PUBLIC | JULY 2026 | VERSION 1.0

Securing Bidirectional Energy

Cybersecurity Architecture for V2G and V2X Systems

A security architecture and operating model for electric vehicles, charging infrastructure, cloud orchestration, artificial intelligence and grid-connected operations.

EXECUTIVE LINKEDIN EDITION

Executive abstract

The operating principles for trustworthy bidirectional energy

V2G and V2X connect domains that have traditionally been governed separately: vehicles, public charging, site energy, cloud software, markets and grid operations. A failure in one domain can propagate financial, operational, safety-relevant or grid-level consequences across the others.

Scope and limitation

This paper is a strategic synthesis. It does not replace normative standards, system-specific risk assessments or jurisdiction-specific regulatory guidance. Risk scenarios are illustrative; likelihood ratings are not assigned without a defined method and stated assumptions.

14	5	4
EXECUTIVE PAGES	TRUST DOMAINS	CORE PRINCIPLES

01 IDENTITY IS THE ROOT CONTROL

Hardware-backed key protection and governed certificate lifecycles reduce credential theft, impersonation and unauthorised access.

02 THE CONTROL PLANE DETERMINES FLEET-WIDE RISK

Cloud APIs, operator accounts and aggregator interfaces can propagate one compromise across an entire fleet.

03 ZERO TRUST IS AN OPERATING DISCIPLINE

Access is granted per request and context, not by network location or prior session.

04 AI ACTIONS NEED DETERMINISTIC CONSTRAINTS

AI-generated actions must remain inside approved authority boundaries and independently verifiable safety policies.

05 RECOVERY MUST PRESERVE SAFE SERVICE

Contain the smallest practical unit, activate tested local safe modes and restore trust through revalidation.

Sources: ISO 15118-20:2022; NIST SP 800-207; NIST AI RMF 1.0

Why V2G cybersecurity is different

Security must connect digital trust to physical energy behaviour

Conventional IT security protects information within defined organisational boundaries. V2G must also govern physical energy flows, real-time grid interactions, fleet readiness and multi-party settlement across organisations that were not designed to interoperate securely.

ENERGY V2X

- V2G - vehicle to grid
- V2H - vehicle to home
- V2B - vehicle to building
- V2L - vehicle to load

TRANSPORT V2X

- V2V - vehicle to vehicle
- V2I - vehicle to infrastructure
- V2N - vehicle to network
- V2P - vehicle to pedestrian

Cyber-physical consequence rule

A serious event is any digital event that can alter charging, discharging, export permission, fleet readiness, site resilience, power quality, grid stability or settlement evidence.

CONSEQUENCE DOMAINS

Event type	Conf.	Financial	Fleet	Safety	Grid
Control-plane compromise	●	●	●	●	●
Certificate or key theft	●	●	○	○	○
OTA firmware corruption	○	○	●	●	○
Metering manipulation	○	●	○	○	●
Lateral movement to site OT	○	○	●	●	●
AI model or agent compromise	○	●	●	●	●

● potentially affected ○ less directly affected

Severity depends on scale, architecture and mitigating controls.

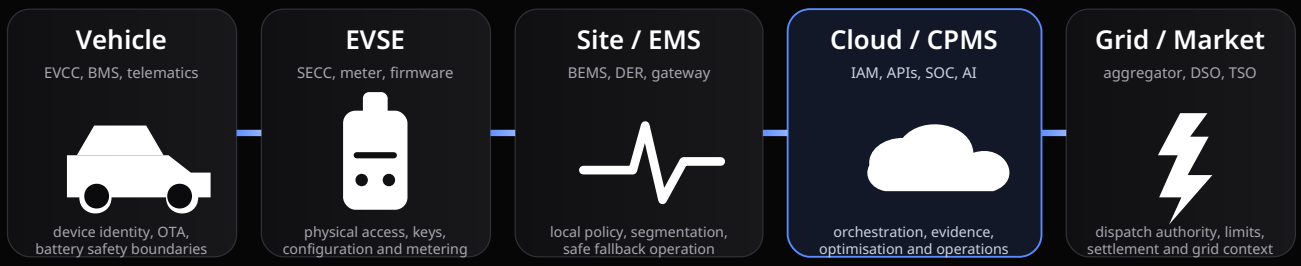
Source basis: Gamma enterprise draft, pp. 3-4; refined for executive readability

End-to-end reference architecture

Separate power, control, identity, telemetry, software and settlement flows

End-to-end V2G security architecture

Five operational domains. Six distinct flows. Multiple trust boundaries.



Six flows to govern

POWER vehicle - EVSE - site - grid

CONTROL cloud - EVSE - EVCC

IDENTITY PKI across every domain

TELEMETRY device - SOC - analytics

SOFTWARE build - sign - deploy - attest

SETTLEMENT meter - aggregator - market

Design rule

Local safety constraints remain authoritative when cloud trust or connectivity degrades.

TRUST BOUNDARIES

EV-EVSE session | EVSE-CPMS | site-cloud | cloud-aggregator | aggregator-utility | maintenance access

CONTROL OBJECTIVE

Authenticate every actor. Authorise every action. Constrain every command. Verify every outcome.

SAFE DEGRADATION

Loss of cloud trust should reduce functionality, not bypass local safety or force uncontrolled shutdown.

Sources: ISO 15118-20:2022; OCPP 2.1; IEC 62443; NIST SP 800-207

Assets, actors and security ownership

Assign accountability before deployment, not after an incident

Actor	Asset / service	Primary security responsibility	Failure consequence
OEM	Vehicle software, BMS, telematics	Secure boot, OTA signing, diagnostics	Fleet-wide update or safety impact
EVSE manufacturer	Charger firmware, SECC, meter	Secure defaults, signed firmware, tamper evidence	Session fraud or lateral movement
CPO / CPMS	Management platform, APIs	IAM, role separation, monitoring	Fleet-wide dispatch manipulation
Fleet / site operator	Fleet, EMS, local network	Segmentation, contractor control, safe modes	Readiness loss or site disruption
Aggregator / utility	Dispatch, market, interconnection	Input validation, limits, authority checks	Grid or market impact
Certificate provider	PKI, trust anchors, revocation	HSM custody, audit, recovery	Systemic identity compromise

Procurement is a security control

- supported lifetime and patch commitment
- coordinated vulnerability disclosure
- hardware key custody and release governance
- operational logging and evidence access
- tested end-of-life and decommissioning process

Named ownership

Every device, certificate type, API, model, software release and incident action needs an accountable owner.

Shared responsibility

No single participant can secure V2G alone. Vehicle, charger, site, platform and grid roles must align on trust and recovery.

01
Name the accountable owner
Every asset, identity, API, model and release.

02
Bind authority to identity
Separate operator, maintenance and workload privileges.

03
Document failure consequence
Fleet, site, market, safety and grid impact.

04
Exercise the handoff
Test escalation, containment and recovery across organisations.

Source basis: Gamma ownership matrix, p. 5; condensed for executive use.

Priority threat scenarios

Design around propagation potential, not only the initial point of entry

01

CLOUD CONTROL-PLANE COMPROMISE

Credential theft or API exploit → persistent CPMS access → malicious fleet dispatch.

CONTROL
MFA, scoped tokens, PAM, rate limits.

02

COORDINATED LOAD MANIPULATION

Compromised CPMS or aggregator → simultaneous charging or export commands.

CONTROL
Command plausibility checks, local limits, staged dispatch.

03

CERTIFICATE OR KEY COMPROMISE

HSM, insider or CA compromise → fraudulent identities or sessions.

CONTROL
Hardware-backed keys, dual control, revocation and audit.

04

MALICIOUS OR FAULTY OTA

Build or signing compromise → unsafe firmware distributed at scale.

CONTROL
Signed artefacts, canary rollout, attestation and rollback.

05

API ABUSE AND BULK OPERATIONS

Overprivileged token → bulk commands, data exfiltration or billing manipulation.

CONTROL
Scoped tokens, bulk-operation controls, replay protection.

06

AI MODEL OR AGENT COMPROMISE

Poisoning or prompt injection → unsafe recommendations or tool actions.

CONTROL
TEVV, policy gates, sandboxing, human approval.

RISK METHOD Likelihood x operational impact x propagation potential. Assign ratings only after system-specific assumptions and threat intelligence are documented.

01
Entry point
API, charger, certificate, update pipeline or model input

02
Initial compromise
credential, firmware, network pivot or unsafe recommendation

03
Propagation
device → site → fleet cohort → grid-connected population

04
Physical consequence
readiness, power, safety, settlement or stability

Source basis: Gamma threat model and priority scenarios, pp. 6-7

Standards and protocol landscape

Use standards as building blocks - not as a substitute for secure engineering

CHARGING AND INTEROPERABILITY

Framework	Domain	Security relevance
ISO 15118-20	EV-EVSE	Bidirectional power-transfer messages and sequence requirements; security depends on broader certificate operations.
IEC 61851	Charging	Physical charging and signalling baseline; not a complete cybersecurity framework.
OCPP 1.6	EVSE-backend	Installed-base reality; security depends on TLS, authentication, implementation and operating controls.
OCPP 2.0.1 / 2.1	EVSE-backend	Stronger security features; 2.1 adds ISO 15118-20, bidirectional charging and DER control.
OCPI	Roaming	Commercial interoperability, API scope, token management and partner governance.
IEC 63110	Infrastructure	Management of charging and discharging infrastructure; distinct from roaming.

VEHICLE, GRID AND GOVERNANCE

Framework	Domain	Security relevance
IEC 62443 / 62351	OT and grid	Zones, conduits and secure power-system communications.
IEEE 1547	DER interconnection	Physical grid limits that cyber controls must not bypass.
ISO/SAE 21434	Automotive	Vehicle cyber engineering and lifecycle governance.
UNECE R155 / R156	Automotive regulation	Cybersecurity and software-update management systems in adopting markets.
NIST SP 800-207	Zero Trust	Per-request authentication, authorisation, posture and policy enforcement.
NIST AI RMF	AI governance	Govern, Map, Measure and Manage AI risks continuously.

IMPLEMENTATION REALITY Protocol compliance alone does not prove a deployment is secure. Configuration, key management, lifecycle governance, monitoring and operational response determine the real outcome.

01
Inventory versions and profiles
Know what is deployed, enabled and optional.

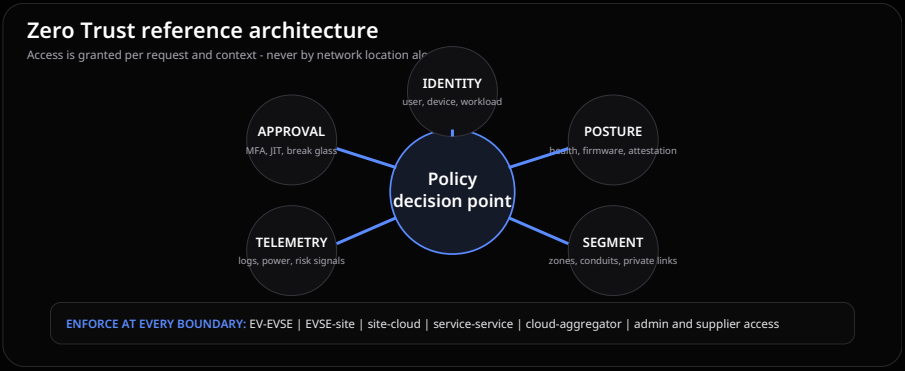
02
Validate implementation
Test certificates, APIs, firmware and failure handling.

03
Operate the controls
Monitor trust stores, tokens, logs and exceptions continuously.

Official sources: ISO, IEC, Open Charge Alliance, IEEE, UNECE and NIST. OCPP 2.1 is IEC 63584-210:2025.

Zero Trust reference architecture

Protect resources and actions - not merely network segments



POLICY DECISION POINT

- evaluates identity, posture, context and risk
- consumes telemetry from every domain
- issues time-limited decisions
- integrates with identity and privileged access

POLICY ENFORCEMENT POINT

- enforces decisions at each trust boundary
- blocks stale or over-broad access
- requires approval for high-consequence actions
- revokes access when posture degrades

01
Authenticate
user, device and workload

02
Assess posture
health, firmware, attestation

03
Evaluate policy
scope, context and risk

04
Enforce
allow, deny or request approval

05
Monitor and revoke
continuous telemetry

IMPLEMENTATION CHECKLIST | unique device and workload identity | mutual TLS | short-lived scoped tokens | just-in-time privilege | break-glass evidence | segmented charging, dispatch, billing and security administration

Official source: NIST SP 800-207, Zero Trust Architecture

Identity, PKI and private connectivity

Automated charging depends on disciplined trust and certificate operations

Identity and certificate trust chain

Separate device, contract, operator, maintenance, workload and settlement identities.

Lifecycle controls

hardware-backed keys | named owner | automated renewal | expiry monitoring | revocation | trust-store updates
CA compromise recovery | immutable audit evidence | signed settlement records

PRIVATE CONNECTIVITY

- private APN, VPN, MPLS or private cellular where justified
- SIM and modem lifecycle governance
- outbound destination allowlists
- route and tunnel monitoring
- secure remote maintenance with MFA and session evidence

PRIVATE DOES NOT MEAN TRUSTED

A private network reduces exposure. It does not replace unique identities, mutual TLS, segmentation, least privilege or continuous monitoring.

HSM | mTLS | JIT ACCESS | REVOCATION | AUDIT EVIDENCE

CERTIFICATE OPERATIONS

inventory | renewal | expiry | revocation | trust-store update | recovery

REMOTE MAINTENANCE

named approval | MFA | JIT access | session logging | rapid revocation

NETWORK CONTROLS

outbound allowlists | SIM governance | tunnel monitoring | segmented routes

Sources: ISO 15118-20; NIST SP 800-207; IEC 62443

Secure software supply chain and OTA

Protect the lifecycle from build system to field recovery

Secure software and OTA lifecycle

A compromised update path can propagate failure across thousands of field assets.

Enterprise target state

SBOM | protected signing keys | secure boot | staged rollout | anti-rollback | device attestation | emergency revocation | supplier patch commitments

SECURE DEVELOPMENT

- SSDLC and code review
- SBOM for every release
- dependency and static analysis
- reproducible builds where practical

RELEASE GOVERNANCE

- protected signing keys in HSM
- dual-control approval
- canary → cohort → fleet
- rollback and emergency revocation

SUPPLIER OBLIGATIONS

- supported lifetime
- patch SLA
- vulnerability disclosure
- running-version evidence
- end-of-life commitments

> A software update path is not a maintenance feature. It is a fleet-wide control surface.

01
Version attested

Know what is running in the field.

02
Rollback tested

Prove recovery before a critical release.

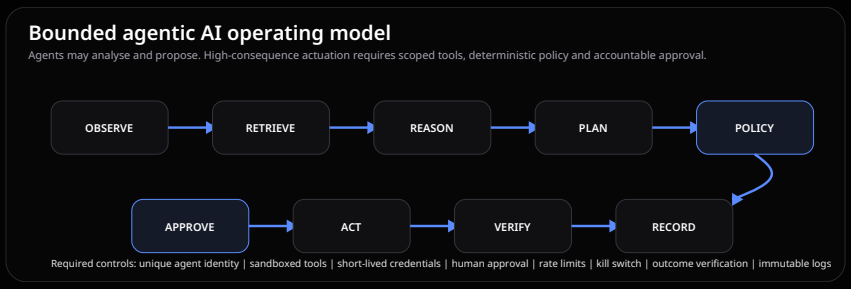
03
Signing authority controlled

Separate build, approval and release duties.

Sources: UNECE R156; ISO/SAE 21434; CISA secure-by-design guidance

Securing AI and agentic AI

Use AI for insight and bounded automation - never unconstrained authority



Use class	Examples	Operating rule
Decision support	Forecasting, anomaly detection, simulation, evidence correlation	Permitted with validation and monitoring
Policy-bounded automation	Scheduling or dispatch inside pre-approved limits	Permitted with deterministic guardrails
Approval-required	Fleet-wide actuation, certificate actions, firmware release	Named human or explicit policy approval
Prohibited	Safety overrides or unconstrained tool access	Do not expose to an autonomous agent

DATA AND MODEL RISK

poisoning | spoofing | drift | adversarial inputs | unsafe objectives | weak lineage

AGENT RISK

prompt injection | tool abuse | privilege escalation | unsafe chaining | hidden actions

REQUIRED CONTROLS

TEVV | signed artefacts | scoped tools | short-lived credentials | kill switch | outcome verification

AGENT THREAT VECTORS

- prompt injection from retrieved content
- tool abuse and over-broad scopes
- privilege escalation through chained calls
- credential exposure in memory or logs

NON-NEGOTIABLE CONTROLS

- unique workload identity per agent instance
- sandboxed execution and allowlisted tools
- short-lived credentials and rate limits
- human approval, kill switch and immutable logs

> Do not provide an agent with unconstrained access to charger control APIs, fleet-wide dispatch, certificate issuance or firmware release functions.

Official source: NIST AI RMF 1.0; NIST AI RMF Generative AI Profile.

Cyber-physical monitoring and response

Correlate digital events with measured power and fleet outcomes

Cyber-physical detection loop

Correlate digital events with measured physical outcomes.

AUTO: enrich, preserve logs, rate-limit, quarantine non-critical sessions. **APPROVAL:** fleet suspension, mass revocation, rollback, site shutdown.

Detection signal	Potential scenario	Response
Dispatch outside site or market limits	Control-plane or model manipulation	Suspend dispatch and notify accountable operator
Certificate anomalies at scale	PKI compromise or insider activity	Emergency revocation and trust-store review
Commanded vs measured power gap	Metering, relay or dispatch manipulation	Alert automatically; isolate site with approval
Firmware drift across a cohort	Failed or unauthorised OTA	Halt rollout, rollback and investigate
Unusual bulk API operations	Credential abuse or API misuse	Rate-limit automatically; revoke with approval

SIGNALS TO COLLECT

- charger and gateway logs
- certificate and token events
- API and remote-access activity
- meter data and power quality
- vehicle state of charge and readiness
- firmware and attestation status

OPERATING PRINCIPLE

Contain the smallest practical unit while preserving safe service and evidence.

PREPARE | DETECT | CONTAIN | FALLBACK | INVESTIGATE | COMMUNICATE | RECOVER | LEARN

Source basis: Gamma monitoring model, p. 15; aligned with NIST CSF 2.0 and OT incident-response practice.

Implementation roadmap

Maturity model and 24-month path to continuous assurance

0-90 DAYS

ESTABLISH FOUNDATIONS

- asset and data-flow inventory
- trust-boundary mapping
- MFA and privileged-access review
- certificate ownership and expiry monitoring
- local safe-mode definition and testing
- critical logging and incident contacts

3-12 MONTHS

HARDEN AND INTEGRATE

- mTLS and scoped APIs
- segmented charging, dispatch, billing and admin zones
- signed OTA, SBOM and rollback
- SOC integration and anomaly detection
- supplier security clauses
- tabletop and technical exercises

12-24 MONTHS

SCALE AND ASSURE

- AI and agent governance
- cyber-physical red-team programme
- cross-party response exercises
- crypto-agility planning
- continuous control assurance
- measured evidence of safe recovery

BOARD AND ENGINEERING METRICS

01 **SBOM coverage**

02 **certificate lifecycle coverage**

03 **time to isolate**

04 **critical remediation time**

05 **safe-mode site coverage**

06 **AI model review cadence**

TARGET STATE A system that knows what is connected, who can control it, what software is running, what constrains each action and how safe service continues when trust degrades.

BOARD | SECURITY | ENGINEERING

OPERATIONS | SUPPLIERS | GRID / MARKET

Source basis: Gamma implementation roadmap, p. 17; terminology refined for enterprise publication.

AMPVERVE RESEARCH

Trust is the operating system of bidirectional energy.

V2G and V2X security is achieved by governing identities, software, communications, cloud services, AI, operations and recovery as one evidence-based system.

01	02	03	04
Authenticate every actor	**Authorise every action**	**Constrain every command**	**Verify every outcome**

SELECTED AUTHORITATIVE REFERENCES

1. ISO 15118-20:2022 - Vehicle to grid communication interface
2. IEC 61851 - Electric vehicle conductive charging system
3. Open Charge Alliance - OCPP 1.6, 2.0.1 and 2.1
4. IEC 63584-210:2025 - Open Charge Point Protocol 2.1
5. IEC 63110 - Management of EV charging and discharging infrastructure
6. IEC 62443 and IEC 62351 - OT and power-system security
7. IEEE 1547-2018 - DER interconnection and interoperability
8. ISO/SAE 21434:2021 - Road vehicle cybersecurity engineering
9. UNECE Regulations 155 and 156
10. NIST CSF 2.0; SP 800-207; SP 800-82 Rev. 3; AI RMF 1.0

SECURING BIDIRECTIONAL ENERGY

Enterprise White Paper | Executive Edition

www.ampverve.com