



FIRST EDITION

IAF ECIAS

Electric Vehicle Charging Infrastructure Assurance Standard

Equipment, sites and digital services
Life cycle assurance for charging infrastructure

DRAFT FOR TECHNICAL REVIEW

Technical validation and formal adoption are required before operational conformity claims. Release conditions are set out in Annex L.

International Automotive Federation

English master text

iaf.com

Publication identity

IAF ECIAS First Edition

Electric Vehicle Charging Infrastructure Assurance Standard

International Automotive Federation

English master text

www.iaf.com

Scope of this publication

This publication establishes proposed requirements for EV charging equipment, installed sites, digital platforms and operational services. It covers electrical safety, interoperability, cybersecurity, reliable charging, accessible use, grid integration and environmental performance throughout the life cycle.

Status and operational use

Technical working text, revision 0.2, dated 13 September 2026. This is a development proposal for technical review and pilot validation. Technical validation and formal adoption are required before an adopted-standard conformity claim. The release conditions in Annex L apply.

Review and configuration identity

This revision retains the full requirement structure and clarifies availability arithmetic, unsuccessful initiation and status-update latency, payment-related failures and timing uncertainty. Product and platform results remain configuration-specific; operational results remain tied to their measurement period.

Reading and navigation

The contents and PDF bookmarks link to the 32 main clauses and 12 annexes. Clause identifiers remain the reference points for assessment work. Annexes A to H, J and K are normative within the draft; Annexes I and L are informative. Every annex begins on a new page.

Contents

Select a section to navigate to it.

1 Scope and intended outcomes	5
2 Document status and application rules	6
3 Terms and abbreviations	7
4 Assessment scope and modular structure	8
5 Governance and competence	8
6 Integrated risk engineering	9
7 Deployment obligations and approval records	10
8 Design and manufacturing assurance	11
9 Electrical safety and protective functions	12
10 Thermal mechanical and fire safety	13
11 Environmental durability and electromagnetic performance	14
12 Power delivery and grid integration	14
13 Physical interfaces and vehicle compatibility	15
14 Communications and service interoperability	16
15 Charging session integrity	17
16 Cybersecurity and trust architecture	18
17 Software updates and configuration integrity	19
18 Privacy data governance and evidence protection	20
19 Metering payment and consumer protection	21
20 Accessibility and user experience	21
21 Site planning and infrastructure integration	22
22 Installation commissioning and handover	23
23 Operation maintenance and reliability	24
24 Continuity incident response and recovery	25
25 Sustainability energy and circularity	26
26 Supply chain integrity and ethical procurement	27
27 Bidirectional charging and energy exchange	27
28 High power and heavy vehicle charging	28
29 Wireless automated and dynamic charging	29
30 Mobile storage assisted and constrained grid charging	30

Contents continued

Select a section to navigate to it.

31 Artificial intelligence and emerging technology governance	31
32 Verification conformity decisions and public claims	32
Annex A Application and responsibility matrix	34
Annex B Engineering limits and deployment parameter schedule	36
Annex C Minimum hazard and failure scenario register	38
Annex D Verification catalogue and test records	40
Annex E Interoperability coverage and acceptance	45
Annex F Operational metrics and proposed pilot thresholds	47
Annex G Digital evidence passport	50
Annex H Cybersecurity treatment and incident schedule	52
Annex I Environmental calculation example	53
Annex J Assessment decision and corrective action forms	54
Annex K Commissioning and operational inspection checklist	55
Annex L First edition development and technology roadmap	57

1 Scope and intended outcomes

1.1 Purpose

This standard establishes proposed requirements for the safety, integrity, interoperability, availability, accessibility and environmental performance of electric vehicle charging infrastructure across its life cycle. The responsible organization shall demonstrate that a declared charging service works safely as an integrated system and that each public claim is supported by current, traceable evidence.

1.2 System boundary

The assessed boundary shall identify the electricity connection, protection and distribution equipment, charging equipment, vehicle interface, local energy systems, communications, remote management, identity services, payment interfaces, user facilities and supporting operations. Dependencies outside organizational control shall remain in the risk and service records. Outsourcing shall not remove accountability for an interface or outcome.

1.3 Applications

The standard applies to residential, workplace, destination, public, highway, fleet, depot and industrial road vehicle charging. It covers alternating current and direct current transfer, fixed and mobile equipment, conductive and wireless transfer, automated connection, bidirectional operation and shared energy resources when included in the declared configuration. Annex A determines the modules that become mandatory for each application.

1.4 Technology boundary

The standard does not prescribe a universal connector geometry or a single communications protocol. The organization shall declare exact implemented interfaces and demonstrate their compatibility. Vehicle traction battery design, complete vehicle approval, utility network approval and non-road vehicle charging are outside the base assessment; their relevant interface risks shall nevertheless be controlled. Battery exchange requires an additional dedicated specification and shall not be represented as assessed by this document alone.

1.5 Life cycle

Requirements apply from concept and procurement through design, manufacture, installation, commissioning, operation, repair, modification, transfer of ownership and decommissioning. A claim for one life cycle stage shall not imply successful assessment of later stages. Product, site, digital platform and operational service evidence shall be identified separately and linked through the configuration record.

1.6 Intended outcomes

The organization shall define measurable outcomes for safe energy transfer, successful charging initiation, truthful power information, accurate billing, secure control, inclusive access, efficient resource use and recoverable service. Targets shall be supported by Annex F and the declared application. Broad statements such as universal compatibility, zero risk, unlimited power or carbon neutral charging shall not be used without a defined boundary and supporting evidence.

2 Document status and application rules

2.1 Working draft status

This document is a proposed first edition working draft for technical development and pilot evaluation. It is not an adopted publication, an issued certificate, a market authorization or proof of regulatory approval. The word shall identifies a proposed normative requirement within this draft. Operational use shall require the applicable engineering approvals independently of the draft development process.

2.2 Requirement language

Shall indicates a requirement, should indicates a recommendation, may indicates permission and can describes capability. Notes and examples are informative unless explicitly designated as requirements. Clauses 1 to 32 and Annexes A to H, J and K contain proposed normative provisions. Annexes I and L are informative. No external normative references are incorporated into this text.

2.3 Local obligations

The organization shall satisfy applicable legal, electrical installation, grid connection, construction, accessibility, metrology, consumer protection, environmental and data requirements for each place of operation. These obligations shall be recorded in its controlled deployment dossier. Conformity with this document shall not be presented as substituting for local approvals or as granting permission to connect to an electricity network.

2.4 Limits and precedence

Where a binding obligation imposes a stricter compatible limit than this draft, that obligation shall apply. Where requirements conflict, the organization shall stop the affected claim or activity, document the conflict and obtain a resolved engineering and legal basis before release. No averaging, commercial waiver or environmental benefit shall compensate for a failed safety or legal requirement.

2.5 Engineering completion

The safety and performance limit schedule in Annex B shall be completed for each assessed configuration before physical verification. Values shall be justified by competent engineering analysis and applicable deployment obligations, independently reviewed, version controlled and fixed before testing. A blank field, an unvalidated threshold or a value selected after observing a result shall block a positive decision for the affected scope.

2.6 Document control

The controlled identity shall be IAF ECIAS First Edition Working Draft 0.2. Changes to requirements, profiles, thresholds and assessment rules shall have recorded rationales, impact reviews and approval status. Future edition adoption shall require closure of the release blockers in Annex L. No draft review record shall imply that IAF has approved an organization or authorized use of a conformity mark.

3 Terms and abbreviations

3.1 Charging equipment and port

Electric vehicle supply equipment, abbreviated EVSE, is equipment that controls and supplies electrical energy to an electric vehicle and, where designed to do so, receives energy from it. A port is the functional capacity to serve one vehicle at a time. A charger with several selectable connectors shall not count each connector as a simultaneously usable port unless simultaneous service is demonstrated.

3.2 Site and charging service

A site is the defined physical charging location including its access routes, bays and shared infrastructure. A charging service is the combined user and technical process for discovering, accessing, authorizing, starting, sustaining, stopping and settling an energy transfer session. A connected controller or responding server alone does not establish service availability.

3.3 Organization and assessor

The responsible organization is the entity accountable for the declared assessment scope. An assessor is a competent person or team evaluating evidence against this document. An independent decision reviewer is a person free from responsibility for the assessed design, implementation and commercial sales decision, with authority to reject insufficient evidence.

3.4 Safe state and critical failure

A safe state is a demonstrated equipment condition that controls the relevant hazardous energy and prevents unsafe restart. It may require isolation, verified discharge, retained mechanical restraint or protected local operation. A critical failure is a condition that creates an unacceptable safety risk, unauthorized hazardous control, material fraud or loss of an essential protective function.

3.5 Configuration and operating envelope

A configuration is an identified combination of hardware, firmware, software, protective settings, interfaces and site conditions. Its operating envelope comprises validated electrical, thermal, environmental, mechanical and communications limits. A capability claim applies only inside that envelope and to the stated combination; a component rating does not establish the integrated system rating.

3.6 Evidence and applicability

Evidence is a retrievable record supporting a requirement, including observations, raw measurements, analyses and signed decisions. Not applicable means a requirement is outside the declared boundary for an evidenced reason. Not tested means the requirement has not been verified. These statuses are distinct and shall not be interchanged to obtain a positive result.

3.7 Technical abbreviations

AC means alternating current; DC means direct current; API means application programming interface; BESS means battery energy storage system; EMC means electromagnetic compatibility; OTA means over the air; PKI means public key infrastructure; SBOM means software bill of materials; SOC means state of charge; V2G means vehicle to grid; V2H means vehicle to home; V2B means vehicle to building; AI means artificial intelligence; UTC means coordinated universal time. These abbreviations identify technologies and functions, not incorporated external publications.

4 Assessment scope and modular structure

4.1 Scope declaration

The organization shall issue a scope declaration identifying legal entity, accountable owner, sites, product families, platform versions, application modules, supported vehicle classes, interfaces, geographical deployment and life cycle stage. It shall identify included and excluded functions and state the boundary of any subcontracted service. The declaration shall be approved before the assessment plan is agreed.

4.2 Assessment objects

Four assessment objects shall be distinguished: product design and manufacture; installed site; digital service platform; and operational charging service. Evidence from one object may support another only where configuration equivalence and interface assumptions are demonstrated. A component test report shall not be promoted into a complete site or service conformity claim.

4.3 Mandatory modules

The core provisions apply to all assessment objects within their responsibilities. Public service, commercial payment, network connectivity, high power, bidirectional transfer, storage integration, wireless transfer, automated connection, mobile deployment and AI functions trigger additional provisions in Annex A. A feature available to users or enabled by remote configuration shall be treated as present even if rarely used.

4.4 Applicability register

Every numbered requirement shall have an owner, applicability status, rationale, evidence identifier, verification method, result and review status. Shared requirements shall name the lead owner and interface contributors. Exclusions shall be approved by the decision reviewer. Safety, truthful scope declaration, traceability and change control shall not be excluded from any assessment object.

4.5 Families and variations

A family grouping shall be supported by an equivalence analysis of protection architecture, insulation, connectors, cooling, firmware, communications, power sharing and intended environment. The highest power unit is not automatically the worst case. Minimum output, longest cable, weakest supply, highest ambient temperature and fault combinations shall be considered when selecting representative samples.

4.6 Claim boundaries

The organization shall publish the actual scope and tested versions with any assessment statement. Unassessed functions shall be described as outside scope or unavailable for use, as appropriate. Future upgrade compatibility shall be a documented design objective until tested; it shall not be described as an existing verified capability.

5 Governance and competence

5.1 Accountable leadership

Management shall appoint an accountable infrastructure owner with resources and authority to stop unsafe operation, fund maintenance and resolve cross-party defects. Named owners shall be assigned for electrical safety, cybersecurity, accessibility, metrology, environmental data and service continuity. Responsibility shall remain documented when multiple organizations jointly operate a site.

5.2 Competence

Personnel performing design, installation, hazardous testing, maintenance or assessment shall have demonstrated competence appropriate to their assigned work. Competence records shall include practical authorization, equipment familiarity, emergency actions and refresher needs. Access to hazardous work or privileged systems shall be withdrawn when authorization expires or responsibilities change.

5.3 Separation of duties

Design approval, installation acceptance, financial reconciliation and conformity decisions shall use independent review proportional to risk. A person shall not approve their own safety-critical work without a documented independent verification. Commercial targets shall not override unresolved technical findings. Conflicts of interest shall be declared and managed before an assessment decision.

5.4 Contractor control

Contracts shall identify required evidence, incident notification, support periods, defect correction, data ownership, access revocation, replacement rights and end-of-service arrangements. The organization shall verify delivery of these obligations. A supplier statement without configuration-specific evidence shall not close a critical requirement.

5.5 Documented information

Controlled procedures shall cover scope, risks, configuration, design changes, commissioning, maintenance, incidents, user complaints and claims. Records shall have identity, owner, creation time, revision, approval and retention rules. Safety and design evidence shall remain retrievable for the declared service life and any longer binding period; personal data retention shall separately follow necessity and applicable obligations.

5.6 Management review

Management shall review safety events, recurring faults, vulnerability exposure, billing disputes, accessibility barriers, resource performance and corrective action effectiveness at least annually and after a critical incident. Decisions shall assign resources, owners and due dates. Unresolved risk shall be escalated without waiting for the next scheduled review.

6 Integrated risk engineering

6.1 Hazard and threat identification

The organization shall maintain an integrated register covering electrical shock, arc energy, overheating, fire, mechanical injury, electromagnetic exposure, vehicle movement, malicious control, fraud, exclusion of users and environmental harm. It shall consider normal operation, reasonably foreseeable misuse, maintenance, degraded modes and end of life. Annex C provides the minimum scenario families.

6.2 Risk evaluation

Each scenario shall identify initiating events, exposed persons or assets, severity, likelihood basis, uncertainty, existing barriers and residual risk. Risk rankings shall be reproducible and approved before mitigation selection. Low observed incident frequency shall not alone justify a low risk where exposure is limited or reporting is incomplete.

6.3 Protective architecture

Risk reduction shall prioritize inherent safety, protective design and verified automatic safeguards before instructions and warnings. Safety functions shall be independent of revenue collection, advertising and cloud optimization to the extent required by the risk analysis. Common causes such as shared power supplies, clocks, communications and software libraries shall be assessed explicitly.

6.4 Fault containment

The organization shall identify fault containment boundaries between ports, power modules, storage, grid interfaces and digital tenants. It shall demonstrate that a fault in one boundary cannot defeat protection in another. Shared resource failures shall trigger a controlled response for every affected port and truthful status reporting.

6.5 Safety case

A configuration-specific safety case shall link hazards to protective requirements, design evidence, verification results, operating constraints and residual risk approval. Assumptions involving vehicles, installers or grid operators shall be explicit and validated at the interface. Unsupported assumptions or unresolved intolerable risks shall prevent release.

6.6 Change and feedback

Risk records shall be reviewed after a new use case, component substitution, software update, incident, recurring complaint or environmental change. Field evidence shall feed back into design and operating controls. A successful initial test shall not exempt later configurations or operating conditions from reassessment.

7 Deployment obligations and approval records

7.1 Jurisdiction register

Each deployment shall have a register of binding obligations, approvals, inspections, connection conditions and renewal events. The register shall identify the affected requirement, responsible person, evidence and next review date. Multi-country product claims shall distinguish configurations and local installation conditions rather than assume one approval applies everywhere.

7.2 Permission to energize

No installation shall enter operational service before required permits, connection permissions, protective coordination, installation checks and commissioning acceptance are complete. Temporary test energization shall follow a separately authorized and controlled test procedure. Public availability shall remain disabled until the accountable owner accepts the commissioning dossier.

7.3 Electrical coordination

Supply capacity, prospective fault conditions, earthing arrangement, protective devices and utility settings shall be coordinated by competent personnel. The deployment dossier shall include single-line diagrams and the approved protection schedule. Replacing a protective device with another nominally similar device shall require verification of its actual characteristics and compatibility.

7.4 Commercial and data duties

The organization shall determine obligations for energy resale, measurement, receipts, taxes, payment security, consumer remedies, data processing and cross-border transfers. User-facing terms shall correspond to the actual operation. Unresolved uncertainty affecting lawful billing or processing shall be corrected before the affected service is offered.

7.5 Ongoing validity

Changes in law, grid conditions, land use or operating arrangements shall trigger a documented impact review. Expired approvals and unresolved inspection conditions shall be treated as nonconformities. Public claims shall be suspended where their lawful basis no longer applies.

8 Design and manufacturing assurance

8.1 Design inputs

Design inputs shall define application, supply and output ranges, simultaneous loading, environment, service life, user population, interfaces, maintenance approach and required protective functions. Requirements shall be traceable to design outputs and verification. Conflicting input assumptions shall be resolved before design approval.

8.2 Component assurance

Safety-critical and security-critical components shall have controlled specifications and approved sources. Evidence shall cover ratings, tolerance, aging, failure modes and compatibility in the assembled system. Counterfeit risk and substitutions shall be assessed. A supplier certificate alone shall not demonstrate performance in the final enclosure, cooling system or installation.

8.3 Design verification

Verification shall include representative worst cases, abnormal operation and relevant single faults. Calculations, simulations and tests shall identify assumptions and limitations. Simulation-only evidence shall not replace physical verification where uncertainty or hazard consequences require direct observation. Failed tests shall be retained with corrective action and retest linkage.

8.4 Manufacturing control

The manufacturer shall control assembly instructions, torque settings, wiring, sealing, protective bonding, firmware loading, key provisioning and inspection equipment. Traceability shall connect each unit to critical components, software identity, production tests and release authorization. Reworked units shall repeat all tests affected by the rework.

8.5 Routine production verification

Every manufactured unit shall undergo the approved routine safety and functional checks appropriate to its architecture. Test fixtures shall detect bypassed protection and incorrect firmware or parameters. A failed unit shall be identified and segregated until correction and authorized retest are complete. Production sampling shall not replace specified checks required on each unit.

8.6 Maintainable design

Equipment shall permit safe inspection and replacement of defined wear items, including connectors, cables, filters, seals and cooling components. The manufacturer shall state service procedures, diagnostic access, spare part dependencies and end-of-support constraints. Repairability shall not introduce unprotected access to hazardous energy or security credentials.

9 Electrical safety and protective functions

9.1 Prevention of electric shock

The design shall prevent accessible hazardous live parts during connection, transfer, disconnection, cleaning and foreseeable misuse. Insulation systems, barriers, protective bonding and enclosure arrangements shall be appropriate to the declared voltage, environment and aging. Verification shall cover intact equipment and the relevant faults in Annex C using the approved limits in Annex B.

9.2 Earthing and fault protection

Protective conductor integrity and the applicable earthing arrangement shall be verified before service. Earth fault and residual current protection shall address AC, pulsating and smooth DC fault components that can occur in the architecture. Loss of protective continuity, neutral abnormalities and upstream protection interactions shall be analyzed and tested where applicable. Software indication alone shall not constitute protective isolation.

9.3 Insulation and isolation monitoring

DC and isolated systems shall monitor or otherwise protect against insulation failure according to the safety case. The design shall identify detection limits, response time, test coverage and behavior during startup, transfer and shutdown. A failed or disconnected monitoring function shall prevent hazardous transfer or initiate a demonstrated safe response.

9.4 Controlled energization

Hazardous output shall not be enabled until the required connection, interlock, vehicle request, polarity, insulation and protective checks are satisfied. The controller shall reject invalid, contradictory or stale inputs. Restart after a protective trip shall require validated conditions and the approved reset policy; repeated automatic retries shall not conceal a persistent fault.

9.5 Shutdown and stored energy

The design shall detect and manage welded contacts, failed switching elements, trapped charge and unintended backfeed from the vehicle or storage. Before accessible release, hazardous energy shall be reduced or contained within the approved limits. Indications of isolation shall correspond to measured or otherwise validated electrical state, not merely to a commanded switch position.

9.6 Overcurrent and surge protection

Conductors, switching devices and protective devices shall be coordinated for overload, short circuit, inrush, surge and fault interruption. The design shall account for parallel power modules and all energy sources. Fault testing shall verify containment and prevention of unsafe re-energization. Protection settings shall be access controlled and included in the assessed configuration.

9.7 Safety function validation

Each electrical protective function shall have defined initiation conditions, safe output, maximum response time, diagnostic coverage, reset conditions and proof-test method. Verification shall include sensor faults, loss of auxiliary power and communications failure. A failed protective function is a critical nonconformity irrespective of whether a normal charging session can still complete.

10 Thermal mechanical and fire safety

10.1 Thermal envelope

The manufacturer shall declare continuous and short-duration power limits over supply voltage, output voltage, ambient temperature, altitude and cooling conditions. Ratings shall distinguish individual ports from shared cabinets. Temperature rise shall be measured at conductors, contacts, semiconductor interfaces and user-accessible surfaces at the approved worst cases.

10.2 Thermal protection

Temperature sensing and protective derating shall prevent operation outside component and touch limits. Open, shorted, detached, biased or stale sensors shall be included in validation. Derating shall occur before hazardous temperatures develop and shall be visible in operational records. Normal commercial control shall not override thermal protection.

10.3 Liquid cooling

Liquid-cooled equipment shall define coolant type, pressure, flow, conductivity where relevant, leak detection, compatibility and maintenance. Loss of flow, blocked paths, leakage into live compartments and freezing shall be tested or otherwise verified within the safety case. Coolant substitution shall require engineering approval and material compatibility evidence.

10.4 Mechanical integrity

Cable supports, handles, couplers, locks, enclosures and fixings shall withstand the declared use cycles, impact, vibration and foreseeable handling. Strain relief and retention shall protect electrical and communication conductors. Damage that defeats protection shall be detectable or prevented from remaining in service. Cable routing shall not create uncontrolled trip or crush hazards.

10.5 Fire and emergency access

The site and equipment design shall address ignition sources, heat propagation, adjacent combustible materials, ventilation, vehicle fire exposure and responder access. Storage and other local energy sources shall have identified isolation arrangements. Emergency information shall distinguish charger isolation from vehicle battery hazards. This standard does not claim that a charger can make a damaged traction battery intrinsically safe.

10.6 Emergency controls

Emergency stop or isolation functions shall be provided where required by the risk assessment and deployment obligations. Their reach, identification, operation, effect and reset shall be validated. Activation shall not create another uncontrolled hazard. Remote stop shall supplement physical protective measures where needed and shall not depend on an unverified communications path.

11 Environmental durability and electromagnetic performance

11.1 Environmental classification

The organization shall declare indoor or outdoor use and credible extremes of temperature, humidity, precipitation, dust, salt, solar radiation, altitude, flooding, vibration, seismic movement and pollution. The classification shall reflect the actual site. A nominal enclosure rating shall not alone establish resistance to all environmental combinations.

11.2 Ingress and condensation

Enclosures and interfaces shall resist the declared water and particle exposure in operating, disconnected and service states. Drainage, seals, ventilation and condensation control shall be verified after relevant aging and mechanical conditioning. Flood exposure shall trigger isolation and an inspection decision; automatic drying shall not constitute evidence that equipment is safe to return to service.

11.3 Aging and corrosion

Materials shall be evaluated for corrosion, ultraviolet degradation, chemical exposure, cable flexing and seal aging over the declared service conditions. Accelerated tests shall identify their relation and limitations to field life. Post-conditioning verification shall repeat the safety and functional checks most affected by deterioration.

11.4 Electromagnetic emissions

Conducted and radiated emissions shall be evaluated at relevant ports, operating modes and simultaneous load conditions. The assessment shall include power conversion, communications, wireless transfer and local storage when present. Equipment shall meet the limits fixed in Annex B for its deployment, including applicable radio permissions.

11.5 Electromagnetic immunity

The system shall maintain protective functions under the specified disturbances, including transient events, radio frequency exposure, electrostatic discharge, supply dips and interruptions. Loss of nonessential functionality may be acceptable only within a predeclared performance criterion. Unsafe energization, protection defeat, material billing corruption or uncontrolled restart shall constitute failure.

11.6 Combined exposure

The verification plan shall justify test sequencing where heat, moisture, corrosion, vibration and electrical stress interact. It shall identify configurations requiring combined or sequential conditioning. A passed test on a pristine specimen shall not establish durability after an unassessed environmental exposure.

12 Power delivery and grid integration

12.1 Truthful power declaration

The organization shall distinguish nameplate capacity, continuous output, short-duration output, installed supply capacity, shared capacity and vehicle-requested power. Public information shall state material power-sharing and derating conditions. A peak value achievable only briefly or by one port shall not be advertised as sustained simultaneous capacity for every port.

12.2 Electrical performance

Power quality, voltage and current regulation, ripple, power factor, harmonic behavior and ramp rates shall be verified against the completed Annex B schedule. Testing shall include minimum stable load, representative part loads, rated continuous load and transitions. Measurement boundaries and auxiliary loads shall be explicit. No universal numeric limit shall be inferred from an equipment category alone.

12.3 Load management

Site control shall keep aggregate demand within the approved connection and conductor limits under normal and degraded conditions. It shall consider phase imbalance, diversity, local generation, storage and non-charging building loads. If remote optimization or metering becomes unavailable, a tested local fallback shall maintain those limits without defeating electrical protection.

12.4 Grid disturbances

Response to loss of supply, voltage or frequency excursions, phase loss and repeated restoration shall be defined with the grid interface requirements. Recovery shall avoid uncontrolled simultaneous restart or oscillation across a fleet. Any intentional ride-through or island operation shall be separately authorized, tested and identified in the scope.

12.5 Dispatch controls

External grid or commercial dispatch commands shall be authenticated, time bounded and checked against local electrical limits and user commitments. Conflicting commands shall follow a documented priority order. Electrical protection shall have highest priority, followed by binding network constraints, user consent and agreed service commitments before economic optimization.

12.6 Capacity evidence

The commissioning dossier shall include simultaneous-load results, feeder constraints and the tested maximum site demand. Future expansion shall not be described as available capacity until the supporting design and permissions are complete. Changes in shared loads or supply conditions shall trigger capacity and protective coordination review.

13 Physical interfaces and vehicle compatibility

13.1 Interface register

Each supported coupler, cable, inlet relationship, adapter and vehicle communication profile shall be identified by exact type, version, rating and limitations in the implementation register. The register shall distinguish native interfaces from adapters. Public claims shall correspond to the tested combinations and shall not imply compatibility with every vehicle using a visually similar connection.

13.2 Coupling safety

Connection and disconnection shall maintain the intended protective sequence and mechanical retention. Partial insertion, incorrect orientation, contamination, worn contacts, damaged latches and drive-away shall be addressed by design and validation. Hazardous transfer shall be inhibited where connection integrity is not established.

13.3 Cable and connector ratings

The system shall enforce the lowest applicable current, voltage, temperature and duty-cycle limits of the actual cable and connector assembly. Cable identification shall resist undetected substitution or corruption where it affects safety. A software power setting shall not authorize a cable beyond its validated rating.

13.4 Adapters and extensions

Adapters and extensions shall be permitted only within an explicitly assessed configuration. Verification shall include protection continuity, locking, signaling, thermal performance and misuse risk. Unsupported chaining or unidentified adapters shall be prevented where feasible or clearly prohibited with a documented residual risk assessment.

13.5 Wear and contamination

Acceptance criteria shall define when a connector, cable or contact requires inspection, cleaning, repair or replacement. Inspection methods shall detect damage likely to cause heating, loss of protective continuity or unreliable connection. Field wear information shall update the maintenance interval and product improvement process.

13.6 Compatibility testing

The organization shall demonstrate interoperability using independent implementations and representative vehicles or validated simulators as required by Annex E. Tests shall include negotiation boundaries, stop requests, reduced capability and failure recovery. A single successful demonstration or protocol declaration shall not establish broad interoperability.

14 Communications and service interoperability

14.1 Interface specification

Machine interfaces shall have controlled message definitions, units, state meanings, timing, error behavior, authentication and version negotiation. The register shall identify supported and unsupported functions. Proprietary extensions shall be documented sufficiently for safe integration and migration and shall not silently change the meaning of a common field.

14.2 End to end compatibility

Verification shall cover vehicle to charger, charger to site controller, charger to management platform, service provider to service provider, payment and energy dispatch interfaces within scope. Evidence shall link the complete tested path and versions. Passing each interface independently shall not replace integrated session testing.

14.3 Data and state consistency

Transaction identifiers, timestamps, energy units, prices and state transitions shall remain consistent across systems. Duplicate, delayed, out-of-order, missing and conflicting messages shall be handled deterministically. Recovery shall not create duplicate charges, phantom sessions or an energized port without an accountable session state.

14.4 Roaming and identity

Where roaming is offered, the organization shall test authorization, tariff presentation, session records, reconciliation, refunds and identity lifecycle across the declared partners. Expired contracts and revoked credentials shall be handled without unintended access. A roaming logo or commercial agreement shall not substitute for operational evidence.

14.5 Portability and exit

The organization shall be able to export asset configuration, service history and required operational records in a documented machine-readable form. A platform migration plan shall address device re-enrollment, keys, authorization, metering records and continuity. Secure credential re-issuance may replace credential transfer where disclosure would weaken security.

14.6 Version management

Compatibility matrices shall identify supported version combinations and retirement dates. New platform or charger releases shall undergo impact-based regression testing before broad deployment. Unknown or incompatible versions shall produce a controlled failure or explicitly tested degraded mode, never an assumed successful negotiation.

15 Charging session integrity

15.1 State model

The organization shall define a state model covering unavailable, available, connected, authorizing, negotiating, charging, suspended, stopping, completed and faulted states. Each transition shall have initiating conditions, permitted outputs and recovery actions. The state shown to users shall correspond to the physical port and service capability.

15.2 Session initiation

Session initiation shall verify required safety checks, user authorization, price acceptance and negotiated electrical limits before transfer. The organization shall record the first eligible attempt separately from retries. Failures before energy flow shall not be hidden by creating a new transaction identifier for each retry.

15.3 Transfer control

Delivered energy shall remain within vehicle requests and equipment, site and user limits. A missing or invalid request shall not be interpreted as permission for maximum output. Charging pause and restart shall preserve session identity, price rules and safety checks. Charging beyond a user-defined budget or energy limit shall be prevented within the declared measurement tolerance.

15.4 Session stop and release

User stop, vehicle stop, contractual completion, fault and emergency actions shall lead to defined shutdown behavior. Required physical isolation and energy reduction shall precede connector release. The user shall receive an understandable outcome and a method to obtain assistance if release fails. Remote release shall not bypass protection.

15.5 Interrupted sessions

Power loss, network loss, platform restart and controller reset shall preserve sufficient records to reconstruct delivered energy and billing. If reconciliation is uncertain, disputed energy shall be held for review and not automatically charged as a confirmed amount. Restart policies shall respect user consent and local protective checks.

15.6 Offline behavior

Offline operation shall have a predeclared security, billing and electrical risk limit. Allowed credentials, transaction value limits, storage capacity and reconnection behavior shall be tested. When those limits are exceeded, the affected service shall enter a controlled unavailable state. Offline free charging, where intentionally provided, shall still preserve essential safety and energy records.

16 Cybersecurity and trust architecture

16.1 Asset and threat model

The organization shall inventory hardware, software, interfaces, accounts, remote paths and trust dependencies. Threat analysis shall cover unauthorized energy control, fleet disruption, grid manipulation, credential theft, payment fraud, malicious updates and physical tampering. Security measures shall be linked to safety consequences and the declared support life.

16.2 Access control

Devices, services and administrators shall use unique identities appropriate to their role. Shared default passwords shall not remain active in deployed equipment. Privileged remote access shall use strong multi-factor authentication, least privilege, time-limited authorization and attributable logs. Service access shall be revoked promptly after completion or contract termination.

16.3 Network separation

Safety control, operations, payment, user connectivity and maintenance traffic shall have defined trust boundaries and restricted communication paths. Public wireless access shall not provide an uncontrolled route to charging control. Internet exposure shall be minimized and reviewed. An unavailable cloud shall not disable locally required protective functions.

16.4 Cryptographic protection

Sensitive communication and commands shall have confidentiality where needed, integrity, peer authentication and replay protection. Keys shall be generated, provisioned, stored, rotated and revoked through controlled processes. Trust store changes shall be authenticated and logged. Expiry, invalid time, compromised issuers and loss of revocation connectivity shall have tested fail-safe or bounded fallback behavior.

16.5 Secure development

Software development shall include threat review, code review, dependency control, secret scanning, security testing and release approval. The organization shall retain an SBOM or equivalent dependency inventory with versions and support status. Known exploitable vulnerabilities affecting the declared configuration shall have an assessed treatment before release.

16.6 Security verification

Independent testing shall cover exposed services, privilege boundaries, management APIs, local service ports, command integrity and physical access relevant to the threat model. Testing shall occur in controlled environments with authorized scope. Production testing that could affect hazardous energy shall require an approved safety plan. Findings shall be corrected and retested under Annex H.

16.7 Long term trust

The organization shall maintain a cryptographic inventory and migration plan for algorithm, key-size and trust-anchor changes over the equipment life. Claims of quantum-resistant security shall identify the actual implemented protection and tested interoperability. Cryptographic migration shall not disable safety, strand deployed equipment or silently accept weaker unauthenticated control.

17 Software updates and configuration integrity

17.1 Release identity

Every deployed software and firmware component shall have an unambiguous version and integrity identifier linked to its hardware and configuration. The organization shall know which devices are affected by a defect. Untracked local modifications and undocumented parameter changes shall block a configuration-specific conformity statement.

17.2 Update authenticity

Updates shall be authenticated and verified for integrity and target compatibility before installation. Unauthorized signing keys, corrupted packages and wrong hardware targets shall be rejected. Boot and execution controls shall prevent unapproved software from controlling hazardous functions. Signing key compromise shall have a tested recovery process.

17.3 Safe installation

An update shall not interrupt a critical protective function or active energy transfer unless the procedure first places the equipment in a safe state. Power interruption, network interruption, insufficient storage and reset during installation shall be tested. The equipment shall recover to a verified operational version or remain safely unavailable.

17.4 Rollback and recovery

Recovery shall balance availability with prevention of downgrade to known vulnerable software. An authorized rollback path shall identify eligible versions, approval, compensating controls and revalidation. Emergency service restoration shall not silently restore compromised credentials or unsafe settings.

17.5 Deployment control

Updates shall use staged release, monitored pilot deployment and stop criteria proportional to risk. Safety, session success, billing and resource metrics shall be checked after deployment. A material regression shall trigger rollback or containment and reassessment of affected claims. The organization shall retain failed deployment records.

17.6 Support life

The declared support period, security contact, end-of-support notice and maintenance dependencies shall be available before procurement. End of support shall trigger a risk review, migration or decommissioning plan. Equipment shall not remain marketed as secure merely because it continues to charge after its essential security support has ended.

18 Privacy data governance and evidence protection

18.1 Data inventory

The organization shall identify data collected from users, vehicles, payments, sensors and infrastructure, including location and behavioral inferences. For each category it shall record purpose, lawful basis where required, access, recipients, retention and deletion. Collection shall be limited to what is needed for the declared service and obligations.

18.2 User choice

Users shall receive clear information before optional collection or secondary use. Consent where relied upon shall be specific, recorded and withdrawable. Access to essential public charging shall not be made conditional on unrelated marketing or unnecessary tracking. Alternative authentication shall be available where required by the applicable service profile.

18.3 Separation and minimization

Operational telemetry shall use pseudonymous or aggregated identifiers where personal identity is not required. Public evidence records shall exclude personal credentials, exact user journeys and payment secrets. Combining vehicle and charging data for profiling shall require an explicit authorized purpose and risk review.

18.4 Protection and retention

Personal and sensitive operational data shall have access controls, protected transfer, backup and verified deletion appropriate to their risk. Safety evidence shall retain necessary traceability without unnecessarily retaining personal data. Deletion from live systems, replicas and backups shall follow a documented lifecycle with justified legal holds.

18.5 Rights and incidents

The organization shall provide processes for access, correction, deletion and complaints as applicable. Suspected data exposure shall be assessed, contained and notified within the binding time limits. Incident evidence shall be protected from alteration and unnecessary dissemination. A commercial confidentiality claim shall not prevent required notification.

18.6 Cross party governance

Data sharing agreements shall identify controller and processor responsibilities or equivalent accountable roles, onward transfer restrictions and exit arrangements. Remote platform changes shall include privacy review. The organization shall verify that exported evidence remains readable and that departing suppliers lose access to operational and personal data.

19 Metering payment and consumer protection

19.1 Measurement boundary

The billing measurement point shall be defined physically and in the transaction record. The organization shall state whether energy is measured before or after conversion, cable loss or other equipment, subject to deployment obligations. User billing shall not include undisclosed auxiliary consumption or double-counted energy. Import and export shall be separately measurable where both occur.

19.2 Meter accuracy

Meters shall be suitable for the declared voltage, current, waveform, direction, temperature and load range. Calibration or verification shall be traceable, current and linked to the actual meter identity. Measurement error, uncertainty, drift, sealing and software integrity shall be assessed against the fixed Annex B limits. A display resolution shall not be presented as an accuracy claim.

19.3 Price transparency

Before commitment, the user shall be shown the currency, energy rate, time-based or session fees, parking and idle fees, taxes where applicable and material conditions. The accepted pricing basis shall be preserved for the session. Undisclosed mid-session price changes shall be prohibited. Dynamic tariffs shall identify the accepted schedule or bounded rule before the user starts.

19.4 Public access and payment

Public charging shall provide a practical ad hoc route without mandatory long-term membership or an unnecessary proprietary application. Payment methods shall comply with local requirements and work for the intended users. QR payment routes shall identify the legitimate service and address physical substitution risk. Failure of one advertised payment method shall be visible and recorded.

19.5 Transaction integrity

Authorization, preauthorization, capture, reversal, refund and receipt generation shall be tested as one process. Retries shall not create duplicate financial capture. A failed session shall release or reconcile holds under the declared payment rules. Timeouts and service outages shall not justify billing estimated energy as a verified meter value.

19.6 Receipts and disputes

Receipts shall identify site, port, session, times, delivered energy, applicable price components, total amount and assistance channel. Users shall have a usable method to dispute a transaction without recreating inaccessible technical evidence. The organization shall reconcile complaints with meter and session records and correct material errors across all affected users, not only the complainant.

20 Accessibility and user experience

20.1 Inclusive design

The site and interface shall support people with mobility, reach, dexterity, visual, hearing and cognitive differences. The accessibility plan shall define the intended user tasks and applicable dimensions and interaction limits. It shall be assessed with representative users and measured site conditions, rather than relying solely on a drawing or accessibility icon.

20.2 Physical access

Accessible routes, charging bays, transfer space, gradients, surface conditions and protective barriers shall permit approach and operation without avoidable obstruction. Cable reach shall consider different vehicle inlet positions. Cable handling forces and control reach shall be measured against the approved Annex B schedule. A heavy connector shall have suitable handling assistance when needed.

20.3 Interface access

Instructions, controls, payment and emergency information shall use legible text, adequate contrast and more than color alone to convey meaning. Audio shall not be the sole information channel. Timed interactions shall allow an accessible extension where safe. The essential journey shall remain possible without relying on an inaccessible smartphone interface.

20.4 Clear operation

The interface shall communicate connection status, charging progress, power constraints, price, stop actions and recovery guidance in understandable language. Essential instructions shall be available in languages appropriate to the deployment. Technical fault codes may accompany user guidance but shall not replace it.

20.5 Assistance and site safety

Public sites shall provide a visible assistance method linked to a unique site and port identifier. Lighting, pedestrian movement, weather exposure and personal security shall be addressed in the site risk assessment. The organization shall test whether assistance can resolve common failed-start and trapped-connector scenarios.

20.6 Accessibility continuity

Maintenance, resurfacing, signage, parked service vehicles and cable replacements shall not remove essential accessible features without an approved alternative. Accessibility complaints shall enter corrective action and trend review. A public accessibility claim shall identify which bays and functions were assessed and any material limitations.

21 Site planning and infrastructure integration

21.1 Site suitability

The design shall consider demand, vehicle dimensions, arrival patterns, queue capacity, dwell times, public access, emergency access and surrounding land use. Depot and heavy vehicle designs shall include turning paths and swept areas. Capacity planning shall distinguish projected demand from measured demand and disclose uncertainty.

21.2 Civil and structural works

Foundations, anchorage, canopies, trenches, ducts, cable routes, drainage and impact protection shall be designed for credible site loads and environmental exposure. Underground services shall be identified before excavation. Civil works shall preserve inspection access and the separation of power, communication and drainage functions where required.

21.3 Traffic and parking

Vehicle approaches, bay markings, bollards and cable positions shall reduce collision, trapping and trip risks. Queues shall not obstruct emergency routes or accessible paths. Availability information shall distinguish a working but occupied port from a failed or physically blocked port.

21.4 Shared energy resources

Solar generation, storage, building loads and charging control shall have coordinated metering, isolation, control priorities and fault response. The site diagram shall identify every source capable of energizing a circuit. Loss of one controller shall not allow uncontrolled export, overload or hidden energized conductors during maintenance.

21.5 Climate resilience

The site assessment shall consider projected exposure over the declared life, including heat, flood, storm, wildfire smoke, water scarcity and salt. Adaptation measures shall have inspection and recovery procedures. Climate projections shall identify location, period, uncertainty and design assumptions; a future-ready claim shall not imply immunity to all hazards.

21.6 Expansion readiness

Reserved electrical capacity, physical space, ducts, communications and access for expansion shall be documented where claimed. Expansion design shall preserve protection, accessibility and emergency arrangements. An installed spare conduit or oversized cabinet alone shall not establish readiness for a new charging technology.

22 Installation commissioning and handover

22.1 Installation control

Installation shall follow approved drawings, equipment instructions and the deployment dossier. Competent personnel shall record wiring, protective bonding, torque, seals, labeling, meter identity and configuration. Deviations shall be reviewed before concealment or energization. As-built records shall show the actual completed installation.

22.2 Pre-energization checks

The installer shall verify mechanical completion, protective arrangements, supply conditions, clearances, isolation devices, accessibility and emergency information. Test instruments shall have suitable ranges and current verification. Failures shall be corrected before operational energization. Annex K provides the minimum handover checks.

22.3 Integrated commissioning

Every operational port shall complete safety checks and an end-to-end session using the installed platform and applicable payment route. Shared power allocation, simultaneous demand, network loss, stop, restart and fault isolation shall be verified. Representative vehicle testing shall supplement simulated loads where actual interoperability or user handling is at issue.

22.4 Public information validation

Site location, connector types, hours, power, accessible facilities, payment methods, tariffs and contact details shall be checked against physical reality and the live service. Fault and occupancy states shall propagate to advertised channels within the Annex F target. Marketing claims shall not precede commissioning evidence.

22.5 Handover dossier

The dossier shall contain the approved scope, as-built diagrams, settings, inspection results, limit schedule, software identities, maintenance plan, spare parts, emergency plan, training and outstanding minor items. Critical and major findings shall be closed before acceptance. The accountable owner shall sign the decision to open the service.

22.6 Early service review

The organization shall monitor the first operational period for defects that laboratory or commissioning tests may miss. Session failures, thermal derating, billing errors, user barriers and lost telemetry shall trigger investigation. Operational performance claims shall remain provisional until the observation requirements in Annex F are met.

23 Operation maintenance and reliability

23.1 Operational monitoring

The organization shall monitor service capability, protective events, temperatures where relevant, communications, meter integrity and unusual control behavior. Monitoring shall distinguish online status from successful charging capability. Missing telemetry shall be identified as unknown and treated conservatively in availability reporting as specified in Annex F.

23.2 Maintenance planning

Maintenance intervals shall reflect manufacturer instructions, risk, use cycles, climate, condition data and field failures. The plan shall cover protection checks, connector wear, cable condition, cooling, seals, firmware, emergency controls and accessibility. Mandatory maximum intervals shall not be extended solely because a predictive model reports no anomaly.

23.3 Fault response

Faults shall have severity, responsible owner, detection time, response target and restoration evidence. Unsafe ports shall be isolated promptly and marked unavailable in all controlled channels. A remote reset shall not close a defect without evidence that its cause and recurrence risk are acceptable.

23.4 Repair and return to service

Repairs shall use approved parts, controlled settings and authorized personnel. The organization shall repeat safety, functional and interoperability checks affected by the repair and record the resulting configuration. Replacement cables, meters, controllers and cooling components shall be traceable. A repaired unit shall not inherit previous test results without an equivalence review.

23.5 Reliability analysis

The organization shall analyze first-attempt success, interruptions, recurrent resets, component failures, repair duration and derating by site, port, configuration and cause. Network averages shall be accompanied by the weakest performing ports and distributions. Repeated defects shall trigger systemic corrective action rather than repeated individual closure.

23.6 Service transfer and closure

Ownership changes or platform withdrawal shall preserve essential records, responsibilities, keys and user remedies. Planned closure shall update public information and provide orderly settlement. Decommissioning shall isolate every energy source, remove or secure credentials and personal data, and route materials to controlled reuse or recovery.

24 Continuity incident response and recovery

24.1 Continuity plan

The organization shall define critical services and acceptable degradation for loss of electricity, communications, platform, payment provider, staffing, cooling or parts. The plan shall identify recovery priorities and dependencies. Critical fleet and emergency transport commitments shall be explicit contractual profiles, not assumed capabilities of a public network.

24.2 Safe degraded operation

Degraded operation shall remain within the approved electrical, security, billing and user-information limits. Essential protection shall continue locally. If a required safeguard or reliable transaction boundary is unavailable, the affected function shall stop safely. Availability targets shall not justify bypassing a protective control.

24.3 Backup and restoration

Configuration, required transaction records and recovery keys shall be backed up with controlled access. Restore tests shall demonstrate readable data, correct configuration and usable credentials on representative replacement hardware or systems. Backups containing compromised settings shall not be restored without review.

24.4 Incident management

Incidents shall be classified, contained, investigated and recorded with time, scope, affected configurations and user impact. Safety incidents, malicious control and material billing corruption shall trigger immediate technical escalation. Reporting to affected parties and authorities shall follow applicable deadlines; internal draft targets shall not delay binding notifications.

24.5 Recovery validation

Restoration shall verify protective functions, configuration integrity, transaction reconciliation, advertised status and absence of the initiating fault. The accountable owner shall approve return to service after a critical incident. A cloud status change alone shall not establish physical restoration.

24.6 Exercises and learning

At least annually, the organization shall exercise a representative outage and cyber incident scenario covering technical and customer support teams. The exercise shall include an inaccessible or remote site where relevant. Findings shall have owners, deadlines and retest evidence. Actual incidents may supplement but shall not automatically replace planned coverage.

25 Sustainability energy and circularity

25.1 Environmental boundary

The organization shall identify material impacts from equipment manufacture, civil works, transport, installation, energy use, auxiliary loads, maintenance, replacement and end of life. Assessments shall state location, life, utilization, data quality and exclusions. A narrow operational energy calculation shall not be presented as a complete life cycle footprint.

25.2 Energy performance

Conversion efficiency, cable loss, standby consumption and site auxiliary energy shall be measured using defined boundaries and load profiles. The organization shall report representative part-load and seasonal operation as well as peak efficiency. Minimum targets shall be set before testing for the application and shall be maintained in Annex B and the procurement specification.

25.3 Carbon accounting

Operational emissions shall use traceable energy quantities and documented emission factors with geographical and temporal relevance. Physical electricity accounting and contractual environmental attributes shall be reported separately. Exported energy, storage losses and renewable attributes shall not be double counted. Avoided emissions and offsets shall be disclosed separately from the measured footprint.

25.4 Resource stewardship

The organization shall quantify material water, coolant and resource use relevant to the site. It shall address leakage, hazardous substances, local water stress, waste and noise. Material substitution shall evaluate safety and durability consequences before environmental benefit is claimed. Cooling water savings shall not be achieved by operating outside verified thermal limits.

25.5 Circular design and procurement

Equipment procurement shall consider service life, modular repair, spare parts, recoverable materials, disassembly and supplier take-back where available. Reused and refurbished equipment shall have provenance, remaining-life assessment and requalification of affected functions. Recycled content shall be supported by traceable data rather than inferred from recyclability.

25.6 Improvement and claims

The organization shall establish time-bound improvement objectives for significant impacts and review actual results. Environmental claims shall identify baseline, method, boundary and uncertainty. Annex I provides an illustrative calculation without imposing a universal efficiency or carbon threshold. Unsupported terms such as zero impact or fully sustainable shall not appear in a conformity statement.

26 Supply chain integrity and ethical procurement

26.1 Supplier risk

Supplier assessment shall consider criticality, manufacturing capability, evidence reliability, cybersecurity support, service continuity, labor and environmental risk. Higher-risk suppliers shall receive additional verification. Price or delivery urgency shall not justify undocumented substitution of safety-critical parts or unsupported software.

26.2 Traceability

The organization shall trace critical components, meters, cables, power modules, secure elements and software dependencies to approved sources and relevant production lots. Traceability shall support targeted recall and configuration identification. Missing provenance shall trigger risk review and, where critical, prevent release.

26.3 Due diligence

Procurement controls shall identify and address credible risks of forced labor, unsafe working conditions, irresponsible material sourcing and severe environmental harm. Assessment shall be proportionate to leverage and risk and shall include evidence of corrective action. A contractual declaration alone shall not close a credible unresolved severe risk.

26.4 Serviceability commitments

Suppliers shall disclose spare part availability, security support, diagnostic access, licensing dependencies and obsolescence plans. The organization shall evaluate concentration risk and alternative repair paths. Business failure or platform discontinuation shall be included in continuity planning for essential dependencies.

26.5 Counterfeit and tamper controls

Incoming inspection, identity checks and secure provisioning shall address counterfeit, altered and unauthorized refurbished components. Suspect parts shall be quarantined and traced to affected assemblies. Confirmed systemic issues shall trigger broader investigation and necessary notification.

26.6 Procurement acceptance

Acceptance shall verify delivered configuration, documentation, software support, environmental data and required test results against the contract. Deviations shall be resolved with independent review. A purchase order marked complete shall not establish technical acceptance or conformity.

27 Bidirectional charging and energy exchange

27.1 Module activation

This clause applies whenever equipment can intentionally export energy from a vehicle to the grid, building, home, local storage or another permitted load. The scope shall identify each supported mode, electrical boundary and permission. Export capability shall remain disabled until its approvals and verification are complete.

27.2 User consent and vehicle limits

Energy export shall require explicit authorization covering minimum retained charge, departure needs, power limits, time windows and compensation where applicable. The controller shall respect vehicle limits and user withdrawal. Unknown or stale SOC data shall trigger a bounded response that protects the agreed reserve.

27.3 Electrical interface

Export operation shall meet the approved grid and installation protection schedule. Unintentional islanding and backfeed into circuits assumed isolated shall be prevented. Intentional island operation shall have verified isolation, earthing, load management, transition and resynchronization arrangements. Import compliance alone shall not establish export compliance.

27.4 Dispatch and aggregation

Aggregated commands shall be bounded by each vehicle, port, site and connection limit. Authentication, replay protection and rate limits shall prevent unauthorized coordinated switching. Loss of the aggregator shall lead to a tested local state. Settlement incentives shall not override safety or user energy reserves.

27.5 Measurement and battery impacts

Import and export energy shall be recorded separately with consistent measurement boundaries. Round-trip losses, settlement rules and any battery degradation assumptions shall be transparent. A claim of increased battery life or guaranteed net savings shall require evidence for the declared use conditions and shall not be inferred from bidirectional capability alone.

27.6 Verification

Tests shall cover transition between import and export, emergency stop, lost grid, lost communications, SOC limits, conflicting schedules, meter direction and restoration. A complete approval shall identify the tested modes and interface versions. Untested V2H, V2B or V2G modes shall remain outside scope even if the same hardware is used.

28 High power and heavy vehicle charging

28.1 Application boundary

This clause applies to any megawatt-class claim, heavy road vehicle deployment or system whose current, thermal or handling risks require high-power measures. The organization shall define voltage, current, continuous power, duty cycle, cooling and vehicle classes. It shall not infer a universal megawatt rating from the connector name.

28.2 High current integrity

Verification shall address contact resistance, current sharing, inductive effects, switching energy, connector heating and fault containment at the declared envelope. The test plan shall include reduced output voltage at maximum current where this is a worst case. Temperature measurement locations shall cover hotspots identified by design analysis.

28.3 Cooling and handling

Cooling performance shall be verified for blocked flow, pump failure, leaks, high ambient temperature and repeated sessions. Cable mass, bending, reach and connection forces shall be assessed with the intended users. Handling assistance or automation shall not introduce crush or trapped-person risks.

28.4 Depot and corridor integration

The site shall address trailer access, turning space, charging position, queues, emergency routes and driver rest or operational schedules. Guaranteed departure energy shall be tied to actual connection capacity and vehicle availability. Shared power planning shall disclose assumptions and manage missed-arrival or delayed-departure conditions.

28.5 Protection and maintenance

High-energy isolation and maintenance procedures shall identify all sources, discharge times, verification points and restricted areas. Arc and thermal hazards shall be assessed by competent personnel. Contact wear, cooling condition and repeated high-load operation shall feed a risk-based inspection and replacement plan.

28.6 Performance claims

Charging time claims shall specify vehicle or simulator, initial and final SOC where applicable, battery temperature, power curve, site sharing and ambient conditions. The measured delivered energy and time shall be retained. An instantaneous maximum power observation shall not establish sustained charging time performance.

29 Wireless automated and dynamic charging

29.1 Wireless module

Wireless charging shall have defined alignment, air gap, power, frequency, shielding, exposure zones and supported vehicle receivers. Verification shall cover misalignment, foreign objects, living-object intrusion, metallic debris and abnormal temperature. Exposure and thermal limits shall be fixed in Annex B and independently reviewed before testing.

29.2 Detection and safe interruption

Detection functions shall prevent or interrupt transfer when hazardous objects or conditions enter the assessed zone. Tests shall include detection blind spots, sensor faults, weather and representative objects. A vision model confidence score shall not alone establish a safe condition. Residual risks shall be reflected in physical design and operating controls.

29.3 Automated connection

Robotic, underbody or overhead connection shall verify vehicle position, immobilization, clear operating space and safe contact before energization. Human approach, trapped objects, loss of position sensing and unexpected vehicle movement shall cause a safe response. Manual recovery shall not require unprotected entry into an energized or moving mechanism.

29.4 Autonomous operation

Unattended charging shall define responsibility for arrival, authorization, docking, charging, release and departure. The control system shall confirm cable or mechanism clearance before motion authorization. Remote supervision and local fallback shall be tested. A successful autonomous demonstration shall not establish safe operation in all public environments.

29.5 Dynamic road charging

Dynamic charging is a conditional extension requiring a dedicated project safety case, roadway permissions and full interface definition. Verification shall address selective segment energization, vehicle speed, road users, debris, weather, maintenance isolation, billing attribution and emergency access. Base stationary charging evidence shall not by itself authorize dynamic operation.

29.6 Module claims

Wireless, robotic, overhead, underbody and dynamic capabilities shall be listed separately with their tested envelopes. Unvalidated concepts shall remain development objectives. The organization shall not use the term future-ready to imply completed assessment of a new energy transfer mechanism.

30 Mobile storage assisted and constrained grid charging

30.1 Mobile deployment

Mobile charging equipment shall define transport state, deployment state, stability, restraint, earthing where applicable, environmental limits and exclusion zones. Pre-use checks shall verify location and configuration after movement. Transport damage and movement during transfer shall be addressed in the safety case.

30.2 Storage integration

Storage-assisted charging shall include the storage system within the relevant safety, fire, metering and control boundary. The organization shall verify battery protection, isolation, thermal management, fault signaling and emergency access. Declared charger power shall distinguish storage-supported duration from sustainable grid-supported output.

30.3 Off grid and weak grid operation

The system shall maintain supply quality and protection across variable generation, weak supply and low stored energy. The available service shall be derated or suspended before unsafe operation occurs. Fuel-based backup, where present, shall be included in emissions, noise, ventilation and fuel safety assessments.

30.4 Emergency deployment

Emergency charging shall have defined competence, deployment checks, safe location criteria and assistance arrangements. Urgency shall not waive electrical isolation, stability or user protection. The operator shall communicate limited capacity, duration and conditions without presenting temporary service as permanent infrastructure approval.

30.5 Multi vehicle applications

Motorcycles, light commercial vehicles, buses, trucks and industrial road vehicles may use this standard where their interfaces and hazards are explicitly assessed. A change in vehicle class shall trigger review of voltage, connection, handling, movement and communication assumptions. Micromobility battery exchange and non-road equipment require separate scope development.

30.6 Performance and recovery

Tests shall include depleted storage, failed local generation, overload requests, thermal derating, emergency stop and restoration after movement. Energy origin and conversion losses shall be accounted for without double counting. The assessment record shall identify the operational duration and replenishment assumptions supporting each power claim.

31 Artificial intelligence and emerging technology governance

31.1 Function classification

The organization shall identify AI used for charging schedules, fault detection, pricing, customer interaction, security or physical automation. Each function shall have intended use, data requirements, operating limits and human accountability. Safety-related inference shall receive assurance proportional to the consequences of error.

31.2 Bounded control

AI outputs shall be constrained by verified electrical limits, user consent, grid obligations and independent protective functions. Uncertain, missing or adversarial input shall trigger a defined fallback. An optimizing model shall not directly change protection settings without controlled engineering authorization and revalidation.

31.3 Data and model assurance

Training and validation data shall have documented provenance, relevance, quality and known gaps. Validation shall cover distribution shifts, uncommon conditions and affected user groups. Model versions, parameters and material dependencies shall be traceable. Performance on a selected demonstration dataset shall not be presented as universal field accuracy.

31.4 Operational monitoring

The organization shall monitor model drift, false alarms, missed faults, unfair service allocation and unexpected behavior. Thresholds for intervention and rollback shall be fixed before deployment. Users shall receive appropriate explanations and a human review route where automated decisions materially affect access, price or remedies.

31.5 Digital models and remote testing

Digital twins and hardware simulations shall have a stated purpose, calibration evidence, error bounds and validated operating domain. Differences between model and field results shall be investigated. A virtual test may support but shall not conceal missing physical safety or user validation.

31.6 Technology transition

Annual horizon review shall consider new vehicle architectures, power levels, storage chemistries, trust systems, communications and charging mechanisms. A new technology shall enter a controlled extension with requirements, hazards, test methods and release criteria before being claimed. Predictions in Annex L are planning scenarios rather than assured future outcomes.

32 Verification conformity decisions and public claims

32.1 Assessment plan

Before testing, the assessor shall approve scope, applicable requirements, sampling rationale, limit schedule, equipment, uncertainty treatment and decision rules. Annex D defines the minimum verification catalogue and Annex E the interoperability coverage. Test plans shall record who performs, witnesses and independently reviews each critical activity.

32.2 Evidence quality

Evidence shall identify specimen, configuration, method revision, test conditions, instrument identity, calibration status, raw results, uncertainty where relevant and deviations. A report shall distinguish measured, calculated and declared values. Incomplete or unverifiable evidence shall be marked not demonstrated rather than passed.

32.3 Measurement decision rule

For a numerical upper safety limit, acceptance shall require the measured value plus its stated expanded uncertainty to remain at or below the limit. For a lower limit, the measured value minus uncertainty shall remain at or above the limit. Where that guard band cannot be met, the result shall be inconclusive or failed as predeclared; it shall not be rounded into a pass. Annex F defines separate service-data rules.

32.4 Nonconformity grading

Critical findings involve unacceptable hazardous conditions, defeat of essential protection, unauthorized hazardous control, intentional evidence falsification or material systematic fraud. Major findings involve missing or ineffective required controls or a material performance failure. Minor findings are isolated limited departures that do not undermine required outcomes. Classification shall be justified and shall not depend on the commercial value of the applicant.

32.5 Decision gate

A positive decision shall require all applicable requirements demonstrated, no open critical or major findings, and closure or an approved time-bound disposition of minor findings that does not conceal an unmet essential requirement. Safety, cybersecurity, measurement and service results shall not be averaged into a compensating score. A limited positive result shall state the exact assessed object and exclusions.

32.6 Assessment status

Permitted draft evaluation statuses are not assessed, under assessment, demonstrated for the stated scope, not demonstrated, suspended and withdrawn. During this working draft phase, a demonstrated result is a pilot assessment record only. Certification and use of any IAF conformity mark require separate adoption and authorization and shall not arise automatically from this document.

32.7 Ongoing assurance

A maintained operational claim shall use the rolling data in Annex F, periodic risk-based surveillance and reassessment after material changes or critical incidents. The surveillance interval shall be set before the claim and reviewed with performance. Product evidence remains version-specific; operational evidence remains period-specific. There is no automatic fixed certificate duration in this draft.

32.8 Transparency and appeals

Public statements shall identify scope, edition, status, assessed configurations, evaluation date, operational data period where applicable and material limitations. Complaints and appeals shall be reviewed by persons independent of the original contested decision. Corrected or withdrawn statements shall be propagated to controlled public channels and recorded in the evidence passport.

Annex A Application and responsibility matrix

Normative within this working draft.

A.1 Application rules

The assessor shall apply the following matrix to the actual offered functions. Core provisions remain applicable according to responsibility for every assessment object. A module marked applicable shall be covered by the complete requirement register, not only the clauses highlighted here. Multiple modules may apply to one configuration.

Module	Mandatory trigger	Principal additional coverage
CORE	Any assessment object	Clauses 1 to 11 and 32 plus relevant lifecycle controls
SITE	Installed charging infrastructure	Clauses 7, 12, 20 to 24 and 25
PUBLIC	Access offered to the general public	Clauses 15, 19, 20, 22, 23 and Annex F
PAYMENT	Commercial charging or energy settlement	Clauses 18 and 19 and transaction tests
CONNECTED	Local or remote digital management	Clauses 14 to 18, 24 and Annex H
GRID	Controlled demand or grid dispatch	Clause 12 and applicable grid permissions
BIDIRECTIONAL	Any intentional vehicle energy export	Clause 27 and direction-specific verification
HIGH POWER	Megawatt claim or elevated current risk	Clauses 10, 12, 28 and thermal verification
HEAVY VEHICLE	Truck bus or industrial road vehicle use	Clauses 20, 21, 28 and handling validation
WIRELESS	Contactless energy transfer	Clause 29 and exposure and object detection tests
AUTOMATED	Mechanized connection or unattended movement	Clauses 29 and 31 where AI is used
DYNAMIC	Energy transfer during road movement	Clause 29.5 and a dedicated extension safety case
MOBILE	Equipment relocated between service uses	Clause 30 and deployment rechecks
STORAGE	Local storage contributes to charging	Clauses 21, 25 and 30
AI	Model-based decisions or control	Clause 31 and function-specific validation

A.2 Responsibility allocation

The organization shall name the lead owner for each interface and require evidence from contributing parties. A responsibility gap shall block completion of the affected requirement.

Evidence area	Typical lead owner	Necessary contributors
Product design and production	EVSE manufacturer	Component and software suppliers
Supply and installation safety	Site owner or integrator	Electrical designer installer and network interface owner
Vehicle interoperability	System integrator	Vehicle interface and platform providers
Cybersecurity and updates	Product and platform owners	Hosting identity and maintenance providers
Price and transaction accuracy	Charging service operator	Meter platform and payment providers
User access and support	Charging service operator	Site owner and accessibility reviewer
Environmental inventory	Responsible scope owner	Equipment energy and waste data providers
Final assessment decision	Independent decision reviewer	Competent assessors and test personnel

A.3 Minimum applicability record

For each numbered clause, the record shall contain requirement identifier, assessment object, module, responsible owner, applicability decision, rationale, evidence links, verification method, result, finding severity and reviewer. The organization shall explain dependencies outside its control and obtain the necessary interface evidence. Not applicable shall never mean evidence unavailable.

Annex B Engineering limits and deployment parameter schedule

Normative within this working draft.

B.1 Completion and independence

For every assessed configuration, a competent designer shall complete each applicable row with numeric limits, units, tolerances, conditions and technical justification. An independent reviewer shall approve the schedule before the test plan is frozen. Shock, leakage, clearance, fault-time and exposure limits shall account for the actual electrical architecture.

The deployment dossier shall retain the technical basis. No external publication is incorporated into this standard. Missing justified values or non-applicability decisions block the associated conformity result. Limits shall not be selected merely to pass existing equipment.

B.2 Required engineering parameters

ID	Parameter requiring a fixed value or envelope	Required conditions and verification link
B01	Supply and output voltage frequency and polarity	Normal range abnormal supply and export modes; D02 D05
B02	Continuous current power and duty cycle	Per port and shared system over voltage and ambient; D06 D10
B03	Accessible voltage and residual energy limits	Touch points discharge endpoint and release time; D04 D05
B04	Protective bonding and conductor continuity limits	Test current path endpoints and temperature; D01
B05	Residual and earth fault detection characteristics	Applicable waveforms trip levels time and coordination; D02
B06	Insulation resistance dielectric withstand and spacing	Test potential duration preconditioning and acceptance; D03
B07	Insulation monitoring thresholds and response	Startup transfer sensor faults and recovery; D03 D04
B08	Overload and short circuit coordination	Prospective fault levels breaking ratings and clearing times; D05
B09	Contact surface and internal temperature limits	Materials access duration ambient and sensor uncertainty; D06
B10	Cooling flow pressure temperature and leakage limits	Coolant properties failure response and service interval; D07
B11	Connector retention force and endurance	Use cycles wear impact partial insertion and release; D08
B12	Environmental operating and storage ranges	Temperature humidity altitude salt dust water and aging; D09
B13	Emission and immunity limits and criteria	Ports frequency ranges modes and acceptable degradation; D11

ID	Parameter requiring a fixed value or envelope	Required conditions and verification link
B14	Output regulation ripple ramp and power quality	Load supply interface and integration window; D10
B15	Export protection and island transition limits	Connection point settings response and restoration; D23
B16	Meter maximum error and allowed uncertainty	Load temperature waveform direction and interval; D18
B17	Accessible dimensions reach and handling force	Route bay controls cable operation and task method; D19
B18	Wireless exposure and object temperature limits	Frequency location exposure duration and alignment; D25
B19	Automated movement force speed and stop distance	Human approach vehicle movement and sensor failure; D26
B20	Storage operating and emergency limits	Energy SOC temperature isolation and fault propagation; D24
B21	Service electrical and security fallback limits	Offline duration value energy and restart conditions; D16 D21
B22	Energy efficiency and standby targets	Conversion boundary auxiliary loads and weighted profile; D28
B23	Noise light and water constraints	Site boundary operating hours and sensitive receptors; D29
B24	Test measurement uncertainty requirements	Instruments coverage factor and decision guard bands; all measured tests

B.3 Record fields

Each row shall identify configuration, owner, numeric limits and units, conditions, justification, binding constraints, method, uncertainty, acceptance rule, approver and revision. Product design limits, installation settings and observed results shall remain distinct.

B.4 Safety function timing

For each protective function, the schedule shall distinguish detection time, controller processing time, actuation time and time to verified safe state. The complete response shall remain within the approved hazard-based limit under worst-case load and timing uncertainty. A fast software log event alone shall not demonstrate that hazardous energy was removed in time.

B.5 Change control

A changed limit shall trigger impact review of design, previous test results, affected deployed units and claims. Historical results shall retain the limits applicable when tested. Relaxing a limit to resolve a failure is prohibited unless an independent engineering review establishes a valid revised basis and the affected assessment is repeated.

Annex C Minimum hazard and failure scenario register

Normative within this working draft.

C.1 Coverage requirement

The organization shall assess every scenario family below and add configuration-specific hazards. The register shall identify the initiating condition, exposed person or asset, protective barriers, common causes, verification, residual risk and owner. A scenario may be excluded only with an evidenced architectural reason.

ID	Scenario family	Required protective outcome
C01	Protective conductor interrupted or misconnected	Hazard prevented and transfer inhibited or safely stopped
C02	Earth fault or DC leakage affects protection	Coordinated detection without hidden protective defeat
C03	Insulation failure under wet or aged conditions	Hazard detected or contained within approved limits
C04	Switching contact welded or semiconductor shorted	No falsely indicated safe release or uncontrolled output
C05	Trapped charge or reverse energy after shutdown	Accessible release only after verified safe condition
C06	Short circuit overload or wrong supply	Fault interruption and containment within ratings
C07	Hot contact cable damage or partial insertion	Unsafe transfer prevented and defect made visible
C08	Cooling loss leak freezing or detached sensor	Controlled derating or shutdown before hazard
C09	Flood condensation salt or environmental aging	Continued protection or controlled removal from service
C10	Radio disturbance surge or control power loss	No unsafe output and controlled recovery
C11	Invalid vehicle request or incompatible adapter	Rejected unsafe negotiation and bounded output
C12	Duplicate stale or contradictory session messages	No unaccounted energy or duplicate settlement
C13	Network cloud payment or identity outage	Bounded offline operation or truthful unavailability
C14	Unauthorized privileged access or replayed command	Rejected control and attributable security evidence
C15	Compromised signing key or interrupted update	Trusted recovery and no unsafe software execution

ID	Scenario family	Required protective outcome
C16	Meter drift tamper clock error or data loss	Error detected and disputed billing contained
C17	User cannot reach connect pay stop or obtain help	Accessible independent task completion or approved assistance
C18	Collision drive-away trapped cable or blocked route	Mechanical and site risk reduced to approved level
C19	Vehicle fire adjacent fire or storage incident	Isolation information response access and containment plan
C20	Export islanding conflicting dispatch or low SOC	Grid protection and user reserve maintained
C21	Wireless foreign object or living-object intrusion	Energy exposure and heating remain controlled
C22	Robot loses position or vehicle moves unexpectedly	Verified safe stop and protected recovery
C23	Mobile unit moves tips or has transport damage	Safe deployment checks and no hazardous transfer
C24	AI drift spoofed data or unfair scheduling	Bounded control fallback and accountable review
C25	Supplier failure orphaned platform or unsupported device	Controlled migration continued protection or retirement
C26	Misstated energy carbon uptime or compatibility claim	Traceable evidence correction and affected claim withdrawal

C.2 Combined and common cause events

The review shall include credible combinations, such as cooling loss during extreme heat, power restoration during a platform outage, a compromised management account during fleet dispatch, and flood damage followed by attempted restart. The organization shall justify the combinations selected; individual single-fault results shall not automatically establish protection against common-cause events.

C.3 Risk closure

For each intolerable risk, the register shall identify the implemented control and successful verification before closure. Warnings, insurance or contractual liability transfers shall not be accepted as substitutes for necessary technical protection. Residual risk approval shall identify the responsible engineering authority and operating restrictions.

Annex D Verification catalogue and test records

Normative within this working draft.

D.1 General test controls

The catalogue defines required verification intent and minimum scenario coverage. Before execution, each test shall be expanded into a controlled laboratory or site procedure using the approved Annex B values, specimen configuration, sequence, instruments, uncertainty and stop criteria. These summaries are not instructions for unqualified persons to conduct energized fault testing. Hazardous tests shall be performed by competent authorized personnel in a controlled facility.

The baseline is one representative specimen per justified design family for each applicable type test, increased where variation or failure mechanisms require it. Every installed port shall receive commissioning checks. Sample count, prior conditioning and representativeness shall be approved before testing. A single specimen does not establish population reliability. Destructive-test specimens shall not return to service without a separately justified release process.

D01 Protective continuity

Identify all required protective paths and accessible conductive parts. Measure continuity using the approved method before and after relevant mechanical and environmental conditioning. Include connection disturbance and the safety case for loss of the path. Pass requires every applicable measurement and response to meet B04 with uncertainty treatment. Retain path diagrams, readings, specimen condition and protective response records.

D02 Earth fault and abnormal supply protection

Apply the approved controlled fault and supply scenarios representing the architecture, including relevant AC and DC components and upstream interaction. Observe detection, interruption and reset. Pass requires the B01 and B05 thresholds and timing to be met without another uncontrolled hazard. Retain waveforms and physical output measurements, not only controller logs.

D03 Insulation and monitoring

Verify the specified insulation and withstand properties at declared conditioning states. Where monitoring is fitted, simulate loss of insulation and monitor failure at startup and during transfer. Pass requires B06 and B07 performance and a safe response to missing monitoring. Record methods, applied conditions, leakage or resistance readings and fault response.

D04 Interlocks and accessible release

Exercise partial connection, broken interlock, stale position signal, commanded stop and release request. Observe output energization and the actual accessible electrical state. Pass requires no hazardous transfer without valid protective conditions and release only within B03 and B07. Retain timing traces, connector state and measured residual energy or voltage.

D05 Switching faults and stored energy

Use the approved fault simulation to represent welded contacts, failed switches, backfeed and loss of control power. Verify isolation indication and trapped-energy management. Pass requires B03 and B08, no uncontrolled restart and safe handling of every included energy source. Retain circuit configuration, measured energy decay and containment observations.

D06 Thermal envelope and derating

Operate at the electrical and ambient points selected by analysis, including maximum current at relevant output voltages and simultaneous loading. Continue until the predeclared stabilization criterion or rated duty endpoint. Induce relevant sensor faults. Pass requires B02 and B09 without unadvertised unsafe overload. Record temperatures, ambient conditions, power curve and derating events.

D07 Cooling fault response

Verify normal cooling and controlled loss of flow, leak indication, blocked path and relevant coolant temperature extremes. Pass requires response within B10 and continued compliance with thermal limits. Record flow, pressure, temperature, shutdown timing and post-test integrity. Where direct fault testing is unsafe, the approved equivalent method shall justify coverage.

D08 Coupler cable and mechanical durability

Apply the approved connection cycles, handling, retention and mechanical conditioning, including relevant wear and contamination. Repeat continuity, insulation and loaded thermal checks affected by the conditioning. Pass requires B11 and no degraded protective function. Record cycle count, force, damage observations, contact condition and follow-up measurements.

D09 Environmental durability

Condition specimens to the declared temperature, moisture, ingress, corrosion, vibration and aging profiles in the justified sequence. Verify operation and relevant safety after conditioning. Pass requires B12 and associated safety limits. Record chamber conditions, duration, specimen state, observed ingress and post-conditioning results. Test coverage shall state what field-life conclusions are justified.

D10 Power quality and shared capacity

Measure output and supply behavior at minimum stable, 10, 25, 50, 75 and 100 percent of declared continuous power where those points are achievable. For other envelopes, justify substitute points before testing. Repeat relevant points under simultaneous load and supply extremes. Pass requires B02 and B14 and truthful shared capacity disclosure. Record load allocation and regulation traces.

D11 Electromagnetic behavior

Test emissions and immunity at relevant interfaces and representative operating modes, including bidirectional and wireless functions if claimed. Monitor protection, session state and meter integrity during disturbances. Pass requires B13 and no unsafe energization or material data corruption. Record modes, performance criteria, disturbance levels and recovery evidence.

D12 Vehicle and backend interoperability

Execute the Annex E matrix across independent implementations and declared profiles. Include initiation, stable transfer, stop, limits and error recovery. Pass requires every mandatory interoperability scenario to succeed within its acceptance criteria; unexplained failures remain findings. Retain vehicle or simulator identity, platform versions, full transaction traces and observed user outcome.

D13 Message robustness and state recovery

Introduce duplicate, delayed, out-of-order, malformed and missing messages within the authorized test environment. Verify safe bounded control and deterministic reconciliation. Pass requires no unsafe state, phantom session, duplicate capture or loss of confirmed energy records. Record injected conditions and matching device, platform and transaction outcomes.

D14 Cybersecurity controls

Test privileged access, segmentation, authentication, API authorization, exposed interfaces, command replay and secret handling against the approved threat model. Pass requires blocked unauthorized control and closure of critical and major findings. Record scope, tester independence, evidence and retests; protect exploit detail from unnecessary public disclosure.

D15 Update and trust recovery

Test valid update, invalid signature, incorrect target, interrupted installation, expired trust and approved rollback. Include signing-key replacement recovery in a representative environment. Pass requires a trusted operational state or safe unavailability, with no unauthorized execution or hazardous output. Record package identities, verification decisions and resulting configuration.

D16 Offline and platform outage

Remove communications, identity and platform services in representative session states. Exercise the declared offline limits and reconnection. Pass requires B21, maintained protection and complete reconciliation without duplicate billing. Record elapsed outage, locally accepted transactions, stored records, public status and recovery outcome.

D17 Payment and user journey

Run every advertised payment route through price acceptance, authorization, charging, stop, receipt and refund. Include timeout, declined payment and repeated user actions. Pass requires correct disclosures and no duplicate or unjustified capture. Record displayed tariffs, accepted terms, masked transaction evidence and user-visible outcomes.

D18 Metering and settlement accuracy

Compare the installed or representative billing meter with a traceable reference across the approved load, temperature and directional points. Check session totals, clock handling and invoice arithmetic. Pass requires B16 with the declared uncertainty rule and exact application of the accepted tariff within stated rounding rules. Retain raw readings, calculations, meter identity and seals.

D19 Accessibility task verification

Measure the site and operating elements against B17 and observe representative users completing approach, connect, authorize, start, stop, release and obtain assistance. Include sunlight, weather or noise where material. Pass requires all mandatory task criteria and deployment obligations met. Record measurements, anonymized task outcomes and unresolved barriers.

D20 Commissioning and status propagation

Verify every port with the installed supply, platform and advertised service route. Change availability and fault states and observe publication channels. Pass requires Annex K checks, accurate port identities and the Annex F status delay limit. Retain as-built settings, session records and timestamped observations.

D21 Continuity and restoration

Exercise a representative outage, restore required records and configuration, and verify normal safe operation. Pass requires the declared recovery objectives, B21 and no unexplained transaction loss. Record recovery timing, backup version, restored configuration and post-recovery checks. Restoration speed shall not compensate for unsafe state.

D22 Operational performance observation

Collect service and session data over the Annex F observation period. Reconcile device logs, user attempts, support records and independent checks. Pass requires the applicable thresholds, complete data accounting and transparent exclusions. Record denominators, missing data, uncertainty, cause groups and underperforming ports.

D23 Bidirectional operation

Test each claimed import, export and island mode, including transitions, grid loss, consent withdrawal, SOC reserve and conflicting dispatch. Pass requires B15, separate metering and maintained user limits. Retain grid interface approval, power traces, user settings and direction-specific settlement. Unsupported modes shall remain disabled.

D24 Storage and mobile systems

Verify storage limits, isolation, depleted-energy behavior and charger output duration; for mobile units repeat relevant checks after movement and deployment. Pass requires B20, stable deployment and safe response to faults. Record energy sources, transport state, deployment checks and actual sustained output.

D25 Wireless transfer

Test the declared alignment and gap envelope, object detection, exposure, heating and abnormal conditions using approved representative methods. Pass requires B18 and protective interruption before a hazardous condition develops. Record object set, detection coverage, exposure positions, alignment and output. A missed hazardous test object shall be a critical finding.

D26 Automated connection and movement

Exercise docking, coupling, release, unexpected approach, position-sensor loss, obstacle intrusion and attempted vehicle movement. Pass requires B19, controlled isolation and safe recovery without unprotected access. Record force, speed, stop distance, detection conditions and interlocks. Limit claims to the tested automation environment.

D27 AI and digital model validation

Validate the declared function using held-out representative and challenging conditions, including missing, shifted and manipulated data. Verify independent control bounds and fallback. Pass requires predeclared performance and intervention thresholds with no breach of essential constraints. Record dataset provenance, model identity, limitations and rollback demonstration.

D28 Energy and environmental data

Measure energy efficiency and standby behavior at the B22 load profile, including auxiliaries and integration boundary. Verify the environmental inventory back to source data and reconcile energy flows. Pass requires metering consistency, predeclared targets and no double counting. Record raw energy, factors, assumptions and uncertainty.

D29 Site and local environmental inspection

Inspect civil works, traffic, drainage, emergency access, lighting, noise and water controls under relevant conditions. Pass requires the approved site criteria and B23. Record measurements, photographs where appropriate, actual bay layout and corrective actions. A site drawing shall not replace observation of the completed works.

D30 Change and recall traceability

Select a representative critical component defect or software vulnerability and trace affected units, owners and configurations. Demonstrate containment, notification preparation and reassessment identification. Pass requires complete identification within the predeclared response target and no untracked units in the sampled population. Record the exercise population and unresolved traceability gaps.

D.2 Mandatory result fields

Each test report shall include test identifier, requirement links, scope, specimen and serial number, hardware and software versions, B-schedule revision, procedure revision, personnel, location, dates, conditions, sample count, instruments, raw evidence, uncertainty, deviations, result, findings and independent review. Pass, fail, inconclusive and not tested shall be used consistently. Test repetition shall preserve the original failed result and the reason for retesting.

Annex E Interoperability coverage and acceptance

Normative within this working draft.

E.1 Coverage dimensions

The matrix shall cover physical interface, vehicle implementation, charger hardware, firmware, local controller, management platform, authentication route, payment route, operating mode and environmental boundary. Exact versions shall be retained in the implementation register. Vendor diversity shall be based on independent implementations, not merely different badges using the same underlying stack.

E.2 Minimum test population

For a product interoperability claim, each declared vehicle interface profile shall be tested against at least three independently implemented vehicle interfaces where available. Each declared management interface profile shall be tested against at least two independent backend implementations where available. At least one real representative vehicle shall be included for each claimed vehicle class and physical coupler configuration; justified shared evidence may support equivalent variants.

Where the market does not provide this diversity, all available independent implementations plus a validated boundary-condition simulator shall be tested. The result shall be explicitly limited to the tested ecosystem; it shall not qualify for an unrestricted broad compatibility claim. These counts are proposed draft coverage minima and do not establish compatibility with every vehicle.

E.3 Required scenarios

Scenario group	Required variations	Acceptance outcome
Normal initiation	Every declared authentication and payment route	Correct price authorization negotiation and energy start
Electrical negotiation	Lower upper and reduced capability boundaries	No output beyond the lowest applicable limit
Simultaneous service	Shared cabinet and site resources	Allocation respects supply and advertised commitments
Pause and resume	Vehicle site user and dispatch initiated	Preserved session and price with safe transitions
Stop and release	User vehicle emergency and fault	Safe shutdown correct settlement and release
Offline and recovery	Loss before and during transfer	Bounded fallback and no duplicate transaction
Identity lifecycle	Expired revoked unknown and renewed credentials	Correct acceptance or rejection without unsafe bypass
Data faults	Duplicates delays malformed and reordered messages	Deterministic state and intact meter records

Scenario group	Required variations	Acceptance outcome
Version change	Current and declared supported combinations	Controlled negotiation and documented limitations
Bidirectional	Each claimed mode and consent transition	Protected import export and settlement

E.4 Repeatability

Each normal initiation route in each required implementation pairing shall complete at least ten consecutive controlled sessions without unexplained failure after the configuration is frozen. Required fault scenarios shall pass individually. A failure shall be investigated, corrected and followed by the affected regression set; failed attempts shall remain in the report. Ten sessions is a repeatability screen, not a statistical reliability guarantee.

E.5 Acceptance and limitations

Acceptance requires every mandatory scenario for the claim to pass, all essential safety outcomes to remain satisfied and no unresolved material interface ambiguity. Field success metrics in Annex F are additional evidence. Simulators shall have validation records, and their limitations shall be explicit. Results shall state the tested matrix rather than merely use a generic interoperable label.

Annex F Operational metrics and proposed pilot thresholds

Normative within this working draft.

F.1 Status of numeric targets

The numeric targets below are proposed IAF draft policy choices for pilot validation. They are not asserted to be universally established industry limits or requirements of any jurisdiction. They become acceptance criteria only for a declared pilot assessment under this draft. Before first edition adoption, feasibility, measurement consistency and user outcomes shall be reviewed under Annex L.

Public operational service claims shall use the baseline targets below. Private and dedicated fleet service profiles shall retain the same metric definitions and disclose contractual targets fixed before measurement; they shall not claim the public baseline unless they meet it. Essential safety, billing integrity and truthful reporting apply to every profile.

F.2 Availability definitions

Scheduled service minutes are the minutes in the assessment period during which the port was advertised or contracted to provide service. The schedule shall be fixed before the period; it shall not be shortened retrospectively. All-cause unavailable minutes are the union of scheduled minutes during which the port could not provide its declared essential service. Overlapping causes shall count once.

Unavailability includes equipment faults, planned maintenance during scheduled hours, external supply failure, required platform or payment failure, unsafe condition, inaccessible required operating features and unknown capability due to missing evidence. Occupancy by a valid charging session is not a fault. A port in use shall count as service-capable only while the session and protective evidence support that status. A separate occupied or blocked status shall remain visible to arriving users.

To calculate all-cause availability, first subtract unavailable minutes from scheduled service minutes, then divide the result by scheduled service minutes and multiply by 100. A zero scheduled-time denominator shall be reported as not applicable, never as 100 percent availability. Port values shall be reported individually. A site-level measure of at least one capable port may supplement but shall not replace the individual-port result. Adjusted availability excluding identified external causes may be reported only alongside the all-cause value, with every exclusion quantified.

F.3 Attempt and success definitions

A user attempt begins at an identifiable physical connection or explicit request to start at a port, whichever first establishes charging intent. Automatic retries and repeated commands within five minutes of that unresolved intent shall remain part of the same first-attempt record. Attempt reconstruction shall use privacy-preserving identifiers and shall not require unnecessary persistent vehicle tracking.

An eligible attempt concerns an advertised supported vehicle and service, valid user authorization or an advertised ad hoc route, and a user intending to charge. Exclusion requires positive evidence of an unsupported vehicle outside the advertised claim, deliberate user cancellation before commitment, or a non-service test event. Platform errors, failed advertised payment, unexplained vehicle errors and missing evidence shall not be excluded as user fault. Both all-attempt and eligible-attempt counts shall be disclosed.

First-attempt success requires transfer to begin within 120 seconds after the later of confirmed physical connection and completed required user authorization, then continue for at least two minutes or reach an earlier verified user-requested completion. A protection trip, unexplained interruption, forced reconnect or

manual retry fails this metric. An infrastructure or advertised payment failure that prevents authorization shall remain an eligible failed attempt; the requirement for valid authorization shall not be used to exclude it. User interaction time before authorization shall be reported separately and shall not conceal inaccessible payment or initiation workflows.

F.4 Threshold schedule

Metric	Proposed public baseline	Reporting and decision rule
All-cause port availability	At least 99.0 percent	Each port over rolling 30 days; no network averaging for pass
First-attempt success	At least 98.0 percent	Eligible attempts over rolling 30 days plus all-attempt rate
Observation sufficiency	At least 30 consecutive days and 200 eligible attempts per site	Below either threshold service success result remains provisional
Data completeness	At least 99.5 percent of expected minute records	Missing capability counted unavailable; raw gap count disclosed
Initiation latency	95th percentile no more than 120 seconds	Report complete eligible initiation population and failures
Status propagation	95th percentile no more than 60 seconds	Physical state to controlled public channels; failures disclosed
Material billing errors	Zero unresolved confirmed cases	Any case requires correction and affected-population review
Safety-critical protective failures	Zero unresolved cases	Immediate block regardless of service percentage
Active critical cyber exposure	Zero unmitigated cases	Block affected scope until verified containment or correction
Complaint acknowledgment	Within 2 business days	At least 95 percent; emergencies handled immediately
Public assistance coverage	All advertised operating hours	Channel verified at commissioning and exercised periodically
Efficiency and standby performance	Meet predeclared B22 targets	Report full tested load profile and auxiliary boundary

F.5 Statistics and disaggregation

Reports shall show raw counts, denominators, exclusions and the observation window. For success proportions, a two-sided 95 percent Wilson confidence interval shall accompany the point estimate. The draft acceptance threshold applies to the observed proportion, not the lower confidence bound; a report shall not describe it as a 95 percent guarantee. The calculation method and rounding shall be reproducible. Time sources used across systems shall be synchronized or have measured offsets. The timing uncertainty and offset correction shall be recorded; a latency result shall not pass where unresolved timing uncertainty crosses its applicable limit.

For percentile metrics, sort the complete observation set and use the nearest-rank value at the ceiling of 0.95 multiplied by the sample count. A start that never reaches energy transfer, or a required status update that never reaches the publication channel, shall be retained as an unbounded delay, ranked after every finite delay. If the selected rank is unbounded, the percentile target is not met. Missing timestamps shall not produce a zero or successful latency value. Unsuccessful starts shall also remain in the success denominator. Results shall be disaggregated by port, interface, payment route and material software version where counts permit. Site-level success acceptance requires no unresolved material defect concentrated in a subgroup even when the aggregate passes.

F.6 Worked availability check

For an always-open port over 30 days, scheduled time is 43,200 minutes. If the union of fault, maintenance, supply-outage and unknown minutes is 360 minutes, availability is 99.1667 percent and meets the proposed 99.0 percent target. A second port at 98.8 percent fails its own target even if the network average exceeds 99.0 percent. This arithmetic example does not establish actual field performance.

F.7 Change during observation

A material configuration change shall be identified in the data and assessed for resetting the observation period. Data from substantially different configurations shall not be combined to conceal a regression. A new or low-utilization site may have completed commissioning while its operational success result remains provisional; those statuses shall be stated separately.

Annex G Digital evidence passport

Normative within this working draft.

G.1 Purpose and identity

Each assessment object shall have a durable evidence passport linking its scope, configuration, tests, operational period and current status. The passport may use a database or a structured file. A public summary shall be separated from restricted technical and personal records. A QR code may provide access to a summary but shall not itself constitute proof of authenticity.

G.2 Minimum record schema

Field	Required content	Visibility
passport_id	Unique persistent identifier with issuing namespace	Public summary
object_type	Product site platform or operational service	Public summary
responsible_entity	Accountable legal entity and contact route	Public summary
document_identity	IAF ECias edition and draft revision	Public summary
assessment_status	Controlled status and reason for limitations	Public summary
scope	Modules application boundaries and exclusions	Public summary
location_scope	Site or geographical deployment as appropriate	Public or restricted by risk
asset_identity	Product model serial port and site relationships	Split public and restricted
hardware_version	Assessed hardware and critical component revision	Restricted with public summary
software_identity	Firmware platform versions and integrity values	Restricted with public version summary
interface_profiles	Exact supported profiles and tested combinations	Public compatibility summary
operating_envelope	Validated ranges and material derating conditions	Public summary
limits_revision	Approved Annex B record and reviewer	Restricted
requirement_register	Applicability owner evidence and result per clause	Restricted

Field	Required content	Visibility
test_evidence	Test identifiers reports raw evidence and integrity values	Restricted
assessment_date	Date and decision record identifier	Public summary
operational_period	Measurement start end and data sufficiency status	Public summary
performance_metrics	Values denominators exclusions and confidence	Public summary
environmental_boundary	Method period energy boundary and assumptions	Public summary
support_status	Support end date contact and migration limitations	Public summary
findings	Severity status actions and verification	Restricted with material public limitations
change_history	Changes responsible approver and affected claims	Restricted with public status history
review_identity	Assessor and independent decision reviewer	As authorized for the assessment
integrity_proof	Signing or equivalent tamper-evident verification	Public verification metadata
next_review_event	Planned surveillance or condition requiring review	Public summary

G.3 Data conventions

Times shall use UTC with explicit timezone and sufficient precision; local display times may supplement them. Energy shall state kWh, power kW, current A, voltage V and temperature degrees Celsius unless another unit is explicitly identified and convertible. Missing values shall have a reason code and shall not be replaced by zero. Identifiers shall remain stable through ownership and platform changes.

G.4 Authenticity and history

Passport changes shall preserve prior versions and the reason for change. Integrity protection shall detect unauthorized alteration and support verification after platform migration. Revoked or superseded status shall remain discoverable. Public summaries shall not expose private keys, exploitable network detail, personal journeys or payment credentials.

G.5 Evidence retrieval

The organization shall demonstrate retrieval of a selected public claim to its requirement, configuration, raw evidence and decision. Links shall remain usable over the declared retention period. A broken link to essential evidence shall be treated as an evidence availability finding until restored.

Annex H Cybersecurity treatment and incident schedule

Normative within this working draft.

H.1 Severity and immediate protection

Severity shall consider exploitability, exposure, affected population, data and safety consequences. Remotely exploitable hazardous control is critical without observed exploitation. Immediate safety risk shall trigger isolation without waiting for the deadlines below.

H.2 Proposed response targets

These internal draft targets require pilot validation. Shorter binding deadlines take precedence. Clock hours start on receipt of credible evidence and shall not pause during internal assignment.

Condition	Initial triage	Required treatment
Active exploitation or credible imminent critical harm	Within 4 hours	Immediate protective action; verified containment target within 24 hours
Critical vulnerability without observed exploitation	Within 24 hours	Affected release blocked; mitigation target within 7 days
Major security weakness	Within 72 hours	Treatment plan within 7 days; mitigation target within 14 days
Other confirmed weakness	Within 7 days	Risk-based owner and due date agreed within 14 days
Suspected signing key compromise	Immediate escalation	Stop affected signing and deployment; revoke or replace trust under controlled recovery

H.3 Closure requirements

Containment shall be verified and distinguished from permanent correction. Critical and major findings shall have dated remediation plans, normally targeting correction within 30 days of validation. Where a safe fix needs longer, independent review shall approve continued effective containment or require the function to remain unavailable. Unmitigated critical exposure shall block a positive decision.

H.4 Vulnerability handling

A discoverable channel shall acknowledge vulnerability reports, protect reporter information and coordinate responsible disclosure. Affected versions and customers shall be identified without publicly exposing exploit instructions. Updates shall follow Clause 17; retests shall address the original weakness and regressions.

H.5 Incident records

The record shall contain discovery time, validation time, severity rationale, affected assets, containment, communications, evidence preservation, remediation, verification and lessons. Regulatory and contractual notification clocks shall be tracked separately. An incident may be operationally recovered while its investigation remains open; those statuses shall not be conflated.

Annex I Environmental calculation example

Informative.

I.1 Illustrative boundary

This example demonstrates transparent accounting for one stationary DC charging site over an assumed reporting period. All numbers are hypothetical and are not IAF performance targets. Grid import is 100,000 kWh, vehicle delivery is 90,000 kWh, charger conversion and cable loss is 6,000 kWh, and site auxiliaries consume 4,000 kWh. There is no local generation, storage or export in this example.

I.2 Energy reconciliation

The balance closes because delivered energy plus conversion and cable loss plus auxiliaries equals imported energy. The site delivery ratio is 90.0 percent, calculated as vehicle delivery divided by grid import. The charging-path efficiency excluding separately measured site auxiliaries is 93.75 percent, calculated as 90,000 divided by 96,000. Reporting only the second number would conceal part of the site energy consumption unless the boundary is clearly stated.

I.3 Operational carbon illustration

Assume a hypothetical location-based electricity factor of 0.400 kg carbon dioxide equivalent per kWh. Operational electricity emissions are 40,000 kg carbon dioxide equivalent. Allocating those emissions to 90,000 kWh delivered produces approximately 0.444 kg carbon dioxide equivalent per delivered kWh. This is not a full life cycle value and makes no claim about vehicle use emissions or avoided emissions.

I.4 Life cycle extension

A complete life cycle model would add allocated equipment manufacture, civil works, transport, maintenance, replacements and end-of-life impacts over a declared life and utilization. If verified embodied impacts were hypothetically 120,000 kg carbon dioxide equivalent and expected lifetime delivered energy were 3,000,000 kWh, the embodied allocation would be 0.040 kg per delivered kWh. Utilization and lifetime assumptions would need sensitivity analysis before a combined claim.

I.5 Storage and renewable cases

For a storage site, charging input, storage loss, storage output and direct supply require separate reconciliation. Renewable generation used on site and energy exported require distinct quantities and allocation rules. Contractual renewable attributes should be reported separately from physical energy flows. The same exported unit or environmental attribute should not support multiple incompatible claims.

I.6 Uncertainty and improvement

The example should be expanded with meter uncertainty, factor uncertainty, missing data and sensitivity to utilization. Potential improvements include reduced standby power, repairable modules, thermal management improvements and better scheduling, provided they do not undermine safety or user commitments. A before-and-after claim needs comparable boundaries and operating conditions.

Annex J Assessment decision and corrective action forms

Normative within this working draft.

J.1 Scope declaration form

The completed declaration shall record responsible entity, contact, object type, site or family identity, modules, hardware, software, interfaces, operating envelope, geography, exclusions, deployment approvals, Annex B revision and authorized signatory. It shall identify whether the result concerns design, installation, digital platform or operational performance.

J.2 Requirement record form

Each requirement record shall contain clause identifier, complete requirement interpretation, owner, applicable or not applicable status, rationale, linked evidence, verification method, result, reviewer and date. A passed result shall be supported by actual evidence. An entry reading to be supplied shall remain not demonstrated.

J.3 Finding and corrective action form

The form shall record finding identifier, affected clause and configuration, objective evidence, severity, immediate containment, root cause, affected population, corrective action, responsible person, deadline and effectiveness verification. Correction of one device shall not close a systemic defect without review of the remaining population. Reopened findings shall retain their history.

J.4 Decision record

The decision reviewer shall record scope completeness, critical and major findings, minor dispositions, evidence sufficiency, engineering limit approval, operational data sufficiency and conflicts of interest. The decision shall state one controlled status with the reasons and limitations. Partial or provisional operational evidence shall not be described as complete operational conformity.

J.5 Suggested pilot statement

The following wording may be used only when supported by the recorded decision: Assessed in a pilot evaluation against IAF ECIAS First Edition Working Draft 0.2 for the stated scope and configurations. Requirements demonstrated are identified in the accompanying evidence record. This is a working draft assessment and does not constitute an adopted-standard certificate or authorization to use a conformity mark.

J.6 Suspension and appeal record

Suspension or withdrawal shall identify the trigger, affected scope, public correction, containment and conditions for restoration. Appeals shall record the disputed decision, independent reviewer, evidence considered and outcome. An appeal shall not postpone necessary safety containment or correction of a materially misleading claim.

Annex K Commissioning and operational inspection checklist

Normative within this working draft.

K.1 Commissioning checklist

The installer and accountable owner shall record pass, fail or justified not applicable for every check below. The result shall link to actual records and the installed configuration. No unchecked critical item shall be accepted as complete.

Check	Required evidence	Release consequence if missing
Scope and approvals	Approved configuration and required permissions	Block service opening
Supply and protection	As-built diagram settings and coordination	Block energization for service
Bonding and insulation	Port-specific inspection and test results	Block affected port
Isolation and emergency action	Verified source identification and response	Block affected scope
Cable connector and enclosure	Condition rating retention and integrity	Block unsafe equipment
Cooling and thermal behavior	Correct fluid flow sensing and limits	Block affected high-load operation
Meter and tariff	Verified identity accuracy and displayed prices	Block commercial billing
Platform and software	Approved versions trust and secure access	Block untrusted control
Session and payment	End-to-end successful route at every port	Block unverified advertised route
Simultaneous load	Supply limits and shared capacity demonstrated	Limit service to verified capacity
Access and assistance	Physical task checks and working support	Block unsupported public access claim
Public data	Correct location port state power and hours	Correct before opening
Handover and training	Maintenance emergency contacts and competence	Block acceptance

K.2 Routine operational inspection

At the risk-based interval, the organization shall inspect damage, overheating signs, cable condition, connector wear, water entry, seals, cooling, labels, access routes, emergency controls and assistance channels. Records shall show date, inspector, findings and action. Cleaning or a remote heartbeat check shall not substitute for required physical inspection.

K.3 Event driven inspection

Additional inspection shall follow flood, impact, fire exposure, suspected tampering, repeated protection trips, major repair, relocation and relevant software or setting change. The inspection scope shall follow the affected hazards. Until safety is established, the equipment shall remain unavailable.

K.4 Return to service record

Return to service shall identify the corrected defect, replaced parts, restored configuration, repeated tests, public status update and approving person. For critical findings, the independent review required by Clause 32 shall be complete. The original outage and defect shall remain in performance reporting.

Annex L First edition development and technology roadmap

Informative.

L.1 Development status

This working draft supplies a full proposed clause structure, requirement language, evidence architecture, test catalogue and assessment forms. It remains a development instrument. Technical consensus, validation of draft service targets, detailed laboratory procedures and authorization of a conformity scheme have not been completed or claimed.

L.2 Release blockers

Decision area	Work required before edition adoption	Required output
Technical scope	Review boundaries and module triggers with competent specialists	Approved scope and resolved comments
Electrical limits	Validate the B-schedule process for diverse electrical architectures	Reviewed deployment parameter templates
Verification methods	Expand catalogue into reproducible laboratory procedures	Controlled procedures and uncertainty budgets
Interoperability	Validate diversity and repeatability coverage in practice	Pilot matrix results and revised coverage rules
Service targets	Test 99.0 percent availability and 98.0 percent initiation choices	Feasibility analysis with transparent failure populations
Accessibility	Validate task methods and region-specific parameter schedules	Reviewed methods and representative user results
Cybersecurity	Exercise treatment deadlines and trust recovery	Evidence of feasible safe remediation processes
Sustainability	Validate boundaries factors and auditability	Reproducible examples and data quality criteria
Decision governance	Approve competence impartiality surveillance and appeals rules	Adopted assessment scheme documentation
Publication	Complete editorial technical and public-comment closure	Authorized first edition and version history

L.3 Proposed pilot coverage

A useful pilot should include AC destination charging, public DC charging, a heavy vehicle depot, a storage-assisted or constrained-grid site, and a bidirectional installation where lawful and available. It should cover hot, cold and wet operating conditions, varied payment routes and different technology providers. Initial observation should extend beyond the minimum measurement window where needed to assess seasonal and low-utilization effects.

L.4 Review method

Each pilot should retain raw data, deviations, implementation burden, unresolved hazards and user outcomes. Review should compare results across configurations without erasing poor-performing groups. Proposed thresholds should be revised only through documented evidence and technical review, with a new version and clear transition rules. A target should not be weakened merely to accommodate a particular applicant.

L.5 Technology scenarios

Over the next development cycles, plausible priorities include larger commercial-vehicle energy demand, more bidirectional service, automated docking, wireless transfer, infrastructure-supported energy exchange, software-defined power systems and evolving cryptographic requirements. These are planning scenarios, not predictions that every technology will become widespread or succeed commercially.

L.6 Proposed contribution of the standard

The intended contribution is a single traceable assessment structure linking device protection, installed infrastructure, digital trust, real charging outcomes, accessible use and environmental evidence. Its value should be judged by reproducible verification and improved field outcomes. No claim of global acceptance, exclusive originality, market leadership or superiority over all existing approaches is made by this draft.

L.7 Next working revision

The next revision should complete specialist review of the safety schedule, select pilot configurations, issue the requirement register and detailed test procedures, collect field results and resolve technical comments. Each revision should preserve stable requirement identifiers where possible and explain every substantive change. Publication and any conformity mark authorization should occur only through an explicit approval decision.