 10-11
10829 Berlin Germany

Contact
Phone +49 30 288 8388-0
Fax +49 30 288 8388-19
Mail coordination@charin.global
Web www.charin.global

Contents

1. Executive Summary 4
2. Scope & Purpose 5
3. Problem statement – What is happening? 6
3.1. Vandalism & Tampering 6
3.2. Theft of components – mainly copper 6
4. Impact assessment 8
4.1. Operational Impact 8
4.2. Safety and Liability Impact 8
4.3. Organizational and Administrative Impact 8
4.4. Insurance and Compliance Impact 9
5. Root causes 10
5.1. Economic Drivers and the Metal Market 10
5.2. Technical and Operational Vulnerabilities 10
5.3. Environmental and Site Factors 10
5.4. Regulatory and Market Gaps 11
6. Stakeholder & Responsibilities 12
6.1. Manufacturers and Installers: Security by Design 12
6.1.1. Physical Robustness and Hardware Hardening 12
6.1.2. Active Deterrence & Response 12
6.1.3. Detection & Sensing Layer 13
6.1.4. Controlled Access and Cable Management Concepts 13
6.1.5. Integration with Digital Security Architectures 14
6.2. Charge Point Operators (CPOs) 14
6.3. Public Authorities, Police, and Regulators 14
6.4. Strategic Partners: Insurers and Standards Bodies 15
7. Multi-Layer Anti-Theft Strategy 16
7.1. Layer 1 – Hardened Hardware 17
7.2. Layer 2 – On-Site Physical Security 17
7.3. Layer 3 – Network & Software 18
7.4. Layer 4 – Policy & Traceability 18

8. Policy, Regulation & Industry Recommendations 20
8.1. Scrap Metal Market Regulation 20
8.2. Support for Public-Space Security Enhancements 20
8.3. Harmonized Incident Reporting Requirements 21
8.4. Encouragement of Technical Standards Development 21
8.5. Legal Deterrence 21
9. Implementation Roadmap 23
9.1. Short-Term (0–6 Months) – Low-Effort Foundation 23
9.2. Mid-Term (6–18 Months) – Targeted Technical Enhancements 23
9.3. Long-Term (18–36 Months) – Ecosystem Integration 23
10. Conclusion & Next Steps 25
11. Reference 26

1. Executive Summary

Cable theft at EV charging stations has emerged as a growing operational and infrastructure security challenge across multiple markets. Incidents primarily target charging cables and associated components, driven by material value in secondary scrap markets as well as opportunistic vandalism. The consequences extend beyond direct equipment loss, affecting station availability, operational costs, safety risk management, and user confidence in public charging infrastructure.

The problem is reinforced by a combination of factors, including exposed hardware design in legacy systems, limited real-time intrusion detection, and site conditions such as low visibility or isolated deployment locations. In many cases, damage is only detected after service interruption, resulting in extended downtime and increased maintenance complexity.

Addressing cable theft requires a coordinated, multi-layer approach involving industry stakeholders, public authorities, and standards organizations. While hardware design improvements, physical security measures, and digital monitoring can help mitigate risks, effective and scalable solutions also depend on supportive policy and regulatory frameworks, as well as consistent enforcement.

CharIN's primary contribution is to represent the industry, raise awareness of the impact of cable theft on EV charging infrastructure, and engage with policymakers and public authorities to support the development of appropriate policy and regulatory frameworks. In parallel, CharIN will consolidate industry experience and facilitate the exchange of best practices to strengthen the resilience of interoperable EV charging infrastructure.

2. Scope & Purpose

The Charging Interface Initiative e. V. (CharIN) is the largest global association focusing on the electrification of all forms of transportation based on a seamless and interoperable charging infrastructure. The Combined Charging System (CCS), the Megawatt Charging System (MCS), and the North American Charging System (NACS) are the common ground on which the CharIN community has built its achievements over the past 10 years. CharIN has been establishing platforms around the globe to ensure a smooth cooperation of actors along value chains. By incorporating actors from the energy sector, the CharIN community thinks ahead and builds an innovative ecosystem capable of electrifying all modes of transport in the years to come.

Today CharIN represents more than 300 leading e-mobility stakeholders, from automakers to utilities, grid operators, component suppliers, and electric vehicle supply equipment (EVSE) manufacturers.

The expansion of electric vehicle (EV) charging infrastructure is a cornerstone of the global transition to sustainable mobility. Yet, alongside this progress, new vulnerabilities are emerging that threaten reliability, user confidence, and the economics of operating charging networks. One of the most pressing and visible challenges is cable theft.

The issue of EV charging cable theft first came into focus through feedback in the Focus Group Connection and the Focus Group Charging Infrastructure, where charge point operators (CPOs), cable manufacturers, and EVSE manufacturers voiced growing concerns about the increasing frequency of theft incidents.

Cable theft at charging stations is a multi-faceted challenge. It is not limited to the direct replacement costs of stolen equipment but also impacts network reliability, customer trust, and the overall perception of EV charging infrastructure. As EV charging networks continue to grow in importance and become an increasingly essential part of the future mobility and energy ecosystem, their resilience and reliability are gaining relevance as a critical infrastructure topic. Addressing the problem therefore requires coordinated efforts across the entire EV charging ecosystem, from hardware manufacturers and operators to policymakers and standardization bodies.

To advance this discussion, CharIN engaged its global Managing Directors to build a common understanding of the scope and severity of the issue. As part of this effort, a short survey was distributed to CharIN members in North America, which confirmed that the issue is both widespread and often severe. These findings provided the initial foundation for developing this position paper.

Currently, there is limited industry-wide guidance for technical or operational anti-theft solutions. While a variety of ideas and pilot approaches exist, they remain fragmented. With this position paper, CharIN aims to consolidate existing knowledge, highlight best practices, and establish a collaborative framework that will enable the industry to develop effective and scalable countermeasures against criminal activities.

3. Problem statement – What is happening?

Cable theft at EV charging stations has become an increasingly common and disruptive problem in many regions. Offenders frequently target charging cables for the resale value of copper, aluminum, or connectors, or as part of broader vandalism patterns affecting public infrastructure.

Common theft methods include:

- Cutting cables directly at the charging station or at a user-accessible point.
- Unbolting or forcefully removing tethered cables from enclosures.
- Targeting weak points such as cable glands, holsters, or installation junction areas.
- Theft during low-visibility hours, especially at poorly lit or isolated sites.
- The theft of upstream electrical components such as switchgear can result in substantially higher replacement and downtime costs.

The problem persists due to low barriers to committing the crime, relatively low risk of being caught, and a thriving secondary market for stolen materials. As a result, EVSE operators face recurring incidents that affect reliability and increase operational complexity.

This chapter establishes the baseline understanding needed for the analysis and recommendations that follow.

3.1. Vandalism & Tampering

Some attacks are acts of vandalism rather than outright theft. Offenders may deliberately damage station components – breaking screens or housings, chewing on connectors, or cutting wires – without taking the pieces. Such tampering can be possibly ideologically motivated (e.g. protest against electric cars) or simply causing destruction. Even if no valuable material is removed, the result is the same: the charging station is disabled until it is repaired. Multiple reports describe cases where entire stations were disabled by such attacks. For instance, in several incidents' operators found large segments of cables severed and left behind, suggesting possible vandalism rather than to extract copper [1]. Any exposed wiring or torn enclosure is a safety hazard, so these acts force immediate shutdowns and repairs. Although specific statistics on just vandalism are scarce, experts warn that these events often coincide with cable thefts and contribute to the overall trend of charging stations failing unexpectedly.

3.2. Theft of components – mainly copper

The more common scenario is direct theft: criminals targeting the cables (and sometimes connectors) themselves. These thefts are usually driven by the small but exploitable scrap value of copper and other metals in the cables. In practice, thieves employ simple methods: cutting the thick charging cable at a junction or splicing point, prying loose the tethered plug, or removing cables from their holsters. They often exploit known weak spots, such as cable glands or unsecured mountings, to pull out wires and connectors quickly [2] [3]. Most thefts occur at night or in poorly lit, low-traffic locations, where perpetrators assume a lower risk of being seen or caught.

Multiple industry sources note that thieves leave in a hurry. In many cases, large portions of the cable are abandoned on site after being cut, indicating that the culprit's primary aim might not even be scrap value [1]. In fact, each cable typically contains only about $15–$20 worth of copper [3] [4], which requires effort to harvest and sell. Analysts suspect that some attacks are driven more by mischief or hostility toward electric mobility, as evidenced by the incomplete thefts. However, the economic motive should not be underestimated: copper prices reached $5.20 per pound in May 2024, reflecting elevated market conditions [3], and even a small payout can finance other illicit activities.

Taken together, these methods make cable theft a low-barrier crime. Offenders need only basic tools (wire cutters, wrenches) and often face little chance of immediate detection. Meanwhile, once cut, a charging station can be instantly out of service. In sum, the problem is multifaceted: opportunistic thieves exploiting easy targets, sometimes embedded within broader vandalism patterns, all leading to frequent and disruptive cable losses.

4. Impact assessment

Cable theft has a multi-dimensional impact on EVSE operation and market confidence. The consequences extend beyond the immediate physical damage and can influence user trust, operator economics, and infrastructure planning.

Key categories of impact include:

4.1. Operational Impact

The financial toll is steep. Operators must dispatch technicians, procure replacement cables (which are expensive and often custom-made), and perform on-site repairs. In one example, a German charging operator estimated that each cable theft incident cost up to €8,000 in repairs [1]. In another case, Minneapolis paid roughly $1,000 for a single cable replacement [4]. A private network in the UK (InstaVolt) suffered 33 theft/damage events across 13 sites in a few months; the 100 cables involved represented about £410,000 in losses (over £4,000 per cable) [5]. Cost figures vary significantly by region, currency, and exchange rate conditions; values are reported in local currency as cited in the underlying sources. These repeated losses quickly add up and strain maintenance budgets. Entire stations are sometimes left offline, which operators describe as “pretty impactful” for customers and communities [3].

4.2. Safety and Liability Impact

Beyond the business impact, cable theft and tampering can also introduce safety and operational concerns. Modern charging systems incorporate multiple safety mechanisms designed to reduce risks in the event of damage; however, physical damage to charging equipment, exposed components, or unsecured cables may still create potential hazards for users, service personnel, or the surrounding environment. In addition, vandalized equipment can result in accessibility issues, trip hazards, and increased liability concerns for site owners and operators. Ensuring that theft incidents are detected, reported, and repaired quickly is therefore important to maintain safe and reliable charging infrastructure.

4.3. Organizational and Administrative Impact

The organizational impact of cable theft includes an increased workload for technical teams and service operators, who must manage unplanned repairs and site interventions. Spare-parts logistics and inventory management also become more complex, as operators need to maintain additional stock and coordinate accelerated replacement cycles. In addition, regulatory and compliance-related activities may be required after repairs. For example, in Germany, the replacement of charging cables may require an Eichrecht-compliant verification or re-certification process to ensure that the charging equipment remains compliant after the intervention. Further administrative tasks can include incident documentation, insurance claims, and coordination with law-enforcement or municipal authorities to ensure proper reporting and follow-up.

4.4. Insurance and Compliance Impact

The rising incidence of cable theft will inevitably influence insurance and regulatory landscapes. Insurers covering EV charging installations will take note of these losses. Networks with frequent claims may see higher premiums or be required to meet stricter security criteria (such as mandatory alarms or fencing) to maintain coverage. On the compliance side, operators must adhere to local regulations for public infrastructure safety and data. For instance, jurisdictions may mandate CCTV cameras or specific lighting standards at public charging sites. Increasingly, demonstrating that a station has adequate anti-theft measures could be a condition for meeting safety codes or for receiving public funding. In the long term, increased costs related to vandalism prevention, insurance, repairs, and compliance measures may affect the overall cost of operating charging networks and could potentially be reflected in higher charging costs for end users.

This underlines the importance of effective and proportionate measures to improve the resilience of EV charging infrastructure.

5. Root causes

The rise in charging cable theft is not the result of a single failure but rather a "perfect storm" of economic incentives, physical design vulnerabilities, and systemic regulatory gaps. As global electric vehicle infrastructure expands, these stations have become increasingly attractive targets for both opportunistic individuals and organized criminal networks.

5.1. Economic Drivers and the Metal Market

The most significant catalyst for theft remains the high resale value of the raw materials used in EV infrastructure, particularly copper. By early 2025, copper prices reached record highs, surging past $5.60 per pound [6] due to massive demand from data centers, renewable energy projects, and the broader global energy transition. For an offender, even a small amount of harvested copper provides a quick, lucrative payout in the black market.

This financial motive is facilitated by a thriving and often under-regulated scrap metal trade. In many regions, informal secondary markets allow thieves to dispose of stolen materials quickly, often with minimal identification checks. Furthermore, the "entry barrier" for these crimes is remarkably low; unlike sophisticated cyber-attacks, physical cable theft requires only basic, widely available tools such as wire cutters or heavy-duty wrenches.

5.2. Technical and Operational Vulnerabilities

Current hardware often prioritizes user convenience and ease of installation over physical security. Many AC and DC charging units feature exposed cable glands and unshielded junction areas that can be easily exploited to pull out or unscrew entire wiring harnesses.

A critical technical deficiency is the "silent failure" problem. This lack of immediate detection creates a “dwell time window” during which attackers can completely remove or significantly tamper the charger without triggering operational response mechanisms, thereby increasing both successful theft probability and total asset loss. Many legacy EVSE models lack integrated sensors to detect tension, vibration, or continuity breaks. Consequently, these units do not trigger immediate alerts when a cable is severed, especially if the station is in an idle state or powered down. This lack of real-time monitoring creates a "window of opportunity" for criminals to operate undetected. Additionally, the industry faces long repair cycles, which can take anywhere from 1 to 7 days, leaving a site looking neglected and inviting repeat incidents.

5.3. Environmental and Site Factors

The physical environment of a charging station heavily influences its risk profile. Thefts predominantly occur during low-visibility night hours at sites characterized by poor lighting or isolated locations, such as peripheral commercial parking lots. Criminals specifically target these "soft targets" where pedestrian traffic is low and there is an absence of visible deterrents like security signage or active CCTV. In many cases, if cameras are present but easily avoided, they fail to act as a meaningful deterrent. Beyond economic gain,

there are also cases of deliberate vandalism where charging infrastructure is damaged without theft of components. In 2024 and 2025, operators in Germany reported incidents where cables were cut and partially left on site, with no removal of material.

5.4. Regulatory and Market Gaps

A significant obstacle to preventing theft is the lack of a harmonized legal and regulatory framework.

- **Resale Oversight:** There is often weak enforcement around metal resale, with many jurisdictions lacking mandatory ID verification or transaction documentation for copper sales. Strengthening traceability requirements for stolen materials could reduce incentives for organized theft.
- **Legal Deterrence:** Infrastructure theft is frequently treated as a minor offense, resulting in limited legal deterrence for repeat offenders. In addition, the prioritization and follow-up of such cases can vary significantly between regions, particularly when charging infrastructure theft is not recognized as a broader infrastructure reliability issue. This can reduce the effectiveness of prevention efforts and leave operators with limited possibilities for recovery or prosecution.
- **Information Silos:** Currently, there are no harmonized reporting requirements or impact assessments across different jurisdictions. The absence of structured reporting channels and shared data between operators, authorities, and law enforcement makes it difficult to quantify the scale of the problem, identify recurring patterns, and allocate appropriate resources for prevention and investigation.

6. Stakeholder & Responsibilities

Mitigating the impact of cable theft requires a coordinated "defense-in-depth" strategy. No single stakeholder can solve the problem alone; rather, every actor in the e-mobility ecosystem must fulfill specific security roles.

6.1. Manufacturers and Installers: Security by Design

Manufacturers and installation providers constitute the primary line of defense in a comprehensive, defense-in-depth approach against charging cable theft and infrastructure tampering. Their role is to ensure that security considerations are systematically integrated into the design, manufacturing, and deployment of charging infrastructure, thereby reducing vulnerability at the source and enabling effective detection and response mechanisms.

6.1.1. Physical Robustness and Hardware Hardening

Charging equipment should consider measures to reduce vulnerability to opportunistic and organized theft attempts while maintaining usability, cost efficiency, and ease of operation. Key considerations include:

- Integration of **appropriate tamper-resistant cable anchoring** and **dispenser interfaces**, particularly in high-risk locations or applications.
- Use of **targeted protective measures**, such as reinforced cable protection systems, in areas with demonstrated theft risks rather than applying additional mechanical complexity universally.
- **Protection of critical transition points** such as connector heads and cable exit zones through suitable design measures.
- Application of **vandal-resistant enclosures** and minimized exposed interfaces where appropriate.

While physical robustness measures can contribute to theft prevention, excessive hardening may increase manufacturing and operational costs and negatively impact usability. Therefore, security-by-design approaches should follow a risk-based strategy, combining targeted physical protection with effective monitoring, rapid detection, and timely response mechanisms.

The objective is not only to make theft attempts more difficult, but also to minimize downtime and operational impact by enabling early detection and efficient recovery actions.

6.1.2. Active Deterrence & Response

In addition to passive mechanical protection, charging infrastructure should incorporate active deterrence and traceability functions that are triggered upon tampering or intrusion attempts. These may include:

- **Forensic marking technologies**, releasing traceable UV-visible or chemically identifiable markers upon mechanical intrusion, enabling post-incident investigation and deterrence of repeat offenses.

- **Local deterrence signals**, such as acoustic alarms and visual indicators (e.g., high-intensity lighting or flashing signals), activated during tampering events.
- Optional integration with remote monitoring systems to support real-time incident escalation.

The effectiveness of these measures depends on a coordinated response process involving charging operators, service providers, and relevant authorities. Timely reporting, prioritization, and follow-up by law enforcement are essential to ensure that detected incidents lead to appropriate action and contribute to long-term deterrence.

Such mechanisms contribute not only to immediate deterrence and evidentiary traceability but also to improved incident management, provided that the supporting operational and regulatory frameworks are in place.

6.1.3. Detection & Sensing Layer

Early detection of cable tampering is essential to enable timely response and minimize damage. Manufacturers should evaluate the integration of multi-modal sensing capabilities, which may include:

- **Acoustic detection systems** capable of identifying characteristic signatures of cutting or forced manipulation.
- **Strain and tension monitoring** to detect abnormal mechanical stress on cables and connectors.
- **Vibration and impact sensors** to identify physical interference or vandalism attempts.
- **Temperature anomaly detection**, supporting identification of thermally induced cutting or tool-based interference. Any sensor continuity breaks resulting from tampering should be identified via temperature anomaly detection as well.
- **Visual monitoring systems**, such as camera-based solutions or live video feeds, to support incident verification, situational awareness, and evidence collection, where permitted by applicable data protection regulations.

Sensor outputs should be integrated into a unified monitoring architecture capable of triggering local alarms and remote notifications, and, where appropriate, initiating protective system responses.

Combining different detection methods can improve reliability by reducing false alarms and enabling a more accurate assessment of incidents.

6.1.4. Controlled Access and Cable Management Concepts

Reducing physical exposure of charging cables can further mitigate theft risk. Manufacturers and installers should consider:

- **Retractable or managed cable systems**, limiting the amount of permanently exposed cable infrastructure.

- **Access-controlled activation mechanisms,** where appropriate, to limit unauthorized access to charging equipment and reduce the risk of misuse or tampering.
- **Connector locking concepts**, preventing unauthorized disconnection or removal during or after charging sessions.

These approaches shift charging infrastructure from a continuously exposed asset to a controlled-access system governed by authenticated user interaction. At the same time, it is essential that these security measures remain transparent to the end user, preserving ease of use and ensuring that secure charging functionalities, such as Plug & Charge, continue to operate in a simple, fast, and user-friendly manner consistent with mass-market EV adoption requirements. Security measures must not introduce friction into the user experience or compromise seamless charging workflows.

6.1.5. Integration with Digital Security Architectures

Physical security measures should be complemented by integration into secure digital charging ecosystems. In particular:

- Alignment with secure communication and authentication frameworks to ensure consistency between charging infrastructure access, system security, and digital identity management
- Logging and traceability of tampering or intrusion events within backend systems to support analytics and forensic investigation.
- Consideration of interoperability impacts in mixed-deployment environments where legacy and advanced security systems coexist.

6.2. Charge Point Operators (CPOs)

CPOs bear the primary operational and financial burden of theft. Their responsibility lies in proactive site management and data-driven security. This includes conducting rigorous site-specific risk assessments to prioritize well-lit, high-traffic locations for new installations. Once a station is live, CPOs must configure their backend management systems (OCPP) to process and escalate "cable integrity" alerts instantly to minimize response latency.

6.3. Public Authorities, Police, and Regulators

The public sector provides the legal framework necessary to increase the risk for offenders. Police forces are tasked with facilitating rapid responses to alarms and coordinating with CPOs to capture evidence like CCTV footage.

Regulators play a vital role by enforcing stricter Scrap Metal Acts. For example, Japan has tightened scrap metal regulations requiring identity verification and transaction records for copper and other specified metals [7], while South Australia introduced the Scrap Metal Dealers Bill in 2025, which proposes mandatory

ID checks and bans on cash payments for scrap metal [8]. Municipalities can further support infrastructure resilience by funding improved public lighting at high-risk charging hubs.

6.4. Strategic Partners: Insurers and Standards Bodies

Insurers can incentivize industry-wide security by linking premiums to risk-mitigation measures. By offering lower rates to operators who implement active alarms or forensic marking, they drive the adoption of best practices.

Finally, industry alliances like CharIN serve as the central hub for harmonization. They are responsible for developing uniform technical standards so that security telemetry is consistent across different manufacturers. By facilitating anonymized data sharing, these bodies help the entire industry identify and prepare for evolving criminal tactics.

7. Multi-Layer Anti-Theft Strategy

The multi-layer anti-theft strategy is structured into four implementation levels to reflect different resource, infrastructure, and operational capabilities. Each layer builds on the previous one to form a comprehensive defense-in-depth model.

This four-tier structure enables operators to start with basic, quick wins and progressively expand to a robust multi-layer defense as budgets, infrastructure maturity, and risk levels evolve.

Figure 1 Multilayered security measures for EV charging infrastructure

7.1. Layer 1 – Hardened Hardware

Tamper-Resistant Design

Components are designed so that opening, cutting, or manipulating them requires specialized tools and leaves visible traces, discouraging opportunistic theft or sabotage.

Reinforced Components

Critical parts such as cables, housings, and connectors use strengthened materials or internal reinforcement to withstand cutting, bending, or mechanical stress.

Locking Interfaces

Connectors and cables include mechanical or electronic locking mechanisms that prevent unauthorized removal during and outside of charging sessions.

Anti-Theft Materials

Use of materials with lower resale value or higher detection probability (e.g. traceable metals) to reduce incentives for material theft.

Physical Robustness

Hardware is engineered to withstand long-term exposure to weather, repeated use, misuse, and low-level vandalism without functional degradation.

7.2. Layer 2 – On-Site Physical Security

Controlled Access

Physical measures (location design, access barriers, zoning) limit who can approach or interact with charging infrastructure, especially outside operating hours.

Perimeter Protection

Structural elements such as curbs, bollards, fencing, or layout design protect charging equipment from vehicles, accidental damage, or intentional ramming.

Surveillance & Lighting

Adequate illumination and camera coverage increase visibility, enable incident investigation, and act as a deterrent against vandalism and theft.

Impact Protection

Dedicated structures absorb or deflect mechanical impacts caused by vehicles, maintenance equipment, or environmental factors.

Deterrence Measures

Visible security elements (lighting, cameras, reinforced structures) reduce the likelihood of attacks by increasing perceived risk for offenders.

7.3. Layer 3 – Network & Software

Secure Communications

Encrypted and authenticated communication channels protect data exchange between vehicles, charging stations, and back-end systems from interception or manipulation.

Continuous Monitoring

Real-time observation of system behavior enables early detection of irregularities, failures, or security incidents.

Intrusion Detection

Software mechanisms identify abnormal patterns or unauthorized access attempts that may indicate cyberattacks or system compromise.

Authentication & Authorization

Only verified users, devices, and systems are permitted to access services or configuration functions, preventing misuse or fraud.

Remote Enforcement

Back-end systems can remotely restrict, disable, or isolate compromised assets to limit damage and maintain system integrity.

7.4. Layer 4 – Policy & Traceability

Compliance & Standards

Alignment with technical, cybersecurity, and safety standards ensures consistent security baselines and regulatory conformity.

Asset Traceability

Components and materials can be tracked across the value chain using digital identification mechanisms, such as RFID or Bluetooth Low Energy (BLE) tags, where applicable. These identifiers enable persistent asset-level traceability from manufacturing through installation and operation, supporting theft prevention, incident investigation, inventory control, and lifecycle management.

Accountability

Clear assignment of responsibilities among operators, manufacturers, and service providers enables effective governance and incident response.

Risk Transfer

Insurance mechanisms help manage residual risks that cannot be fully eliminated through technical or physical protections.

Incentive Alignment

Policy and market instruments reward secure design and operation, encouraging proactive investment in infrastructure protection.

8. Policy, Regulation & Industry Recommendations

Policy and regulatory instruments play a critical role in reducing both the attractiveness and feasibility of EV charging cable theft. Effective mitigation requires coordinated action across legislative authorities, municipalities, industry stakeholders, and standards organizations. This section outlines structured recommendations grouped by intervention domain.

8.1. Scrap Metal Market Regulation

Unregulated or weakly regulated secondary metal markets remain a primary enabler of copper-driven infrastructure theft. Strengthening oversight mechanisms reduces the economic incentive for cable theft.

Recommended measures include:

- Mandatory licensing and registration of scrap metal dealers within centralized national or regional registries
- Obligatory identity verification for all sellers, with retention of transaction records including material type, weight, and origin declaration
- Restrictions or prohibitions on cash payments for copper and other high-value non-ferrous metals to improve transaction traceability
- Defined reporting thresholds requiring dealers to notify authorities of unusually large, frequent, or otherwise suspicious transactions
- Enforcement mechanisms including penalties for non-compliant trade practices and unregistered operations

8.2. Support for Public-Space Security Enhancements

Charging infrastructure located in public or semi-public environments is strongly influenced by surrounding site design, lighting conditions, and surveillance availability. Municipal frameworks and permitting processes therefore play a critical role in reducing exposure to theft and vandalism.

Recommended measures include:

- Integration of minimum security requirements (e.g. lighting levels, visibility standards, camera coverage) into public EV charging procurement frameworks
- Inclusion of security-by-design criteria in permitting and approval processes for new charging installations
- Targeted co-funding or incentive programs to retrofit high-risk or legacy charging sites with lighting, surveillance, and physical protection measures
- Adoption of standardized site-risk classification approaches to prioritize investment in high-exposure or low-visibility locations

8.3. Harmonized Incident Reporting Requirements

A major barrier to effective mitigation is the absence of standardized, cross-operator incident data. Improved comparability of incident reporting enables trend detection, risk mapping, and evidence-based policy development.

Recommended measures include:

- Definition of standardized incident categories (e.g. attempted theft, partial cable theft, full asset removal, vandalism with service interruption)
- Voluntary or mandatory reporting frameworks for charge point operators, depending on national regulatory context
- Establishment of centralized or federated incident databases at national or regional level, with anonymized data aggregation
- Standardized reporting fields, including location type, asset type, downtime duration, attack method, and estimated loss
- Publication of aggregated statistics to support industry-wide risk assessment and mitigation planning

8.4. Encouragement of Technical Standards Development

Standardization is essential to ensure consistent implementation of anti-theft and tamper-detection measures across heterogeneous charging infrastructure deployments.

Recommended measures include:

- Development of standardized requirements for tamper detection, cable integrity monitoring, and intrusion signaling within relevant IEC/ISO standardization frameworks
- Extension of existing communication protocols (e.g. OCPP and related interfaces) to support structured reporting of security-relevant events and telemetry
- Consideration of certification frameworks for security-relevant EVSE components, including cables, connectors, and dispenser systems, as a future development area
- Definition of interoperability requirements for security telemetry to ensure compatibility across manufacturers and backend systems
- Promotion of standardized test and validation procedures for physical and digital anti-theft features under controlled conditions

8.5. Legal Deterrence

Effective deterrence requires both appropriate legal classification of offenses and robust evidentiary frameworks capable of supporting prosecution.

Recommended measures include:

- Classification of EV charging infrastructure theft and vandalism as aggravated offenses or critical infrastructure-related crimes where applicable under national legislation
- Strengthening of penalties proportional to the economic and systemic impact of infrastructure downtime and service disruption
- Improvement of law enforcement effectiveness through faster processing and admissibility of EVSE-generated evidence, including CCTV data, backend telemetry, fault logs, and component serialization
- Alignment with relevant European and national frameworks on critical infrastructure protection, resilience, and repairability, particularly regarding rapid restoration of damaged charging assets where applicable
- In alignment with CharIN guidance on Legal Metrology [9], ensure harmonized interpretation and implementation across jurisdictions to avoid fragmented compliance requirements for EVSE manufacturers and operators.

9. Implementation Roadmap

The measures presented in this roadmap are intended as guidance to support CPOs and other stakeholders in improving the resilience of charging infrastructure against cable theft. As security requirements, risk exposure, operational environments, and available resources differ across deployments, the recommendations should be applied selectively and adapted to individual use cases. The suggested timeframes provide a practical orientation rather than a fixed implementation sequence.

9.1. Short-Term (0–6 Months) – Low-Effort Foundation

The focus is on immediate deterrence and leveraging existing system capabilities with minimal capital expenditure.

- Deterrence & Lighting: Deploy clear signage indicating active CCTV and tamper detection. Enhance site visibility through improved or motion-activated lighting.
- Asset Management: Register all cables and connectors using serial numbers or QR codes for tracking. Implement basic visual inspections during routine maintenance.
- System Activation: Enable existing telemetry alerts in EVSE backend systems, such as offline status or connector faults.
- Audit: Conduct high-risk site audits using a standardized security assessment checklist.

9.2. Mid-Term (6–18 Months) – Targeted Technical Enhancements

Moving toward active monitoring and physical hardening of the infrastructure.

- Surveillance & Physical Barriers: Install fixed CCTV viewpoints covering all EVSE units and integrate them with monitoring tools. Deploy physical barriers like bollards or protected housings.
- Advanced Hardware: Transition to reinforced or cut-resistant cable jackets for new installations. Pilot forensic marking (UV tracers or dye-spray) to link offenders to crime scenes.
- Sensing & Response: Install tamper-detection sensors (vibration, tension, continuity). Integrate these alerts into a central OCPP monitoring dashboard.
- Operations: Coordinate with security personnel or site patrols at strategic, high-risk locations.

9.3. Long-Term (18–36 Months) – Ecosystem Integration

Achieving high-level security through advanced automation and industry-wide collaboration.

- Advanced Hardware & Automation: Deploy fully armored or retractable cable systems with locking mechanisms. Embed GPS/RFID tracking beacons into cable assemblies.
- Intelligent Monitoring: Implement AI-based video analytics to detect suspicious behavior (loitering, cutting postures). Utilize remote lockdown capabilities upon tamper detection.
- Public & Industry Collaboration: Integrate on-site systems with municipal security networks and shared public lighting. Participate in industry-wide incident databases to identify regional patterns.
- Standardization: Establish formalized standards and certification schemes across entire networks.

10. Conclusion & Next Steps

EV charging cable theft is a multi-faceted issue and addressing it requires collaboration across the entire EV charging ecosystem.

- Tailored solutions are required for different stages of the charging station lifecycle
- Scale of impact varies significantly: some operators experience isolated incidents, while others face hundreds of thefts annually, particularly in urban environments
- Charging stations are most vulnerable during installation and commissioning phases, before monitoring and security systems are fully operational
- Primary motivations are linked to copper resale, although connector resale and vandalism also occur
- Operational impact is significant, with cable replacement often requiring 1–7 days, specialized repair crews, and resulting in extended downtime
- Detection limitations remain, as many systems do not immediately alert operators when cables are cut, particularly when stations are de-energized

CharIN will continue to collect best practices, promote industry-wide data sharing, and support the development of global recommendations for mitigating cable theft in EV charging infrastructure.

11. Reference

This document was created by the experts of the Focus Group Charging Infrastructure and Focus Group Connection of the CharIN association.

Special thanks for the contribution go for:

- Daniel Porubcsanszki (Allego)
- Stefan Scheubner (EnBW)
- Dominik Ziriakus , IONITY
- Robert Schädel , Amphenol
- Alexander Schramm , Amphenol
- Holger Haussmann , HUBER+SUHNER
- Harald Braun , Mercedes-Benz
- Kor Meelker , ChargePoint
- Kevin Wahl , Southwire
- Markus Kroner , Phoenix Contact
- Nuno Costa , EFACEC
- Sergej Pahl , Prysmian
- Sybille Korrodi , HUBER+SUHNER
- Keisuke Kanazawa , Mazda
- Ziyu Chen , Sungrow EMEA
- Volker Hummeltenberg , HUBER+SUHNER
- Ville Naumanen , Kempower
- Mariano Rigotti , Amphenol AIPG
- Andrzej Chmura , Shell
- Annette Reeb , IONITY
- Mark Swinburn , NXP
- Semih Tetik , CharIN e.V.
- Alexander Janissek , CharIN e.V.
- Min-Jung Lee, Korea Office , CharIN e.V.
-

Sources:

[1] B. Wehrmann, "Clean Energy Wire," 14 Oktober 2025. [Online]. Available: https://www.cleanenergywire.org/news/spike-vandalised-ev-charging-stations-raises-suspicions-ideological-offenders-germany.

[2] M. Vughn, "Autoweek," 16 Januar 2025. [Online]. Available: https://www.autoweek.com/news/a63437589/chargepoint-makes-cut-proof-cable-for-ev-chargers/.

[3] W. Malone, "Inside EVs," 22 June 2024. [Online]. Available: https://insideevs.com/news/723769/charger-vandalism-grows-electrify-america/.

[4] S. Edelstein, "Green Car Reports," 20 June 2024. [Online]. Available: https://www.greencarreports.com/news/1143565_public-ev-charging-cables-magnet-for-thieves.

[5] K. M. Ross, "EV Infrastructure News," 5 June 2025. [Online]. Available: https://www.evinfrastructurenews.com/ev-technology/chargepoint-operators-make-security-a-priority-as-cable-theft-on-the-rise.

[6] J. Showen, "ECAM," 14 01 2026. [Online]. Available: https://ecam.com/en-ca/security-blog-ca/high-copper-prices. [Accessed 26 01 2026].

[7] "The Act on the Prevention of the Disposal of Stolen Specified Metals (Outline)," [Online]. Available: https://www.npa.go.jp/bureau/safetylife/scrap/00_gaiyoupontie_english.pdf.

[8] "Crackdown on scrap metal theft," [Online]. Available: https://premier.sa.gov.au/media-releases/news-archive/crackdown-on-scrap-metal-theft.

[9] "Industry call: reducing complexity in EV Charging Regulation," 13 05 2026. [Online]. Available: https://www.charin.global/news/ev-charging-regulation/.