



FIRST EDITION

IAF CVES

Connected Vehicle and Ecosystem Standard

Interoperability, reliability and security
Vehicle, infrastructure and service assurance

DRAFT FOR TECHNICAL REVIEW

Technical validation and formal adoption are required before formal conformity certification. Release conditions are set out in Clause 2 and Annex J.

International Automotive Federation

English master text

iaf.com

Publication identity

IAF CVES First Edition

Connected Vehicle and Ecosystem Standard

International Automotive Federation

English master text | Revised technical text 0.2 | 13 September 2026

Scope of this publication

This working draft proposes requirements for evaluating connected vehicles, components, infrastructure and services as an interacting system. It is intended for vehicle manufacturers, suppliers, road operators, connectivity providers, service operators and evaluation teams preparing an IAF connected vehicle assurance programme.

The proposed benchmark asks whether information arrives in time, retains its meaning, comes from an authorised source and can be used without creating unacceptable risk. It also examines what happens when communications, positioning, infrastructure, trust services or commercial support fail.

Status and operational use

This revised technical text is prepared for the International Automotive Federation. It remains a development proposal pending technical validation and formal adoption. Normative provisions describe the intended operation of an adopted edition; the operational release conditions in R02-06 apply. The corporate presentation does not itself authorise conformity certification.

Numerical values identified as draft benchmark values are original proposals for validation. They are not universal safe limits, measured product results or established regulatory requirements. Application safety budgets may require stricter limits. Annex J identifies the decisions and validation work needed before publication.

Reading and navigation

The contents link to all main clauses and annexes. Requirement identifiers remain stable for assessment traceability. Each annex begins on a separate page. Quantitative results, configuration identity and operating limitations shall be read together.

Document control and interpretation

Field	Value
Proposed designation	IAF CVES First Edition
Full title	Connected Vehicle and Ecosystem Standard
Current status	Working Draft 0.2 for technical development
Intended issuing body	International Automotive Federation
Document language	English
Revision date	13 September 2026
Adoption status	Not adopted in this working draft
Change control	Changes to requirements, profiles and benchmark values require a documented revision

Normative language

Clauses 1 to 30 and Annexes A to H contain proposed normative provisions. Annex I provides an informative worked example. Annex J is an informative development and validation register. A requirement identifier such as R09-03 identifies a provision for traceability and review. Annex requirements use their annex section and row or test identifier. Recommendations expressed using should remain recommendations even when they appear in a numbered provision.

The words shall and shall not express requirements; should expresses a recommendation; may expresses permission; can describes capability or possibility. Notes and examples do not establish additional requirements. The word verified refers only to evidence actually reviewed within a specified assessment boundary.

Application of the requirements

The document contains no normative references to other organisations or their standards. It specifies assessment outcomes and assurance controls rather than inventing a universal radio technology. Every operational assessment must bind these requirements to a complete, versioned implementation profile. An incomplete profile cannot support an interoperability claim.

Revision changes

Revision 0.2 clarifies the operational release conditions, timing and freshness acceptance, timestamp integrity, emergency completion and independent implementation testing. It strengthens statistical stopping rules and adds methods for installed equipment and complete application outcomes. The edition retains 30 main clauses and 10 annexes.

Contents

Select a section to navigate to it.

1 Scope	6
2 Application and interpretation	6
3 Terms and abbreviations	7
4 Assessment objects and application profiles	9
5 Governance and deployment obligations	10
6 Risk and safety assurance	10
7 Architecture and dependency control	11
8 Connectivity and radio performance	11
9 Message meaning and interoperability	12
10 Time, positioning and information integrity	13
11 Identity, trust and cryptographic services	13
12 Cybersecurity and misuse resistance	14
13 Privacy and data governance	15
14 Vehicle-to-vehicle safety services	15
15 Infrastructure, traffic and smart city integration	16
16 Vulnerable road users and inclusive participation	16
17 Emergency and incident integration	17
18 Cloud, edge, network and service interfaces	18
19 Cooperative perception, manoeuvres and remote assistance	18
20 Human interaction, accessibility and service transparency	19
21 Software, configuration and supply chain integrity	19
22 Lifecycle, service continuity and retirement	20

Contents continued

Select a section to navigate to it.

23 Performance, reliability and resilience	21
24 Physical environment, energy and resource use	21
25 Verification and validation programme	22
26 Evidence, measurement and decision uncertainty	23
27 Conformity evaluation and decision rules	24
28 Public claims and the connectivity assurance record	24
29 Operation, incidents and corrective action	25
30 Future technology and controlled extension	25
Annex A Binding profiles and applicability	27
Annex B Metrics, benchmarks and statistical decisions	29
Annex C Scenario catalogue and test methods	33
Annex D Evaluation workflow and evidence descriptors	39
Annex E Risk and assurance worksheets	41
Annex F Evidence package and public record	43
Annex G Change, incident and reassessment controls	45
Annex H Emerging capability extension requirements	47
Annex I Worked evaluation example	49
Annex J Development, validation and publication register	51

1 Scope

This document establishes a common method for assessing connected vehicle functions and the ecosystems that support them throughout development, deployment, operation, maintenance, ownership transfer and retirement. The assessed outcome is a bounded connectivity capability supported by reproducible evidence.

R01-01 The applicant shall identify each assessed vehicle, component, infrastructure asset, service or ecosystem, its intended use and its integration boundary. The assessment shall include all external dependencies whose failure or misuse could invalidate the claimed connectivity outcome, even where those dependencies are operated by another party.

R01-02 Scope shall address relevant vehicle-to-vehicle, vehicle-to-infrastructure, vehicle-to-vulnerable-road-user and vehicle-to-network interactions. It shall include roadside communications, cloud and edge processing, emergency integration, traffic management and smart city interfaces whenever these are implemented or claimed.

R01-03 Passenger cars, motorcycles, buses, goods vehicles, special purpose vehicles, automated shuttles and retrofit devices may be assessed. The applicant shall specify vehicle categories, installation variants, operating speeds, road types, users and deployment markets rather than extrapolate a result between unlike categories.

R01-04 An assessment shall distinguish connectivity assurance from approval of braking, steering, crashworthiness, charging electrical safety or an automated driving system as a whole. Where a connected input influences those functions, the interface, failure behaviour and allocation of assurance responsibilities shall be assessed; separate obligations for the complete function remain applicable.

R01-05 Claims shall state the tested geography, profiles, services, configurations and operating conditions. A vehicle component result shall not be promoted as complete vehicle conformity. A connected city demonstration shall not be promoted as compatibility with every city, infrastructure operator or radio technology.

2 Application and interpretation

The standard is designed for several assessment objects without allowing exclusions to remove the very function being claimed. A common core is combined with application modules and a frozen deployment profile.

R02-01 The applicant and evaluator shall establish an applicability register before testing. Every requirement shall be marked applicable or not applicable, with a technical reason and a responsible reviewer. Lack of evidence, unavailable test equipment, outsourced operation or a failed test shall not justify a not applicable decision.

R02-02 Clauses 1 to 7 and 25 to 30 shall apply to every assessment, interpreted at the assessed boundary. Requirements in Clauses 8 to 24 and Annexes A to H shall apply whenever the corresponding function, interface, dependency or claim exists. Absence of a function shall be disclosed and verified where its exclusion could mislead a user.

R02-03 An implementation profile shall define all parameters necessary for repeatable evaluation. A stricter applicable legal obligation or application safety limit shall govern over a draft benchmark. A conflict that cannot be resolved shall stop the affected conformity decision and be recorded for technical disposition.

R02-04 A requirement may be satisfied by an alternative technical design only where its stated outcome is preserved and equivalent or stronger evidence is demonstrated. The evaluator shall document the comparison, assumptions and limitations. An alternative shall not waive a mandatory failure response or silently relax a numerical limit.

R02-05 Passing a pilot exercise shall be described as a pilot result against Working Draft 0.2. It shall not be labelled formal certification under an adopted IAF standard. Adoption, assessment authorisation and permissions to use any future mark are separate decisions.

R02-06 Operational release shall require documented technical validation of the selected benchmarks, complete binding profiles and test vectors, approved test and decision methods, competent evaluation and decision arrangements, and formal adoption by the issuing body. The release record shall identify the applicable revisions and unresolved limitations. Until these conditions are met, results shall remain pilot results; Annex J supports the release work.

3 Terms and abbreviations

The following meanings apply throughout this document. Operational profiles may add terms but shall not redefine the terms below in a way that changes their assurance meaning.

Term	Meaning
Applicant	Entity responsible for requesting an assessment and supplying truthful evidence
Evaluator	Competent party that performs or reviews the assessment
Decision authority	Party authorised by the scheme to decide conformity independently of the applicant
Assessment object	Identified vehicle, component, infrastructure, service or ecosystem within the evaluation boundary
Connected ecosystem	Vehicles and supporting assets and organisations that jointly deliver a connected function
Connectivity operating domain	Declared conditions in which a connected service is intended to meet its requirements
Binding profile	Frozen set of interfaces, versions, semantics, parameters and expected behaviours used for testing
Service contract	Technical definition of a service, including timing, meaning, authority, failure response and responsibilities
Eligible opportunity	Predefined event or time opportunity in which the claimed service is required to act
Timely valid delivery	Delivery that meets authentication, syntax, semantic, relevance and deadline requirements
Transport latency	Time from defined sender interface entry to defined receiver interface delivery

Term	Meaning
End-to-end latency	Time from a defined source event or sample to the specified usable application outcome
Age of information	Elapsed time since the source observation represented by information used at the receiver
Integrity	Confidence that information and system operation are not corrupted and meet declared error bounds
Authenticity	Evidence of an authorised origin or identity; it does not establish that content is factually correct
Availability	Fraction of eligible demand time during which the defined service is usable within its limits
Continuity	Ability to sustain required service over a stated session or manoeuvre without an unacceptable interruption
Degraded mode	Declared reduced capability with controlled behaviour and an explicit status indication
Safe fallback	Application specific action that controls risk when normal connected operation cannot continue
Common cause failure	One event that defeats multiple elements assumed to provide independent protection
Trust domain	Set of participants operating under a defined credential and authorisation policy
Misbehaviour	Incorrect or misleading communications, whether accidental, compromised or malicious
Pseudonym	Identifier intended to reduce routine linkability without removing authorised accountability
Replay	Reuse of previously valid information outside its authorised context or time
Evidence package	Controlled records linking a claim and its requirements to methods, results and decisions
Critical nonconformity	Failure that permits an unacceptable safety, security or privacy consequence or invalidates essential evidence
Major nonconformity	Unmet applicable requirement that materially affects the claimed capability or its assurance
Minor nonconformity	Limited failure without current evidence of a material capability impact, still requiring correction
V2V	Vehicle-to-vehicle communication
V2I	Vehicle-to-infrastructure communication, including its reverse direction where applicable
V2P	Vehicle-to-pedestrian or other vulnerable road user communication
V2N	Vehicle-to-network communication

Term	Meaning
V2X	Vehicle communication with relevant vehicles, infrastructure, people and networks
VRU	Vulnerable road user, including people walking, cycling or using mobility aids
RSU	Roadside unit
OBU	Onboard unit
API	Application programming interface
OTA	Over the air software or configuration delivery
P99	Empirical 99th percentile, with the estimator and sample population declared
AI	Artificial intelligence

4 Assessment objects and application profiles

The result must identify what has actually been assessed. The following object codes are scope descriptions, not quality grades.

Code	Object	Required boundary statement
V	Complete vehicle integration	Vehicle variant, installed hardware and software, external dependencies and enabled services
C	Component or retrofit device	Hardware and firmware, host assumptions, installation limits and required integration tests
I	Infrastructure	Site or asset family, installation geometry, controller interfaces, power and backhaul
S	Connected service	Production release, service region, interfaces, providers and operating responsibility
E	Ecosystem deployment	Identified combination of vehicle, infrastructure and service configurations with operational agreements

R04-01 The applicant shall select one or more object codes and the modules in Annex A. Every enabled safety-relevant connected function shall be included or explicitly isolated from the claim, with evidence that its exclusion does not undermine included functions.

R04-02 Every claimed service shall have a service contract covering inputs, outputs, authoritative sources, message validity, timing, security, privacy, availability, foreseeable misuse, degraded behaviour and responsible parties. Annex A defines the minimum fields.

R04-03 The connectivity operating domain shall include geography, road geometry, traffic density, speed, weather, visibility, radio conditions, positioning conditions, participating populations, network coverage and infrastructure maturity. Conditions that have not been demonstrated shall be disclosed as unverified.

R04-04 Variant selection shall represent the worst credible combinations of antenna position, processor load, bodywork shielding, power condition, communication module, software branch and service provider. Claimed equivalence between variants shall be justified and reviewed before evidence is reused.

R04-05 An ecosystem assessment shall allocate each interface to an owner and identify who resolves faults that cross organisational boundaries. A supplier statement alone shall not establish that the assembled system meets end-to-end requirements.

5 Governance and deployment obligations

Connected services distribute responsibility across organisations. The assurance case must show who can change, stop, restore and explain each part of the service.

R05-01 The applicant shall designate accountable owners for system safety, cybersecurity, personal data, service operation, software release and corrective action. Roles may be combined where competence and independence are maintained; conflicting approvals shall be assigned to a separate reviewer.

R05-02 A deployment obligations register shall identify the markets and duties applicable to radio use, vehicle operation, emergency interfaces, personal data, consumer information and infrastructure access. Evidence of relevant authorisations shall be retained in the assessment file. This document does not itself grant legal permission to deploy.

R05-03 Contracts between participating parties shall allocate incident reporting, outage notification, security patching, data handling, credential management, maintenance, evidence access and termination responsibilities. No essential responsibility shall remain assigned only to an undefined third party.

R05-04 Personnel performing configuration, security testing, traffic integration and decisions shall have documented competence. Evaluation personnel shall disclose interests and shall not assess their own unresolved design decisions without independent review.

R05-05 The applicant shall maintain a configuration controlled requirement register and a documented route for complaints, incident reports and correction requests. Changes to claimed capability shall be approved with a record of the evidence considered and the person responsible.

6 Risk and safety assurance

Communication performance is one contributor to safety. A fast message may still be false, irrelevant, ambiguous or too old for the current decision.

R06-01 The applicant shall analyse hazards from absent, delayed, duplicated, contradictory, mislocated and unauthorised information. The analysis shall include deliberate misuse, incorrect but validly signed data, nonparticipating road users, equipment faults and reasonably foreseeable user misunderstanding.

R06-02 Each safety-relevant service shall allocate a complete time budget from source observation through detection, communication, validation, decision, human response where relevant and physical action. Margins shall address uncertainty, worst credible motion and processing contention. A generic communication threshold shall not replace this analysis.

R06-03 Hazard controls shall distinguish prevention, detection, containment and fallback. A single remote message shall not directly authorise a safety-critical action without application specific validation, authority checks and a safety justification for the level of dependence placed on it.

R06-04 The safety case shall examine common causes across redundant paths, including shared power, antennas, timing sources, credentials, software, network operators and backhaul. Two communication paths shall not be counted as independent merely because they have different logical names.

R06-05 Residual risks, assumptions and operating restrictions shall be accepted by a designated competent owner before release. Open risks that can lead to an uncontrolled hazardous action shall block the affected claim. The hazard register shall link each control to tests and in service monitoring.

R06-06 Fallback shall be evaluated in its traffic context. Loss of connectivity shall not automatically cause abrupt braking, an unsafe stop or transfer of responsibility to an unprepared user. The design shall show that the selected response can be executed within the available time and operating space.

7 Architecture and dependency control

The architecture record shall enable an evaluator to follow a single service through all its sources, processing stages, interfaces and control decisions.

R07-01 The applicant shall maintain diagrams of data flows, trust boundaries, control authority, physical connections and external dependencies. Every wireless, wired, diagnostic, maintenance and cloud interface shall have an owner, access policy and monitored failure state.

R07-02 Safety-relevant processing and communications shall be protected from entertainment, advertising, unrelated analytics and passenger device workloads. Resource budgets shall cover processor time, memory, queues, storage, power, thermal limits and network capacity under concurrent peak activity.

R07-03 Network or service discovery shall establish the identity and capability of a peer before enabling privileged functions. An available access point or reachable server shall not by itself establish a trusted service relationship.

R07-04 Gateways shall enforce explicit message, command and data policies in both directions. Conversion between radio or application domains shall preserve source age, provenance, uncertainty and permission limits, and shall identify any transformation that changes the interpretation of information.

R07-05 A dependency inventory shall record service endpoints, remote configuration sources, cryptographic services, maps, time sources, software packages and failure effects. Hidden reliance on an unavailable commercial account, expired subscription or discontinued backend shall be treated as a service limitation.

8 Connectivity and radio performance

Radio technologies may differ between markets. The assessment focuses on declared operating conditions and demonstrated behaviour of the installed system.

R08-01 The binding profile shall identify the communication paths, modes, bands, channel settings, transmit constraints, antenna configurations, payload sizes and access assumptions used by each service. A service advertised as direct communication shall be tested without reliance on a wide area network.

R08-02 Installed performance shall be evaluated across line of sight and obstructed conditions, relevant distances and approach angles, changing speeds, dense traffic and representative interference. Antenna blockage by vehicles, trailers, loads, passengers or accessories shall be included where credible.

R08-03 Congestion control shall preserve a documented priority policy and prevent lower priority services from exhausting resources needed by safety-relevant services. Admission, rate limiting and shedding behaviour shall be demonstrated at the declared maximum load and during controlled overload.

R08-04 Multi path operation shall include duplicate detection, ordering, source age preservation and common cause analysis. Switching between direct, mobile, local wireless and satellite paths shall not silently change a service from real-time operation to delayed information.

R08-05 The equipment shall detect loss of an essential antenna, radio function or connection state where required by the hazard analysis. Detection and service status changes shall meet the allocated time budget, and a restored signal shall not immediately restore safety-relevant authority without health checks.

R08-06 Range claims shall state the measurement geometry, environment, traffic load, message type and timely delivery criterion. A best case maximum range shall not be represented as a guaranteed operating distance throughout the claimed domain.

9 Message meaning and interoperability

Interoperability requires agreement on meaning as well as successful receipt of bytes. The same location, signal state or warning must not lead to incompatible decisions across implementations.

R09-01 The binding profile shall freeze the message schema, encoding, versions, optional fields, units, coordinate frames, time base, precision, permitted ranges and unknown value representations. The evaluator shall have executable test vectors and expected decoded values for every claimed message type.

R09-02 Receivers shall validate message length, structure, permissions, freshness, physical plausibility and relevance before releasing data to an application. Unrecognised mandatory fields or incompatible versions shall cause a controlled rejection or explicitly limited operation, not a guessed interpretation.

R09-03 A relay or gateway shall preserve the observation time and shall not make old data appear new by replacing its source timestamp with a forwarding timestamp. Derived information shall carry both the original observation provenance and the time of derivation where needed to interpret its validity.

R09-04 Interoperability testing shall exercise independent implementations and all claimed combinations of sender, receiver, infrastructure and service version. Bidirectional functions shall be tested in both directions. Shared source code or a common emulator shall be disclosed and shall not be treated as independent implementation diversity.

R09-05 Retries, acknowledgements, cancellation, replacement, sequence wraparound and duplicate suppression shall have deterministic semantics. Transactional actions shall prevent repeated execution following a timeout or reconnect. Broadcast services shall not be judged using an acknowledgement model they do not implement.

R09-06 The assessment shall include malformed, boundary, unsupported and contradictory inputs. No mandatory semantic test may fail while an interoperability claim remains positive, even if average delivery performance is high.

10 Time, positioning and information integrity

Position and time errors can turn a technically correct message into an unsafe instruction. Declared accuracy must be supported by measured error distributions and a response to loss of integrity.

R10-01 The profile shall define the time reference, timestamp precision, synchronisation method, permissible offset and response to uncertainty. Tests shall include clock drift, reset, discontinuity, rollover, delayed synchronisation and inconsistent time sources.

R10-02 Position-related services shall specify coordinate reference, map version, vehicle reference point, orientation, lane association and uncertainty. Positioning performance shall be tested with independent ground truth in urban canyons, tunnels, junctions and other relevant conditions rather than inferred from a receiver specification.

R10-03 Receivers shall reject or downgrade information when declared position or time uncertainty exceeds the application limit. Missing coordinates, unknown heading or invalid speed shall not be converted into plausible default values such as zero.

R10-04 The applicant shall establish an integrity monitor for functions whose safety depends on bounded position or time error. The evidence shall cover detection time, missed detections, false alarms and protection against false confidence during spoofing, jamming or sensor disagreement.

R10-05 Spatial relevance shall consider direction of travel, road level, lane geometry and event extent. A warning from an adjacent motorway, bridge, tunnel level or opposite carriageway shall not be presented as an instruction for the current path without a justified association.

R10-06 Claims of lane level capability shall define the lane discrimination objective and allowable error for the intended geometry. No single accuracy number shall establish suitability for all lane widths, turning movements or road layouts.

R10-07 The freshness policy shall define permissible clock uncertainty and future timestamp tolerance. A timestamp beyond that tolerance shall be rejected or quarantined. Negative measured age shall not be silently set to zero and treated as fresh information. Message age limits shall be evaluated with the uncertainty allowance specified in Annex B.

11 Identity, trust and cryptographic services

Identity services support accountable participation while limiting unnecessary tracking. An authenticated message remains subject to plausibility and relevance checks.

R11-01 The applicant shall define credential issuance, activation, renewal, revocation, expiry, recovery and retirement for devices, services, administrators and privileged roles. Private keys shall be protected against extraction and unauthorised use in a manner proportionate to their safety and security impact.

R11-02 Authorisation shall bind a credential to permitted functions and contexts. A general vehicle credential shall not grant authority to request emergency priority, modify a traffic signal, issue a road closure or remotely control another vehicle.

R11-03 The system shall verify the required identity chain and permissions, and shall define behaviour for expired, revoked, unknown or unreachable trust information. Offline operation shall have a bounded policy

for cached trust state. Failure to contact a trust service shall not automatically authorise an otherwise untrusted action.

R11-04 Pseudonym changes shall reduce routine linkability while preserving service continuity within its safety constraints. The design shall assess tracking through payload content, trajectory, network identifiers and certificate timing, rather than treating identifier rotation alone as anonymity.

R11-05 Key compromise and mass credential invalidation shall be exercised. Revocation distribution capacity, detection delay, offline exposure, restoration and effects on legitimate participants shall be measured against the profile's declared limits.

R11-06 The cryptographic inventory shall identify algorithms, parameters, keys, trust anchors and protection lifetimes. The design shall support controlled algorithm and trust anchor migration, with downgrade protection, mixed version testing and an explicit plan for information requiring long-term confidentiality.

12 Cybersecurity and misuse resistance

Security controls shall cover the complete path from vehicle and roadside hardware to service administration and remote operations.

R12-01 The applicant shall maintain a threat analysis covering remote access, local radio, maintenance ports, mobile applications, supply chain packages, cloud accounts, insiders and physical access. The analysis shall link attack consequences to service and vehicle hazards and to the protections required at each boundary.

R12-02 Systems shall enforce least privilege, separation of duties for high impact changes, authenticated administration and protected secrets. Default shared credentials shall not remain in deployed equipment. Remote privileged human access shall use multiple independent authentication factors or a documented and tested control providing equivalent protection. Diagnostic or maintenance access shall be time bounded and auditable where it can change assessed behaviour.

R12-03 Secure startup, software authenticity checks and runtime controls shall protect safety-relevant executable code and configuration. Failure of integrity checks shall enter a controlled recovery state and shall not silently boot unverified software with operational privileges.

R12-04 Security testing shall include parser robustness, access control, replay, resource exhaustion, credential misuse and isolation between domains. Tests shall use approved environments and authorised endpoints. Public traffic systems or emergency systems shall not be exposed to uncontrolled intrusive testing.

R12-05 The applicant shall maintain a vulnerability intake route, triage criteria, containment options and correction process throughout the declared support period. An exploitable issue with a credible path to uncontrolled safety-relevant action shall block release or trigger suspension of the affected capability until effective containment is verified.

R12-06 Misbehaviour detection shall distinguish valid identity from credible content and shall address false accusation. Reports shall preserve relevant evidence, minimise personal data and permit review. Automatic exclusion policies shall be tested against legitimate unusual behaviour and coordinated false reports.

R12-07 Security monitoring shall detect compromise without exhausting resources or degrading essential vehicle functions. Forensic records shall protect integrity, control access and preserve the time uncertainty needed to reconstruct event order.

13 Privacy and data governance

Connected mobility can reveal routes, identities and behaviour even when names are absent. Privacy controls must address the complete information flow and the people affected by it.

R13-01 The applicant shall map personal and potentially identifying data across collection, processing, transmission, storage, sharing and deletion. Purposes, authorised recipients, legal basis, retention limits and responsibility for each flow shall be documented before deployment.

R13-02 Safety communications shall contain no unnecessary persistent identifiers or sensitive occupant information. High frequency trajectories, device identifiers and combined datasets shall be assessed for reidentification and tracking risk. Pseudonymous data shall not be assumed anonymous.

R13-03 Optional analytics, advertising and secondary commercial uses shall be distinguishable from essential services. Users shall receive clear choices where required, and withdrawal from an optional purpose shall not silently disable unrelated safety functions.

R13-04 Ownership transfer, rental return, shared vehicle sessions and account deletion shall revoke prior access and remove or segregate personal data. Tests shall demonstrate that a former user cannot retrieve subsequent location, cabin data or remote control privileges.

R13-05 Cross-border data routes and service migrations shall preserve the applicable privacy controls. Access requests, corrections, deletion obligations and authorised preservation for incidents shall have auditable workflows. Evidence retention shall be reconciled with minimisation and legal retention duties.

R13-06 Cabin sensing, child-related information, health indicators and emergency disclosures shall receive a dedicated necessity and access review when present. Continuous recording shall not be the default substitute for a targeted event record where the narrower record can meet the purpose.

14 Vehicle-to-vehicle safety services

V2V services shall be assessed at the receiving application, including the conditions under which warnings or assistance are withheld.

R14-01 Every claimed V2V use case shall define its triggering conditions, required information, affected road users, action deadline and cancellation logic. At minimum, the applicability review shall consider abrupt deceleration, stationary vehicles, queues, intersection conflicts, wrong way movement, lane changes and approaching emergency vehicles.

R14-02 Tests shall include participating and nonparticipating vehicles, unequal equipment capability, mixed vehicle sizes and occlusion. Lack of a connected message shall not be interpreted as evidence that a road, lane or conflict region is clear.

R14-03 The receiving application shall assess path relevance and message credibility before issuing a warning or influencing control. A message from a stopped vehicle on another road level, a parked vehicle or a road user outside the conflict area shall be tested for inappropriate activation.

R14-04 Repeated, stale or contradictory events shall not create an uncontrolled warning cascade. Suppression, escalation and cancellation shall be deterministic and shall preserve time critical warnings where the hazard remains present.

R14-05 Performance reporting shall include timely correct activations, missed activations, unnecessary activations, cancellation delay and behaviour when information is unavailable. Network delivery percentages shall be reported separately from application effectiveness.

R14-06 A claim that connectivity prevents collisions or improves safety by a quantified amount shall require an appropriate study design and outcome evidence beyond communication tests. Simulated or predicted benefits shall be identified as such.

15 Infrastructure, traffic and smart city integration

Smart city compatibility shall be expressed as demonstrated interfaces and services within identified deployments.

R15-01 The infrastructure module shall cover applicable signal status, intersection geometry, speed and lane restrictions, roadworks, closures, reversible lanes, parking, road weather and traffic priority services. The profile shall identify which source has authority to issue, amend and cancel each information type.

R15-02 Signal messages shall be bound to the correct controller, intersection, approach and movement. Tests shall include adaptive timing, inconsistent map and signal versions, controller restart, maintenance mode and loss of synchronisation. A received permissive state shall not authorise ignoring physical signals or unresolved conflicts.

R15-03 Priority and preemption requests shall have separate permission rules, validity periods and audit trails. A legitimate request shall not be treated as a guarantee that priority has been granted. The vehicle shall verify the current response and act within its own safety obligations.

R15-04 Roadside installation records shall include asset identity, antenna orientation, surveyed geometry, controller connection, power protection, environmental limits and maintenance access. Moving or replacing an RSU shall trigger configuration and relevance checks before service restoration.

R15-05 City and corridor interfaces shall define data provenance, update frequency, expiry, conflict handling and service health. Map changes and temporary restrictions shall include effective times and cancellation paths that prevent obsolete instructions from remaining active.

R15-06 Connected tolling, parking, charging discovery and multimodal services shall separate commercial transactions from safety authority. Payment failure shall not create an unsafe vehicle command. Transaction reconciliation shall address duplicate charges and interrupted sessions where these services are in scope.

R15-07 Claims across municipalities, road operators or borders shall be supported by the profile and interoperability matrix for each claimed combination. Unavailable city interfaces shall be disclosed without treating a generic API demonstration as actual deployment acceptance.

16 Vulnerable road users and inclusive participation

Connected safety must account for people who carry no device and people whose devices provide inaccurate or incomplete information.

R16-01 The VRU module shall define the supported user groups, device types, carrying positions, motion patterns and operating environments. Evaluation shall include walking, cycling, crossing, stationary users, mobility aids and groups where relevant to the claim.

R16-02 No device signal shall be required for a person to be considered a potential road user by the vehicle's overall safety concept. Absence of a VRU transmission shall not be displayed or interpreted as absence of people.

R16-03 Tests shall address pocket and bag placement, body shielding, low battery, denied permissions, suspended applications, intermittent connectivity and inaccurate positioning. Shared devices and multiple devices carried by one person shall be considered in duplicate and identity handling.

R16-04 Warning effectiveness shall be evaluated against relevant user characteristics, including hearing, vision, language and mobility limitations. Unsafe reliance on a person reading a small screen or reacting within an unvalidated time shall not support a positive safety claim.

R16-05 Privacy evaluation shall address persistent observation of children, pedestrians and other noncustomers. Infrastructure sensing and object sharing shall minimise identifying details and shall prevent an object identifier from unnecessarily becoming a long-term tracking identifier.

17 Emergency and incident integration

Emergency integration shall distinguish a locally generated event, successful communication and acceptance by the responsible responder. These are separate outcomes.

R17-01 The emergency service contract shall define manual and automatic triggers, location data, minimum event data, routing, acknowledgements, voice or accessible alternatives where provided, retry rules, cancellation and fallback. The user shall be informed when delivery or acceptance has not been confirmed.

R17-02 End-to-end tests shall use authorised test endpoints that represent the receiving service. An acknowledged test receiver shall not be presented as proof of operational responder integration unless the operational interface and acceptance arrangements are also evidenced.

R17-03 Tests shall include primary power loss, damaged or blocked antenna conditions, poor location, network rejection, duplicate triggers and roaming. Backup power capability shall be measured over the declared temperature range and end of life capacity assumptions.

R17-04 Emergency data shall be limited to what is needed for the defined response. The system shall prevent fabricated emergency authority, unauthorised priority requests and disclosure to an unverified recipient. Legitimate emergency access shall have a traceable permission model.

R17-05 Coordinated response services shall define roles for traffic management, roadside assistance and emergency responders. No single delivery acknowledgement shall imply that all participating organisations have received the event or begun action.

R17-06 A disaster or congestion mode shall prioritise essential information, limit retry storms and state the services still available. Satellite or alternative paths shall be labelled according to their demonstrated latency, coverage and receiving endpoint capability.

R17-07 Emergency acceptance criteria shall identify each required outcome, including data receipt, event acceptance and any required voice or accessible communication channel. Partial success shall be reported as partial success. A data acknowledgement alone shall not pass a service contract that also requires another outcome.

18 Cloud, edge, network and service interfaces

Backend availability is part of the connected function whenever the vehicle depends on remote processing, data or authorisation.

R18-01 Service APIs shall have versioned contracts for authentication, authorisation, payload semantics, errors, rate limits, retries, timeouts and compatibility. Input validation shall apply equally to internal and external producers.

R18-02 Service deployment shall control isolation between tenants, vehicles and regions. Tests shall include wrong vehicle identifiers, stale sessions, unauthorised fleet access and cross tenant data requests. A valid account shall not provide access to every vehicle associated with a service provider. Object-level permissions shall be checked on every protected request, including requests that use a substituted vehicle or tenant identifier.

R18-03 Edge relocation, mobile network handover and backend failover shall preserve session authority, event ordering and data age. Tasks that cannot finish before their deadline shall be cancelled or downgraded rather than delivered as if still actionable.

R18-04 The operator shall maintain end-to-end health monitoring that distinguishes network reachability, server response and usable application output. A successful health page response shall not alone establish that a safety-relevant service is available.

R18-05 Remote actions such as unlock, start, immobilisation or configuration changes shall verify user authority, vehicle identity and current operating state. Delayed or duplicated commands shall not execute outside their permitted context. Where movement may be affected, the vehicle shall enforce a local safety boundary.

R18-06 Recovery shall address corrupted databases, stale replicas, loss of a region, expired credentials and unavailable dependencies. Backup restoration shall be tested for correctness and age of restored state, not merely successful server startup.

19 Cooperative perception, manoeuvres and remote assistance

Advanced cooperation increases dependence on information from others. Its assessment requires a clear allocation of decision authority and an explicit response when cooperation ends.

R19-01 Shared perception shall communicate relevant observation time, sensor or source provenance, coordinate frame, uncertainty and object lifecycle. Receivers shall account for duplicate observations and correlated sources before combining confidence values.

R19-02 Cooperative perception tests shall include occlusion, false objects, missed objects, inconsistent classifications, delayed tracks and coordinate errors. The application shall avoid treating several relayed copies of one observation as independent evidence.

R19-03 Manoeuvre coordination shall define request, negotiation, commitment, expiry, cancellation and abort states, including the behaviour of each participant. Missing acknowledgement, changed capability or lost contact shall not leave incompatible commitments active.

R19-04 Platooning and coordinated motion claims shall establish limits for spacing, speed, vehicle dynamics, membership changes and communication loss. Timing and reliability requirements shall be derived from the actual control and safety analysis. Generic draft communication values in Annex B shall not qualify a closed loop control function.

R19-05 Remote assistance shall be distinguished from remote driving. The profile shall define whether a remote party supplies advice, route permission or continuous control, and shall state local vehicle authority, operator competence, sensory coverage, command freshness and takeover limits.

R19-06 Remote control shall cease to authorise new motion commands when its freshness, identity or situational information exceeds declared limits. Recovery from a disconnected session shall require revalidation of current context and shall not execute buffered movement commands.

R19-07 A remotely supported automated vehicle shall demonstrate a safe response to loss of the operator, video stream, network and backend individually and in common cause combinations. A theoretical network service level shall not establish the safety of the complete remote operation.

20 Human interaction, accessibility and service transparency

People need to understand what a connected function is doing, what it depends on and when it cannot be relied upon.

R20-01 The user interface shall distinguish available, degraded, unavailable, unverified and disabled service states when that distinction affects safe use. It shall avoid presenting signal strength as proof that every connected safety service is functioning.

R20-02 Warnings shall convey the relevant action or hazard without requiring unnecessary interpretation during driving. Competing notifications, repeated alerts, nuisance warnings and cancellation behaviour shall be evaluated under representative workload.

R20-03 The applicant shall conduct user evaluation for safety-relevant interactions using representative participants and tasks. Recruitment, sample justification, response measures, errors and foreseeable misunderstanding shall be documented. A small convenience sample shall not justify broad population claims.

R20-04 Essential status and warnings shall use accessible combinations of visual, audible or tactile means as appropriate. Localisation shall preserve meaning, urgency, units and road context. The design shall address users unfamiliar with the local language where the claim includes cross-border use.

R20-05 Setup, subscription and privacy choices shall explain what capabilities depend on external coverage, infrastructure or payment. Users shall receive clear notice of service withdrawal or reduced support that affects a purchased or safety-relevant function.

R20-06 Health monitoring or fatigue inference may be included only when implemented and separately validated for its declared use. This document does not establish a clinical diagnosis, cabin ergonomics certification or general wellbeing rating.

21 Software, configuration and supply chain integrity

An assessment is valid only for an identifiable configuration. Software changes can alter message meaning, timing, trust and failure behaviour without changing the vehicle hardware.

R21-01 The applicant shall maintain an inventory of hardware, software, libraries, models, calibration and configuration for every assessed function. The inventory shall identify supplier, version, integrity identifier, relevant dependencies and support status.

R21-02 Build and release processes shall protect source, build inputs, signing keys and release approval. Reproducibility or equivalent traceability shall permit the evaluator to link the installed image to the reviewed release and test evidence.

R21-03 Updates shall verify authenticity, integrity, target compatibility, prerequisites and installation conditions. Tests shall include interrupted download, interrupted installation, insufficient power, corrupted packages, incompatible dependencies and attempted installation of unauthorised older software.

R21-04 Recovery shall return the system to a known authorised state or a defined restricted state. A rollback shall not silently restore a known exploitable vulnerability. Where rollback is unsafe, the release plan shall provide another recoverable means to maintain essential functions.

R21-05 Deployment shall use staged exposure, health checks and stop criteria proportionate to risk. The operator shall be able to identify the affected population and halt distribution when a defect or adverse trend is detected.

R21-06 Every change shall receive an impact assessment against the claim, profile, hazards and evidence. Changes to timing, message semantics, radio configuration, trust policy, safety logic, data handling or AI behaviour shall trigger the relevant regression tests and decision review under Annex G.

R21-07 Supplier discontinuation, compromised packages and unavailable source or keys shall have an exit and recovery plan. Replacement components shall undergo integration checks; a nominally equivalent part number shall not automatically preserve assessed connectivity performance.

22 Lifecycle, service continuity and retirement

Vehicle service life may exceed the life of a network generation, cloud service or commercial relationship. The applicant must make those dependencies visible and manageable.

R22-01 Before deployment, the applicant shall declare the support period, its start basis, supported functions, update responsibilities and limitations. The declaration shall distinguish vehicle life, software support, network access and subscription entitlement.

R22-02 A continuity plan shall address network retirement, provider failure, expired service agreements, trust anchor replacement, account loss and business closure. Essential safety behaviour shall remain controlled when a commercial service ends.

R22-03 Maintenance instructions shall include antenna and cable checks, configuration validation, credential servicing, diagnostics and requalification after repair. The system shall detect or record modifications that can invalidate the assessed installation.

R22-04 Ownership transfer and resale shall preserve supported safety functions where contractually provided and clearly state which services require reactivation. Previous owners, fleet accounts and repair tools shall lose permissions no longer justified.

R22-05 Retirement shall revoke credentials, disable remote authority, erase or retain data according to documented duties and update the status of the assessment record. Decommissioned roadside equipment shall not continue to broadcast apparently valid traffic information.

R22-06 Notifications of material service withdrawal shall be early enough for a safe transition under the deployment obligations and contractual commitments. The applicant shall document the notice period and mitigation instead of implying indefinite connectivity.

23 Performance, reliability and resilience

Performance claims shall use complete measurement boundaries and realistic load. Good average performance cannot conceal deadline failures or loss of service in a critical scenario.

R23-01 Each service shall declare limits for relevant latency, age of information, timely valid delivery, availability, continuity, recovery time and data integrity. Safety-relevant services shall also specify failure detection and fallback deadlines. Annex B supplies measurement definitions and draft reference values.

R23-02 Measurements shall include full enabled security processing, production message sizes, certificate lifecycle activity, diagnostic loads and competing traffic. Disabling security or reducing the payload to improve performance shall invalidate comparison with the production claim.

R23-03 The evaluator shall measure distributions and tail behaviour by scenario, route, condition and implementation pair. Results shall include missing, late, rejected and duplicated messages. Reporting latency only for the successfully received subset shall be labelled conditional and accompanied by the total eligible opportunity count.

R23-04 Resilience tests shall include burst loss, prolonged outage, handover failure, severe congestion, backend failure, trust service outage, loss of time reference and restoration. The system shall maintain the declared safety boundary throughout degradation and recovery.

R23-05 Availability shall be computed over eligible demand time with an exclusion policy fixed before observation. Unplanned outages and failures inside the claimed domain shall remain in the denominator. Planned maintenance shall be reported separately and shall not disappear from a continuous availability claim.

R23-06 Redundancy claims shall identify independent failure assumptions and quantify the residual common cause exposure. A fallback service with different capabilities shall be reported as degraded operation rather than full availability.

R23-07 The operator shall monitor service indicators at a frequency capable of detecting material loss of the claimed capability. Monitoring gaps, missing probes and unobserved regions shall be reported, not treated as successful operation.

24 Physical environment, energy and resource use

The connected function shall remain controlled under its installation environment and shall account for the resources needed to deliver its benefits.

R24-01 Environmental qualification shall cover the declared temperature, humidity, vibration, shock, ingress, corrosion, power variation and electromagnetic environment of each installation. Applicable test severities shall be specified in the binding profile with an installation and risk rationale.

R24-02 Functional communication checks shall be performed before, during where feasible and after environmental exposure. A physically intact enclosure shall not establish that timing, sensitivity, positioning or trust storage remains within requirements.

R24-03 Power management shall protect vehicle startup, essential functions and any declared emergency reserve. Sleep, wakeup, low battery, repeated reconnect and failed update behaviour shall be evaluated for battery drain and missed service availability.

R24-04 Energy and resource claims shall specify measurement boundaries, service workload and comparison baseline. Vehicle energy, roadside power, network processing and backend use shall not be selectively omitted where the claim describes an ecosystem benefit.

R24-05 The design should support repair, replacement and continued compatibility of connectivity equipment. Where hardware replacement is needed for network or cryptographic migration, the applicant shall describe the installation, data and requalification implications.

R24-06 A claim of reduced congestion, emissions or energy consumption shall disclose the study conditions, counterfactual baseline and uncertainty. Communication conformance alone shall not be treated as evidence of an environmental improvement.

25 Verification and validation programme

The evaluation programme combines documentary review, controlled testing, independent interoperability and representative field evidence. Each method answers a different question.

R25-01 Before testing, the evaluator shall approve the scope, frozen profile, hazard based scenario selection, acceptance limits, instrumentation, sampling plan and stop criteria. Acceptance criteria shall not be chosen after observing the results.

R25-02 The programme shall include design review, bench testing, software or hardware simulation where justified, controlled track or site testing and field observation appropriate to the claim. Simulation shall be validated against relevant physical measurements and its gaps shall be stated.

R25-03 The scenario catalogue in Annex C shall be screened in full. Applicable scenario families shall be selected with a documented risk and coverage rationale. Omitted cases shall identify the absent function or domain condition; difficult or unfavourable cases shall not be excluded to improve a result.

R25-04 Instrumentation shall have sufficient accuracy, synchronisation and sampling rate for the decision limits. Calibration, configuration, uncertainty and data loss shall be recorded. Test tools shall be verified against known inputs and expected outputs before use.

R25-05 Controlled fault injection shall establish degraded and recovery behaviour before road observation of safety-relevant services. Road tests shall use authorised conditions and competent personnel. Unsafe failures shall be explored by simulation, bench or closed site methods instead of exposing the public.

R25-06 Independent interoperability shall include at least two counterpart implementations developed independently of the assessed implementation and of one another for each claimed interface role, unless

fewer exist. If fewer exist, the evidence limitation shall block a broad multi-vendor claim and confine the result to the named tested configuration.

R25-07 Tests shall be repeatable from retained setup records, version identifiers and data. An evaluator shall record deviations, invalid runs and retests with reasons. A failed valid run shall remain visible after a later successful retest.

R25-08 The verification matrix shall cover both communication delivery and the complete claimed application outcome. It shall also route applicable physical, environmental, power, privacy and human interaction requirements to appropriate tests or objective evidence. The method cards in Annex C establish a minimum method set and shall be extended where a requirement is not adequately covered.

26 Evidence, measurement and decision uncertainty

Evidence shall support the exact claim and shall allow another competent reviewer to understand the measurement and its limits.

R26-01 Each applicable requirement shall link to objective evidence, an acceptance criterion, a result, a reviewer and the assessed configuration. Absence of evidence shall be recorded as not demonstrated, not pass.

R26-02 Every quantitative result shall state the unit, measurement endpoints, sample population, test conditions, estimator, uncertainty and acceptance rule. The report shall separate raw observations, statistical estimates, modelled values and engineering judgements.

R26-03 One sided confidence limits shall be used for success rate claims as specified in Annex B. Correlation between messages, runs or route segments shall be addressed through independent blocks or a justified clustered analysis. A large number of messages in one journey shall not automatically establish a large independent sample.

R26-04 For an upper limit, conformity shall require the relevant upper uncertainty bound to remain at or below that limit. For a lower limit, the lower bound shall remain at or above it. An overlapping decision interval shall be reported as inconclusive unless a predeclared, justified decision rule resolves it.

R26-05 The evidence package shall preserve raw data integrity, tool versions, transformations, exclusions and chain of custody. Reanalysis shall be reproducible. Access restrictions needed for security or privacy shall not prevent authorised technical review.

R26-06 Confidential implementation details may be retained in a controlled annex to the assessment file. Public summaries shall accurately describe scope and limitations without exposing secrets, personal data or exploit details.

R26-07 The sampling plan shall predeclare sample size or a statistically justified sequential stopping rule, analysis populations and treatment of multiple comparisons. Testing shall not stop solely because a favourable confidence bound first appears. Repeated analyses shall control the declared error rate, and additional testing after a failure shall follow a documented correction and retest plan.

27 Conformity evaluation and decision rules

Conformity is a statement about a defined scope and a defined configuration. It cannot be created by averaging away an unmet requirement.

R27-01 Each applicable provision shall receive pass, fail, inconclusive or not assessed status. Not applicable shall be used only under Clause 2. A positive decision shall require all applicable mandatory provisions to pass and all required evidence to be available.

R27-02 Critical and major nonconformities shall block a positive decision. Minor nonconformities shall be corrected and verified before a positive decision under this draft's proposed scheme. An improvement recommendation that does not identify an unmet requirement shall be recorded separately.

R27-03 The applicant shall analyse the cause and extent of each nonconformity, implement correction and provide regression evidence. Repeating only the successful portion of a failed scenario shall not close the finding.

R27-04 The decision authority shall be separate from the applicant and independent of the work being judged. It shall review applicability, evidence sufficiency, unresolved findings, competence and claim wording before issuing a decision.

R27-05 Annex D defines the decision workflow and evidence descriptors. No total score, optional feature count or commercial status shall compensate for a failed mandatory requirement. Comparisons shall use like profiles, domains and evidence types.

R27-06 Appeals shall be reviewed by a competent person who was not responsible for the disputed decision. New evidence or interpretation shall be documented; the applicant shall not receive permission to conceal a material failed result while an appeal is pending.

28 Public claims and the connectivity assurance record

A concise public record shall make the assessment useful without implying capabilities that were not evaluated.

R28-01 Every published result shall identify designation, edition, object, configuration baseline, assessed modules, binding profile, operating domain, evaluation date, decision status, decision authority and material limitations. Annex F defines the minimum record.

R28-02 A public statement shall distinguish component capability, complete vehicle integration and deployed ecosystem performance. Claims shall not assert universal compatibility, uninterrupted connectivity, immunity from attack or guaranteed prevention of collisions. Specific performance claims shall remain bounded by the evaluated profile, domain and evidence.

R28-03 The assurance record shall be versioned and linked to a controlled status source where one is operated. A machine-readable record or QR pointer shall not itself constitute proof of conformity; the issuer, integrity and current status shall be verifiable.

R28-04 The result shall state which changes or events require reassessment and whether continuing operational monitoring forms part of the scope. A test result represents the evaluated configuration and evidence period; it shall not imply that future updates or deployments have already passed.

R28-05 Use of a future IAF mark shall require explicit scheme authorisation. This working draft does not create an active mark, registry, certificate or grant of recognition. Prototype records used during piloting shall be conspicuously labelled pilot or example.

29 Operation, incidents and corrective action

Operational evidence shall feed back into the requirements, test catalogue and published assessment status.

R29-01 Operators shall monitor the indicators required by the service contract, including material losses of timing, availability, trust, data quality and interoperability. Monitoring shall include unusual clusters, affected variants and infrastructure or provider changes.

R29-02 Incident procedures shall assign triage, evidence preservation, containment, stakeholder notification, recovery and closure responsibilities. Urgent safety actions shall not wait for completion of a root cause report. Applicable reporting deadlines shall be identified in the obligations register.

R29-03 When a critical condition can invalidate a public claim, the responsible parties shall restrict or suspend the affected function or claim as appropriate and notify the decision authority without undue delay. Restoration shall require evidence that the control is effective for the affected population.

R29-04 Corrective action shall address similar products, deployments and dependencies, including systems that have not yet failed. The applicant shall verify that the correction does not introduce unsafe timing, compatibility, privacy or recovery behaviour.

R29-05 Scheduled reviews shall occur at a documented risk-based interval and after the triggers in Annex G. Reviews shall examine operational trends, changes in threats, infrastructure and technology support, and the continuing validity of the operating domain.

R29-06 Useful lessons shall be converted into revised controls, test scenarios and user information while protecting personal and sensitive security data. Closure shall record who accepted the residual risk and how effectiveness will continue to be checked.

30 Future technology and controlled extension

The architecture should accommodate future communications without allowing a technology label to substitute for evidence. Candidate capabilities require the same discipline as existing ones.

R30-01 New radio generations, satellite paths, integrated sensing, novel roadside computing and other communication mechanisms may be introduced through a versioned extension profile. The extension shall define interface behaviour, maturity, restrictions, fallbacks and the evidence needed for its specific claim.

R30-02 AI used to interpret connected data, detect misbehaviour or support decisions shall have a declared function, training and evaluation data provenance, operating limits and change control. Validation shall include distribution shift, missing data, unusual road users and adversarially misleading inputs relevant to the threat model.

R30-03 Adaptive or learning behaviour shall remain within a validated operational boundary. Online model changes shall not bypass release approval for safety-relevant decisions. A model update that alters assessed behaviour shall trigger impact analysis and reassessment.

R30-04 Generated language, synthetic data or a digital twin shall not be treated as authoritative live traffic evidence without validation of its source, purpose and fidelity. A generative interface shall not invent road permission, emergency acknowledgement or remote driving authority.

R30-05 Migration towards quantum-resistant protection shall test larger credentials and messages, verification cost, bandwidth, storage, mixed fleets and downgrade resistance. An algorithm name alone shall not establish deployment readiness or interoperability.

R30-06 Satellite and other discontinuous paths shall demonstrate coverage gaps, acquisition time, blockage, handover, outage and receiver acceptance. They may support an emergency or informational service within measured limits; they shall not be presumed suitable for real-time cooperative control.

R30-07 The extension process shall retain backward compatibility where safe, identify deliberate incompatibilities and provide migration and retirement rules. Annex H defines minimum acceptance questions for emerging capabilities; Annex J records development work before adoption.

Annex A Binding profiles and applicability

Normative within the proposed draft

A1 Required profile package

Before operational evaluation, the applicant shall deliver the following complete package. All fields shall contain a value, a justified not applicable entry or a stated limitation. An unfilled field affecting acceptance shall prevent a positive decision.

Profile element	Required content
Identity	Profile identifier, revision, owner, issue date and integrity identifier
Object	V, C, I, S or E; exact product, installation, release and assessed boundary
Domain	Markets, routes or site families, geometry, speed, traffic, environment and network conditions
Functions	Enabled services, modules, intended outcomes and explicit exclusions
Participants	Sender, receiver, gateway, controller, backend and operational owners
Physical interface	Radio paths, frequencies, channel use, antenna details, power and host interfaces
Logical interface	Complete encoding, schema, versions, field rules, units, coordinate frames and errors
Test vectors	Valid, invalid, boundary, duplicate, stale, contradictory and unsupported messages with expected outcomes
Timing	Source event, observation, send, receive, validation and output points; clock uncertainty
Acceptance	Per service limits, confidence rules, sample plan and failure conditions
Authority	Trust domains, credential roles, permissions, expiry and revocation behaviour
Data use	Purposes, recipients, retention, access and transfer controls
Failure handling	Detection, degraded operation, fallback, recovery and unavailable state indication
Operations	Monitoring, incident contacts, service dependencies, support period and change triggers
Approval	Applicant approval, technical review, evaluator acceptance and change history

The message package shall be sufficiently detailed for two independent teams to implement the same interface without undocumented bilateral assumptions. This standard does not define a common radio waveform or a complete wire encoding. A claim between different profiles shall therefore require a tested conversion profile and an explicit statement of the functions preserved. Identical service names alone do not establish interoperability.

A2 Module selection

Module	Subject	Application rule
M01	Core connectivity and assurance	All objects; Clauses 1 to 13 and 23 to 28 as applicable to the boundary
M02	V2V functions	Every claimed V2V safety or traffic service; Clause 14
M03	Infrastructure and city interfaces	Every claimed V2I or smart city service; Clause 15
M04	Emergency integration	Every emergency communication or responder integration claim; Clause 17
M05	Vulnerable road users	Every connected VRU function; Clause 16
M06	Cloud edge and connected services	Every remote processing, API or account dependent service; Clause 18
M07	Advanced cooperative functions	Shared perception, manoeuvre coordination or remote assistance; Clause 19
M08	User interaction	Every human facing function; Clause 20
M09	Lifecycle and operations	All objects with boundary appropriate responsibilities; Clauses 21, 22 and 29
M10	Emerging capability extension	Every future technology claim beyond the frozen baseline; Clause 30 and Annex H

A complete connected vehicle and ecosystem claim shall include M01, M02, M03, M04, M08 and M09, plus every additional module implemented in the claimed service chain. It shall cover a vehicle integration boundary and its declared external ecosystem dependencies. A limited component, service or infrastructure result is permitted, but shall identify the object and modules immediately beside the claim. Missing emergency or V2V functionality shall therefore yield a limited scope result rather than an unqualified complete claim.

A3 Minimum service contract

For each service the applicant shall record a unique service identifier; purpose and intended users; initiating event; eligible opportunity definition; input sources; source authority; receiver action; timing and freshness limits; spatial relevance; required availability; privacy controls; failure response; test cases; operational indicators; and responsible parties. The same identifier shall be used in evidence and the public record.

For event-driven services, the definition shall specify when a new event starts, how it differs from a retransmission, how it ends and how cancellation propagates. For periodic services, it shall specify the expected generation interval, permissible variation and behaviour when the source has no valid observation. For transactional services, it shall define idempotency and when the user may regard a transaction as accepted.

A4 Applicability record

The applicability register shall identify each requirement and selected annex obligation, its applicability and reason, evidence, result, reviewer and date. Module summaries shall not replace this traceability. Changes to exclusions shall be reviewed for their effect on scope and public claims.

Annex B Metrics, benchmarks and statistical decisions

Normative within the proposed draft

B1 Measurement boundaries

Every measurement shall distinguish the original observation, event detection, sender application input, radio transmission where observable, receiver delivery, security and semantic acceptance, and application output. The report shall state which intermediate times were directly measured and which were inferred.

Transport latency is the elapsed time between the profile's sender and receiver interface points. End-to-end latency begins at the source event or observation defined in the service contract and ends at the usable output. Age of information begins at the observation represented by the data, not at retransmission or forwarding. Human response and vehicle actuation shall be added where the safety budget depends on them.

If clocks are not synchronised sufficiently for one-way measurement, the evaluator shall use another validated method or report the measurement as inconclusive. Half of round-trip time shall not be reported as measured one-way latency without validating path symmetry and processing effects.

B2 Draft reference classes

The following are proposed starting points for pilot comparison under the conditions in B3. They are deliberately defined as candidate IAF benchmark values and require validation under Annex J. They are not universal safety thresholds. A risk derived limit that is stricter shall apply. A weaker result may be reported descriptively but shall not pass the selected reference class.

Class	Intended comparison	Transport P99 ceiling	Source age ceiling at use	Timely valid delivery floor
REF I	Nonurgent informational service	2000 ms	60 s	99.0 percent
REF T	Time sensitive traffic advisory	500 ms	1000 ms	99.0 percent
REF W	Rapid hazard warning input	100 ms	200 ms	99.9 percent
REF C	Cooperative motion or remote control	Derived for each application	Derived for each application	Derived for each application
REF E	Emergency end-to-end service	Defined by routing and receiver agreement	Defined for each data item	Defined by the complete service contract

REF W concerns a communication input, not proof that a warning or control function is safe. Information older than its source-age ceiling shall be rejected or explicitly downgraded before actionable use. Such an opportunity counts as a delivery failure for the selected class. For REF I, REF T and REF W, timely valid delivery shall satisfy the transport deadline equal to the listed transport ceiling, the listed source-age ceiling and any stricter application deadline, after the declared uncertainty allowances are applied. The conditional P99 test and the timely valid delivery floor are separate checks; both shall pass. A class without a complete acceptance contract cannot receive a pass result. No generic number in this table qualifies REF C or REF E.

B3 Reference workload and stress conditions

The profile shall freeze the production payload and security overhead, generation rules, participant population, topology and background traffic. A periodic reference stream may use 10 messages per second with a 300 byte application payload solely for reproducible pilot comparison; the report shall also test actual production traffic and shall identify the reference stream as synthetic. Protocols that cannot support this stream shall use their declared production stream and shall not claim an identical workload comparison.

Baseline, declared peak load and controlled overload shall each be exercised. As a draft minimum, controlled overload shall offer 120 percent of the declared peak application input rate for 10 minutes in a protected test environment. This is a test stress proposal, not a permission to exceed legal radio limits. The evaluator shall observe whether rate control, shedding and recovery preserve the safety boundary. Normal service performance is required inside the claimed domain; overload beyond that domain requires controlled degradation and recovery.

Outage injections shall include 100 ms, 1 s, 10 s and 60 s where meaningful, plus an outage exceeding the declared maximum tolerable duration. The programme shall also include the specific burst and timing boundaries found in the hazard analysis. Each failure transition shall be exercised at least 30 times per selected critical stratum as a screening minimum, with additional trials required by the statistical acceptance rule. Thirty trials do not demonstrate a 99.9 percent success claim.

B4 Required metric definitions

Metric	Required computation or observation
Timely valid delivery ratio	Number of eligible opportunities producing the correct validated delivery before its deadline divided by all eligible opportunities
Conditional latency percentile	Percentile among delivered observations, with late and missing counts reported alongside it
Age at use	Receiver use time less original observation time, including clock uncertainty
Application success	Eligible hazard or service events with the correct outcome within the application deadline divided by all eligible events
Miss rate	Eligible events without the required application outcome divided by all eligible events
Nuisance activation rate	Unnecessary activations divided by declared nonhazard exposure, such as operating hours or independent negative scenarios
Availability	Eligible demand time with usable service inside all mandatory limits divided by total eligible demand time
Outage duration	Time from loss of required service until verified restoration of the same service level
Recovery time	Time from removal of the injected fault to verified restoration, separately from fault detection time
Position error	Difference from independent ground truth, with coordinate frame and error distribution stated
Warning cancellation delay	Time from the defined event end to removal or valid replacement of the warning
Security misuse outcome	Whether unauthorised input reached a protected action, and whether containment met its deadline
Energy per service outcome	Measured energy within the declared boundary divided by successfully completed service outcomes

One broadcast event may create several eligible receiver opportunities if the profile defines them in advance. Correlation among those receivers shall be accounted for. Duplicates shall not increase the success numerator. Rejected malformed test inputs shall be recorded in the robustness population rather than silently mixed with valid delivery opportunities. A malformed production message required for an eligible event counts as failure of that event.

B5 Sample size and confidence

For a success fraction, the default decision confidence shall be a one-sided 95 percent exact binomial bound when trials are reasonably independent with a stable success probability. The evaluator shall state the assumptions. A justified alternative shall be fixed before testing where clustering or changing conditions require a different model.

For zero observed failures in n independent trials, the one-sided 95 percent lower confidence bound for success equals the n th root of 0.05. Consequently, at least 299 independent successes with zero failures are needed to support a 99.0 percent floor, and at least 2995 are needed to support a 99.9 percent floor. These are statistical calculations, not proposed road safety targets. With failures, the exact bound shall be recalculated; collecting a nominal count alone is insufficient. For k successes among n independent trials, with k greater than zero, the lower bound is the 0.05 quantile of the beta distribution with shape parameters k and n minus k plus one. With zero successes, the lower bound is zero. These are fixed-sample rules unless the approved analysis includes a valid sequential design.

The acceptance population shall be specified before testing. Each critical stratum for which the success floor is claimed shall meet its own rule, or a justified simultaneous analysis shall control the stated error rate across strata. Pooling easy and difficult conditions shall not hide a failed critical condition. Independent journeys, resets or blocks shall be used where consecutive transmissions share persistent channel, source or processing conditions.

Percentile reporting shall state the estimator and an uncertainty interval appropriate to the sample dependence. Fewer than 100 delivered observations cannot adequately characterise an empirical P99 tail. Having 100 or more observations does not by itself establish adequate precision; the interval width and dependence assumptions shall also support the decision. Even a large conditional latency sample shall not replace the timely delivery confidence test.

B6 Measurement uncertainty and decision rules

The uncertainty budget shall include clock alignment, timestamp placement, reference equipment, quantisation, sampling, processing instrumentation and analysis. Uncertainty shall be small enough to distinguish the decision from the limit. If it is not, the result is inconclusive.

For a maximum latency limit, the chosen upper confidence and measurement uncertainty allowance shall remain within the limit. For a minimum delivery ratio, the lower confidence bound shall meet the floor. The evaluator shall avoid double counting the same uncertainty component and shall document how statistical and measurement uncertainty are combined.

Zero observed unsafe actions is a necessary condition in tests designed to expose a prohibited action. It shall not be described as proof of a zero real world failure rate. A critical unsafe action shall fail the relevant safety gate regardless of a favourable aggregate success ratio.

B7 Reliability observation

An availability claim shall have a predeclared exposure period, monitoring resolution, eligible time definition and outage classification. As a draft field evidence minimum, a continuously operated ecosystem service shall be observed for at least 30 consecutive days including relevant peak periods. This minimum is for coverage and does not, by itself, establish a rare outage probability or an annual service level.

Mean values shall be accompanied by maximum observed outage, duration distribution, service region and monitoring gaps. A 99.9 percent availability objective, if selected by the profile, shall be demonstrated over the stated observation window and shall not automatically be extrapolated to a year.

Annex C Scenario catalogue and test methods

Normative within the proposed draft

C1 Scenario selection and coverage

The evaluator shall screen every scenario below against the declared scope. The catalogue is a minimum coverage framework, not an exhaustive list of all hazards. The hazard analysis shall add scenarios where the architecture, road environment or failure mechanism is not represented.

ID	Scenario family	Principal evidence
S01	Unobstructed approach at lower and upper domain speeds	Timely delivery and application deadline
S02	Obstructed intersection with crossing traffic	Relevance and warning effectiveness
S03	Abrupt deceleration behind an occluding vehicle	Source to warning timing and miss rate
S04	Stationary vehicle or queue around a bend	Event extent and early warning limits
S05	Wrong way vehicle on divided roads	Direction discrimination and false warnings
S06	Merge or lane change with mixed participants	Conflict prediction and unavailable data behaviour
S07	Bridge above a road or adjacent tunnel	Road level and lane association
S08	Adaptive traffic signal timing	Signal age and geometry binding
S09	Signal and map version mismatch	Rejection and controlled unavailable state
S10	Roadworks and moving maintenance vehicles	Temporary event lifecycle and cancellation
S11	Closure or reversible lane transition	Authority and effective time handling
S12	Emergency vehicle priority request	Role permission and grant confirmation
S13	Pedestrian crossing from occlusion	Detection, relevance and uncertainty
S14	Cyclist or mobility aid with poor device placement	Radio and user performance limitations
S15	Road user without transmitting equipment	Absence handling and safety assumptions
S16	Dense crowd or many devices per person	Duplicate identity and congestion behaviour
S17	Dense traffic and competing services	Priority, capacity and tail latency
S18	Mobile network or edge handover	Session continuity and command age
S19	Tunnel or urban canyon	Position integrity and fallback
S20	Controlled positioning or time spoofing	Detection, false confidence and containment
S21	Drift, time reset or timestamp wrap	Freshness checks and event ordering
S22	Burst loss and sustained outage	Detection, degraded state and recovery

ID	Scenario family	Principal evidence
S23	Shared backhaul or power failure	Common cause exposure
S24	Cloud region loss or stale replica	Service correctness after recovery
S25	Credential expiry or mass revocation	Trust continuity and permission enforcement
S26	Replay, duplicate or reordered event	Suppression and bounded action
S27	Signed but implausible or conflicting data	Content validation and trust handling
S28	Malformed messages and resource exhaustion	Isolation, availability and parser behaviour
S29	Gateway conversion between profiles	Semantic equivalence and source age
S30	OTA interruption or bad target package	Integrity, recovery and authority
S31	Mixed software or trust versions	Compatibility and downgrade protection
S32	Emergency call with poor location or power loss	End-to-end acceptance and user status
S33	Duplicate emergency triggers or responder rejection	Retry, cancellation and failure indication
S34	Ownership transfer or rental return	Access revocation and data separation
S35	Antenna repair or RSU relocation	Requalification and profile identity
S36	Temperature, vibration or electrical disturbance	Communication before and after exposure
S37	Long parking and repeated failed reconnect	Energy use and essential reserve
S38	Cross-border or operator transition	Legal profile, trust and service compatibility
S39	Cooperative perception with correlated reports	Object fusion and false confidence
S40	Manoeuvre cancellation or platoon member loss	State agreement and safe separation
S41	Remote assistance operator or video loss	Local authority and stale command rejection
S42	AI distribution shift or misleading input	Performance limits and safe rejection
S43	Satellite blockage or delayed delivery	Service class limits and receiver status
S44	Disaster load and emergency traffic surge	Priority, retry control and degraded service
S45	Service provider closure or network retirement	Migration and supported fallback
S46	Malicious or mistaken misbehaviour reports	Legitimate participant protection and review
S47	Charging parking or toll transaction interruption	Identity, duplicate prevention and reconciliation
S48	Nuisance alerts under high driver workload	Comprehension, distraction and suppression

C2 Common test record

Each executed test shall record test identifier, requirements, profile revision, selected scenario, hypotheses, configuration, tools, calibration, clock alignment, environment, payload, load, test population, repetitions, acceptance rule, raw evidence identifiers, observed results, deviations and reviewer. The evaluator shall retain both valid failed runs and successful retests.

The programme shall maintain a matrix linking each requirement to its scenario, test method, configuration, evidence and result. A design review may close a documentary requirement; it shall not replace a required performance test. Multiple methods may support one requirement. Every failed or inconclusive critical scenario shall receive a documented disposition before the decision review.

The following method cards define minimum procedural steps. The binding profile shall add exact signal levels, messages, coordinates, traffic timings and application criteria. A method card with missing acceptance parameters cannot be used to issue a positive result.

T01 Message semantics and conversion

Applies to Clauses 9 and 10 and scenarios S09, S21, S26, S29 and S31. Configure the sender and receiver to the frozen profile. Inject every message type with nominal, minimum, maximum, unknown, missing and invalid values. Exercise units, coordinate frame, time base, version and extension handling. For gateways, compare original and converted meaning using independent decoding.

Record accepted values, rejections, source age, provenance and resulting application outputs. Pass only if every mandatory vector produces the specified interpretation or rejection, no stale value is made current and no unauthorised output occurs. Unsupported semantics shall produce an explicit limited or unavailable state.

T02 Independent interoperability

Applies to Clauses 4, 9 and 25. Construct the full claimed sender and receiver matrix, including distinct implementations, directions and versions. Run normal service exchanges, boundary vectors, cancellation and reconnect cases for every applicable pair. Repeat with production security and representative load.

Record implementation diversity and shared dependencies. Pass only if all mandatory semantic cases pass and each claimed pair meets its selected performance rule. Unavailable counterparts shall remain a documented limitation rather than a simulated multi-vendor success.

T03 Timing and congestion

Applies to Clauses 8, 10 and 23 and scenarios S01, S17 and S18. Align instrumentation, validate timestamp boundaries and run baseline and peak production workloads. Inject the overload in Annex B in a protected environment. Repeat across the domain conditions and critical strata selected before testing.

Record all eligible opportunities, accepted and rejected deliveries, conditional latency, age at use, application outcomes and queue state. Pass the performance portion only within the claimed domain and its confidence rules. During beyond domain overload, pass the resilience portion only if the declared degraded behaviour and safe boundary are maintained.

T04 Connectivity loss and recovery

Applies to Clauses 6, 7 and 23. Interrupt each relevant path for the durations in Annex B and for the hazard derived boundary cases. Inject common cause loss of shared power, backhaul or trust service. Restore each dependency in different orders and with old data waiting in queues.

Measure detection, unavailable indication, fallback and recovery times. Pass only if prohibited actions do not occur, stale information is not released as current and recovered service authority is revalidated. An unsafe transition fails even if steady state operation before and after the fault meets its targets.

T05 Time and position integrity

Applies to Clause 10 and scenarios S07, S19, S20 and S21. Use independent ground truth to vary position and time error within and beyond the declared integrity limits. Exercise geometry ambiguity, drift, resets, loss of reference and controlled deceptive input in an authorised environment.

Record actual error, reported uncertainty, detection time, missed detections, false alarms and receiver action. Pass only if the system meets the profile's error bounds when claiming valid output and enters its required limited state when integrity cannot be supported.

T06 Trust and security boundaries

Applies to Clauses 11 and 12. Present valid, expired, revoked, unknown and wrong role credentials; replay valid messages in a new context; and inject signed implausible content. Exercise parser and resource stress against authorised test targets. Attempt permitted laboratory checks of isolation between noncritical and protected domains.

Record permission decisions, protected outputs, detection and containment times, service effects and evidence integrity. Pass only if all mandatory rejection rules operate, no unapproved authority crosses a boundary and required service or controlled fallback is preserved. A valid signature on false content shall not bypass application checks.

T07 Traffic and infrastructure integration

Applies to Clause 15 and scenarios S08 to S12. Connect the assessed system to a controlled traffic controller or validated equivalent. Vary actual signal phases, geometry versions, temporary restrictions and priority permissions. Introduce stale maps, inconsistent states and operator maintenance conditions.

Record the authoritative state, transmitted state, vehicle interpretation and status shown to users. Pass only if the correct movement and validity are established, stale or conflicting instructions are withheld and priority is not assumed without a valid grant. Field scope requires evidence of the actual deployment interface as well as a bench result.

T08 Emergency delivery

Applies to Clause 17. Trigger manual and simulated automatic emergency events through an authorised test receiving endpoint. Include poor location, primary power loss, blocked path, roaming, rejection, retry and duplicate triggers. Use the production data and security configuration.

Record trigger, routing attempt, receiver acceptance, available communication channel, location quality and user status. Pass only if the complete declared service contract is met and failures are truthfully indicated. A simulated responder result shall retain its simulated label.

T09 Update and configuration recovery

Applies to Clauses 21 and 22 and scenarios S30, S31 and S35. Test authentic and unauthorised packages, wrong target, interruption at installation stages, power variation and recovery. Repeat interoperability and timing checks on the restored state and the intended final state.

Record installed versions, integrity evidence, recovery action and population controls. Pass only if the system reaches an authorised recoverable state, does not restore prohibited vulnerabilities and preserves the required safety boundary. Installation success alone is insufficient.

T10 Privacy and ownership lifecycle

Applies to Clause 13 and scenario S34. Execute enrolment, optional consent choices, withdrawal, rental return, sale and account removal. Attempt authorised test access using the former user's credentials and examine controlled traces of data flows and stored records.

Pass only if permissions and data handling match the declared policy, a former user cannot access subsequent activity, and required deletion or retention is verifiable. Evidence supplied to the evaluator shall minimise personal information.

T11 Cooperative and remote functions

Applies to Clause 19 and scenarios S39 to S41. Inject correlated perception, contradictory tracks, participant departure, cancelled commitments and delayed remote commands. Remove operator availability, video, timing and network access separately and in selected common cause combinations.

Record source lineage, commitment state, local authority and motion related outputs. Pass only against the application specific safety and performance limits, with no residual stale command authority. Generic REF W timing is insufficient for this test.

T12 Human and field validation

Applies to Clauses 16, 20, 25 and 29. Observe representative users and deployed conditions through a predeclared programme. Include relevant peak loads, low participation, nuisance alerts, service outages and status transitions. Use controlled methods for hazards unsuitable for public road testing.

Record participant coverage, task completion, misunderstandings, unsafe responses, exposure and operational indicators. Pass only if the profile's usability and field criteria are met with sufficient evidence. State the demographic, geographic and seasonal limitations of the observation.

T13 Environment, power and installed equipment

Applies to Clauses 8, 22 and 24 and scenarios S23, S35, S36 and S37. Test the installed equipment or a justified representative assembly at the environmental and electrical severities fixed in the profile. Include antenna or cable disturbance, supply variation, low battery, sleep and wake cycles, declared emergency reserve and communication under thermal or mechanical stress where applicable.

Record communication performance, integrity checks, power consumption, reserve capability and recovery before, during where practicable and after exposure. Pass only if the declared performance or controlled fallback is maintained, installation assumptions remain valid and latent faults do not leave a falsely healthy service indication. Physical survival alone shall not establish functional conformity.

T14 Complete application outcome

Applies to Clauses 6, 14 to 20, 23 and 26. For each claimed service, execute independent positive events, negative events and boundary conditions using verified ground truth. Measure source observation, validated receiver information and the required application outcome. Include event cancellation, contradictory inputs, nonparticipating road users and irrelevant nearby events where applicable.

Record timely correct outcomes, missed outcomes, nuisance activations, cancellation delay and any prohibited action. Use the application-specific acceptance limits and statistical plan. Pass only if all mandatory outcome and failure-response criteria are met. A successful message reception or a favourable network percentile shall not substitute for the required application outcome.

C3 Verification routing

The evaluator shall use the following routing as a starting point and add evidence where necessary. Documentary requirements still require record review. A route to a method is not evidence that the requirement has passed.

Requirement area	Principal methods	Additional evidence
Scope governance and architecture	T02 T04 T06	Profiles, responsibilities and risk records
Radio timing and semantic integrity	T01 T02 T03 T05	Calibration and uncertainty budgets
Trust cybersecurity and APIs	T01 T04 T06 T09	Threat analysis and administrative access tests
Privacy and ownership	T10	Data flow, retention and access records
V2V infrastructure and VRU outcomes	T07 T12 T14	Ground truth and service-specific limits
Emergency integration	T04 T08 T13 T14	Receiver agreement and complete outcome criteria
Cooperative and remote functions	T05 T06 T11 T14	Control authority and application safety case
Human interaction	T12 T14	Participant coverage and comprehension findings
Updates lifecycle and operations	T04 T09 T10 T13	Support, incident and reassessment records
Physical environment and energy	T03 T13	Exposure severities and energy boundaries
Quantitative decisions	T03 T12 T14	Sampling, raw data and independent analysis
Emerging capabilities	Applicable methods plus extension tests	Annex H extension package

Annex D Evaluation workflow and evidence descriptors

Normative within the proposed draft

D1 Evaluation stages

Stage	Required output	Condition to proceed
1 Scope review	Object, modules, domain and obligations register	Claim is bounded and responsibilities are allocated
2 Profile review	Complete binding profile and applicability register	Interfaces and acceptance criteria are testable
3 Design review	Hazard, threat, privacy and architecture evidence	Uncontrolled hazards are resolved for testing
4 Controlled testing	Bench, simulation, track and fault results	Mandatory controlled test requirements pass
5 Interoperability	Independent pair and version matrix	Claimed combinations pass or scope is explicitly limited
6 Field validation	Representative operational and human evidence	Field criteria and evidence coverage are met
7 Findings closure	Corrections and regression evidence	All applicable nonconformities are closed
8 Independent decision	Reviewed statement with scope and limitations	Applicable requirements pass and evidence is sufficient
9 Continuing review	Operational indicators and change dispositions	Public status remains accurate for the current scope

Stages may overlap when doing so does not bypass a required safety or evidence condition. An infrastructure or component scope may use integration evidence from a representative host, but the result shall state that host and the installation limits. A complete ecosystem result requires evidence through the actual service chain.

D2 Evidence descriptors

The report shall use the following descriptors independently. They identify the kind of evidence available and are not a ranking of product quality.

Descriptor	Meaning	Limitation
Design reviewed	Requirements and design records examined	Does not show runtime performance
Bench demonstrated	Controlled functional and robustness tests completed	Does not establish field suitability by itself
Interoperability demonstrated	Named independent implementation pairs tested	Does not cover untested pairs or profiles

Descriptor	Meaning	Limitation
Field demonstrated	Identified deployment conditions observed	Does not cover every geography or season
Operationally monitored	Indicators observed for a stated period	Depends on monitored scope, resolution and changes

D3 Mandatory decision gates

The decision review shall confirm that scope and identity are accurate; every safety-relevant dependency is addressed; authority and privacy boundaries are enforced; required messages retain their meaning; critical failure responses are demonstrated; performance limits meet their decision rules; and all mandatory evidence is traceable.

Any failed gate blocks a positive result for the affected scope. The authority may issue a limited scope result only when the limitation is technically justified, the excluded function is isolated and the public wording cannot imply the excluded capability. An unresolved flaw in a shared core component cannot be removed by changing only the marketing description.

D4 Findings and outcome vocabulary

Status	Required interpretation
Pass	Applicable provision meets its acceptance rule with sufficient evidence
Fail	Applicable provision is not met
Inconclusive	Available evidence or uncertainty does not permit a decision
Not assessed	Applicable provision has not yet been evaluated
Not applicable	Verified scope justification excludes the provision under Clause 2
Positive scoped decision	All applicable mandatory requirements pass for the stated scope
Negative decision	One or more applicable mandatory requirements fail
Decision deferred	Required evidence or findings closure is incomplete
Suspended	Previously positive claim is temporarily withheld because its continued validity is in doubt
Withdrawn	Claim is no longer authorised for the stated scope

During development, these shall be prefixed by pilot where an actual pilot is conducted. No pilot result shall imply scheme authorisation that has not been granted.

Annex E Risk and assurance worksheets

Normative within the proposed draft

E1 Hazard record fields

Every hazard record shall identify the service and operating condition, initiating event, affected people or assets, unsafe outcome, severity rationale, exposure, likelihood evidence where available, detection and controllability, controls, residual risk, verification and responsible acceptance. Numerical risk scores may organise work but shall not override a credible severe hazard merely because its probability is unknown.

Field	Required entry
Hazard identifier	Stable identifier linked to the service and profile
Cause and condition	Fault, misuse, incorrect data or domain condition initiating the hazard
Consequence	Observable unsafe or harmful outcome
Existing assumptions	Participant, sensor, operator, network and infrastructure assumptions
Control allocation	Prevention, detection, containment and fallback with owners
Time and integrity budget	Maximum acceptable age, error, detection delay and response delay
Verification	Test scenario, method, acceptance limit and evidence
Residual decision	Remaining limitations, responsible acceptance and review triggers

E2 Required hazard prompts

The following records are prompts for analysis, not completed product risk assessments. Each applicable prompt shall be evaluated for the actual architecture and domain.

Prompt	Example unsafe outcome	Control and evidence to examine
H01 Stale event replay	Unnecessary abrupt response after the hazard ended	Original time preservation, expiry and cancellation tests
H02 Wrong lane or road level	Warning or priority applied to the wrong movement	Survey, coordinate checks and S07
H03 Signed false information	Incorrect action despite valid authentication	Plausibility, independent context and S27
H04 Missing participant	System assumes an unconnected person is absent	No absence inference and S15
H05 Shared communications failure	Redundant paths fail at the same time	Common cause analysis and S23
H06 Credential service outage	Unsafe bypass of trust checks	Bounded offline policy and S25
H07 Correlated perception reports	Artificially inflated confidence	Source lineage and S39

Prompt	Example unsafe outcome	Control and evidence to examine
H08 Delayed remote command	Movement authorised in an obsolete situation	Command expiry, local constraints and S41
H09 Emergency delivery ambiguity	Occupant believes help has been summoned when it has not	Distinct acceptance status and S32 to S33
H10 Software update mismatch	Previously compatible systems disagree	Version matrix and S30 to S31
H11 Previous owner access	Location disclosure or unauthorised remote action	Transfer revocation and S34
H12 Congestion induced starvation	Warning deadline missed during peak traffic	Priority, admission control and S17
H13 Service retirement	Essential function disappears without a safe transition	Support declaration and S45
H14 Unclear service status	Driver relies on unavailable connectivity	User comprehension and S48
H15 Malicious false reports	Legitimate road users are excluded from cooperation	Reviewed misbehaviour decisions and S46

E3 Safety argument structure

For every safety-relevant claim, the applicant shall state the top level claim, its operating assumptions, the reasoning connecting controls to risk reduction, the evidence for each control and remaining uncertainty. Arguments shall identify independence assumptions and information that can invalidate the conclusion.

The evaluator shall challenge at least the source correctness assumption, the communication availability assumption, the receiver interpretation assumption and the fallback feasibility assumption. A list of implemented controls without evidence of their effectiveness is not a complete assurance argument.

E4 Threat and privacy linkage

The threat analysis shall connect misuse of identity, message content, configuration and service administration to the hazard records. The privacy analysis shall connect data categories and recipient permissions to misuse or disclosure consequences. Conflicting controls shall be resolved explicitly; for example, accountability logging shall not justify unlimited retention of identifiable journeys.

Annex F Evidence package and public record

Normative within the proposed draft

F1 Controlled evidence index

Record	Minimum content
E01 Application	Applicant, object, claim and requested scope
E02 Binding profile	Complete Annex A package with controlled revisions
E03 Applicability	Provision level decisions and reasons
E04 Architecture	Interfaces, owners, dependencies and trust boundaries
E05 Risk analyses	Hazard, threat, privacy and residual decisions
E06 Test plan	Methods, scenarios, acceptance limits and sampling
E07 Equipment record	Tool versions, calibration and uncertainty
E08 Raw results	Logs, captures, observations, hashes and time basis
E09 Analysis	Reproducible calculations, exclusions and confidence
E10 Interoperability	Implementation pairs, diversity and compatibility results
E11 Human and field evidence	Participants, routes, exposure, conditions and limits
E12 Findings	Failures, cause analysis, corrections and regression
E13 Decision	Independent review, outcome and authorised wording
E14 Operational plan	Monitoring, incident response, support and retirement
E15 Change record	Release history, impact assessments and reassessment

Every index entry shall have an identifier, revision, owner, creation date, access classification, integrity identifier, retention rule and link to applicable requirements. A missing record shall be justified by the assessed boundary rather than left ambiguous.

F2 Assessment report structure

The report shall state its status and conclusion first, followed by scope, configurations, profile, limitations, methods, quantitative findings, qualitative findings, deviations, nonconformities, corrective actions and decision. It shall state whether the system was operated with production security and whether field endpoints were operational or simulated.

The report shall identify the evidence reviewed directly and the evidence supplied by another party. It shall disclose limitations that affect independence or replication. A digest or summary may accompany the report but shall not replace the detailed evidence needed for authorised review.

F3 Connectivity assurance record fields

Public field	Required value
Record identifier	Unique controlled identifier assigned by an authorised scheme process
Status	Pilot, positive scoped decision, suspended, withdrawn or other defined status
Standard	IAF CVES and the exact adopted edition or draft revision
Object	V, C, I, S or E with product or deployment description
Configuration	Public version identifier linked to the detailed baseline
Modules	Assessed modules and explicit unavailable or excluded capabilities
Profile	Binding profile identifier and revision
Domain	Geographic and operational limits understandable to users
Evidence	Available descriptors from Annex D and observation period
Performance	Service class and measured results where appropriate, with test conditions
Decision	Date, responsible decision authority and scope
Limitations	Dependencies, unverified conditions and supported combinations
Lifecycle	Support declaration and change or reassessment conditions
Current status source	Authoritative status location if an operational registry exists

The record shall not publish personal route histories, private keys, detailed vulnerabilities or confidential infrastructure credentials. A restricted evidence identifier may be used instead. The machine-readable representation shall use a documented schema and distinguish unknown, not applicable and not assessed values.

F4 Permitted claim pattern

After adoption and a positive authorised decision, a suitable statement is: Evaluated against IAF CVES First Edition for the identified object, modules, profile and operating domain stated in the assessment record. The specific record shall accompany the claim.

Before adoption, the wording shall instead identify a pilot evaluation against IAF CVES Working Draft 0.2 and state that it is not an issued conformity certification. This document supplies the record structure but does not create an actual assessment result.

Annex G Change, incident and reassessment controls

Normative within the proposed draft

G1 Trigger matrix

Trigger	Minimum review and evidence
New vehicle variant or antenna installation	RF performance, host resource effects and integration risks
Message schema or version change	Semantics, all affected pairs and invalid input handling
New radio path or network operator	Domain, timing, outage, roaming and common causes
New city or controller interface	Authority, geometry, signal semantics and field acceptance
Trust anchor or credential policy change	Permission, mixed fleet, expiry and revocation tests
Security vulnerability or compromise	Exposure, containment, correction and regression
Software or AI model release	Behavioural impact, risk review and affected test suite
Cloud region or provider migration	Identity, data route, failover and service correctness
Road geometry or RSU location change	Survey, map binding, relevance and installation checks
New personal data purpose	Necessity, permissions, privacy and user information
Material field performance deterioration	Scope validity, fault cause and decision status
Network or commercial service withdrawal	Support commitments, migration and fallback
Safety incident or credible near miss	Hazard assumptions, affected population and immediate controls

G2 Change decision

The applicant shall classify the change as having no assessed behaviour effect, a bounded effect requiring partial reassessment, or a major effect requiring a new scope or full affected programme. The evaluator shall review the classification. The first category shall have positive evidence of no effect and shall not be selected solely because the release is described as minor.

Partial reassessment shall include shared dependencies and regression effects beyond the directly changed component. The decision record shall identify which evidence remains valid, which is replaced and which public fields change. A new version identifier shall be assigned whenever the assessed baseline changes.

G3 Incident workflow

On receipt of a credible incident, the responsible operator shall determine whether immediate containment is necessary, preserve relevant evidence and identify the potentially affected population. Safety-relevant containment shall proceed without waiting for commercial agreement between suppliers. Notifications shall follow the obligations register and operating agreements.

The incident record shall include detection time with uncertainty, symptom, affected service and profile, initial severity, containment, communication, cause analysis, correction, regression evidence, restoration decision and effectiveness review. Exact reporting and response deadlines shall be defined by risk and applicable duties before deployment.

G4 Restoration criteria

Restoration shall require verification that the unsafe or unauthorised condition is controlled, the correction is deployed to the required population, compatibility is preserved, monitoring is active and users receive any changed instructions. The decision authority shall update a suspended public status only after reviewing sufficient evidence.

Annex H Emerging capability extension requirements

Normative within the proposed draft

H1 Extension package

Every extension shall identify its purpose, technical maturity, supported operating domain, changed assumptions, data and authority boundaries, application safety case, test methods, performance limits, interoperability impact and exit strategy. Demonstrations and prototypes shall remain distinguishable from deployable capability.

Capability	Questions that the extension shall resolve
Next generation terrestrial radio	Which interfaces change, which previous participants remain supported and how are congestion and mixed fleets tested
Satellite or other nonterrestrial links	What are measured coverage, acquisition, delay, blockage and endpoint acceptance limits
Integrated sensing and communications	How are sensing and communication resources shared and how are correlated failures controlled
AI-based message interpretation	What bounds its output, what data supports evaluation and what happens outside the validated distribution
Federated or distributed learning	How are participants authorised, poisoning detected, personal data protected and updates approved
Cooperative perception	How are source age, uncertainty, duplication and common observation lineage preserved
Digital twins and simulation	Which physical behaviours are validated, what model error remains and what cannot be inferred
Remote assistance and operation	Who has current authority, which information is fresh and how does local control respond to lost contact
Quantum-resistant migration	How are larger messages, mixed credentials, processing cost and downgrade attempts handled
Dataspaces and shared mobility records	What defines purpose, access, semantic compatibility, retention and withdrawal
Connected energy and charging services	How are scheduling and payment separated from electrical protection and vehicle safety authority
Disaster resilient connectivity	Which essential services survive, how are priorities enforced and what is unavailable

H2 Evidence maturity

An extension record shall identify whether evidence comes from analytical reasoning, simulation, laboratory demonstration, controlled site trials or deployed operation. A capability demonstrated only in simulation shall not be described as proven under real traffic conditions.

For capabilities that influence safety, the programme shall examine at least one relevant domain boundary, one input integrity failure and one common cause failure. The applicant shall define stop criteria before exposing the capability to broader operation.

H3 Compatibility and change control

Extensions shall not modify the meaning of existing fields or identifiers without versioning and explicit receiver behaviour. Unsupported participants shall receive a safe limited service or an unambiguous refusal. A fallback to a previous algorithm or message version shall not bypass the current security policy.

H4 Future development position

The proposed IAF direction is to evaluate new technology through observable service outcomes, source credibility, interoperability and controlled failure behaviour. Future capabilities may broaden coverage and utility, but forecasts shall remain forecasts until the required evidence is obtained. Publication of a roadmap shall not create a present conformity entitlement.

Annex I Worked evaluation example

Informative

I1 Example scope

This fictional example illustrates the proposed assessment method and reports no actual product or test result. The object is an ecosystem combining an installed passenger vehicle receiver, two independently developed roadside implementations and a traffic warning backend. The service warns of a stationary queue ahead on a declared urban corridor. Emergency integration is absent, so the result can only use a limited scope claim under Annex A.

The profile includes normal urban operation up to a declared 70 km/h, specific road geometry, installed antennas and measured network conditions. It excludes automated braking and remote driving. A separate onboard function remains responsible for the vehicle's general collision response; the connected warning does not indicate that an unconnected road user is absent.

I2 Illustrative timing allocation

Suppose the design team allocates 800 ms from observation of a qualifying queue event to a driver warning. This is an assumed design allocation for the example, not a safe response time for a real vehicle.

Stage	Illustrative allocation
Source observation and event detection	250 ms
Message preparation and dispatch	80 ms
Transport	100 ms
Receiver validation and relevance	70 ms
Warning presentation	100 ms
Engineering margin	200 ms
Total	800 ms

The communication portion resembles REF W, but the full source-age ceiling of REF W would not automatically be met because the source detection and preparation stages already consume 330 ms. The evaluator must therefore examine observation semantics and cannot assign REF W from transport latency alone. The team must reduce those delays, select a different justified service contract or report that the class is not met. This example deliberately shows why every time boundary matters.

Human reaction and braking distance are outside this 800 ms warning generation budget. A real safety claim would also analyse approach speed, queue visibility, road friction, driver behaviour, available distance and the hazards of unnecessary warnings.

I3 Illustrative statistical decision

Suppose 3000 genuinely independent eligible opportunities all produce timely valid delivery. The one-sided 95 percent lower success bound is approximately 99.9002 percent, so the sample narrowly supports a 99.9 percent communication delivery floor for that defined population. If the observations were consecutive packets in one persistent channel condition, independence would not be established and that conclusion would not follow.

Even with this delivery result, a failed stale message rejection test would block a positive decision. Likewise, missing independent infrastructure pairs, insufficient field exposure or an inconclusive timing uncertainty result would prevent an unqualified claim.

I4 Example limited claim

A future authorised limited claim could state the assessed queue warning service, object code E, the specific modules, binding profile, corridor domain, software baseline and evidence period. It would disclose the absence of emergency integration and would not state that the complete vehicle ecosystem meets all modules or that it works with every city.

Annex J Development, validation and publication register

Informative development material

J1 Purpose

This register identifies work needed to turn the proposed requirements into a credible adopted standard and an operational evaluation programme. It distinguishes drafting completion from technical validation and institutional adoption.

Work item	Required output before operational publication	Current draft state
J01 Designation and scope approval	Approved name, ownership and intended scope	Proposed IAF CVES
J02 Technical committee review	Reviewed clauses and resolved technical comments	Review required
J03 Deployment profiles	Complete wire profiles and executable conformance vectors for selected markets	Structure supplied; actual profiles required
J04 Numerical calibration	Pilot evidence supporting or revising Annex B values	Candidate values only
J05 Safety review	Independent review of budgets, fallback and advanced functions	Method supplied; application evidence required
J06 Interlaboratory repeatability	Independent laboratories evaluating common systems and discrepancies	Protocol planning required
J07 Interoperability pilot	Diverse senders, receivers, infrastructure and backend combinations	Pilot execution required
J08 Field representativeness	Evidence across relevant roads, traffic, users and environmental conditions	Programme design required
J09 Security and privacy review	Technical validation of threat coverage and data controls	Review required
J10 Statistical review	Confirmation of dependence models and decision rules	Draft method supplied
J11 Scheme governance	Competence, impartiality, decisions, appeals and status policies	Proposed structure supplied
J12 Public records and mark rules	Approved wording, registry operation if selected and permissions	No active scheme created
J13 Obligations and rights review	Market duties and implementation licensing assessment	Deployment specific review required
J14 Consultation and comment closure	Stakeholder feedback, dispositions and final consistency check	Consultation required
J15 Formal adoption	Authorised decision, release date, controlled edition and transition rules	Not adopted

J2 Suggested pilot programme

The initial pilot should cover a vehicle integration, a roadside installation and an ecosystem service chain, with at least two independent counterpart implementations for each claimed interface role. It should include an urban intersection, an obstructed hazard warning and a network loss or trust failure case. These pilot choices are recommendations for learning and do not reduce the full applicability obligations.

The pilot should compare evaluator interpretations, configuration effort, measurement uncertainty, reproducibility, false positives, missed events and practical access to evidence. Proposed benchmark values should be retained, tightened or changed only after reviewing the relationship between measured outcomes and the intended service use.

J3 Comment and change register

Comment field	Required review content
Identifier	Unique comment number and draft revision
Location	Clause, requirement, table row or test method
Issue	Specific ambiguity, omission, inconsistency or unsupported parameter
Proposed change	Replacement wording or method with a technical reason
Evidence	Pilot result, analysis or operational observation
Disposition	Accepted, revised, deferred or rejected with a reason
Closure	Responsible reviewer, decision date and resulting revision

J4 Publication readiness

The drafting team should verify that every shall is testable, every threshold has a rationale and measurement rule, every permitted exclusion preserves a truthful scope, every future technology claim states its maturity and every annex reference is correct. The final release should include the approved profile process, competent evaluation capacity and a clear public explanation of what an IAF CVES result means.

The intended contribution is a consistent way to connect device performance, vehicle integration, infrastructure behaviour, source credibility and continuing service responsibility within one assessment. Recognition will depend on adoption, technically credible implementation and demonstrated use; it is an objective of the programme rather than an existing fact asserted by this draft.