



FIRST EDITION

IAF DIGITAL SYSTEMS INTEGRITY

Cyber resilience and secure development
Update integrity and privacy

Connected vehicles and digital platforms
Lifecycle assurance and evidence-based conformity

DRAFT FOR TECHNICAL REVIEW

Technical review, industry consultation and pilot assessment precede formal adoption.
This proposed edition does not itself authorize conformity claims.

International Automotive Federation

English master text | 13 September 2026

iaf.com

Publication identity

IAF Digital Systems Integrity First Edition

Cyber resilience, secure software development, update integrity and privacy

International Automotive Federation

English master text | 13 September 2026

www.iaf.com

Foreword

IAF Digital Systems Integrity defines requirements for maintaining trustworthy digital behaviour throughout the automotive lifecycle. It brings vehicle electronics, software, connected services, artificial intelligence, update infrastructure and personal data processing into one evidence-based assessment boundary. Its intended outcome is that a digital compromise is prevented where practicable, contained when prevention fails, and recovered from without creating unacceptable physical or privacy harm.

This proposed First Edition is submitted for IAF technical review, industry consultation and pilot assessment. Publication and scheme approval are separate decisions. No conformity decision is created by this document itself. The numerical criteria in this text are proposed IAF requirements; they are not measurements of industry performance or claims of universal scientific thresholds.

The standard is written for vehicle manufacturers, component and software suppliers, platform operators, mobility providers, fleet operators, engineering organizations and assessment teams. Responsibilities follow control over the product and service, while the system integrator retains responsibility for the complete declared scope.

Document structure

Clauses 1 to 26 set the scope, technical requirements and conformity rules.

Annexes A to C provide the mandatory evidence register, 32 verification cases and acceptance parameters.

Annexes D to F provide worked examples, implementation records and future technology scenarios.

Contents

Select a section to navigate to it.

1 Scope and intended outcomes	4
2 Interpretation and mandatory rules	4
3 Terms and abbreviations	5
4 Scope declaration and integrity profiles	6
5 Governance and engineering accountability	7
6 Threat analysis and risk decisions	8
7 Asset identity and digital configuration	9
8 Architecture and trust boundaries	10
9 Identity cryptography and trust renewal	10
10 Secure software development	11
11 Build and release provenance	12
12 Supplier and service dependencies	13
13 OTA and other update integrity	13
14 Cloud mobile applications and remote operations	14
15 Privacy and responsible data use	15
16 Cyber resilience and safe recovery	16
17 Vulnerability handling and corrective updates	17
18 Monitoring incident response and evidence	17
19 Artificial intelligence and adaptive software integrity	18
20 Connected interfaces and automated mobility	19
21 Production diagnostics repair and transfer	20
22 Support continuity and end of life	20
23 Verification and technical assessment	21
24 Conformity decisions and change control	22
25 Digital integrity passport and transparency	23
26 Performance review and technology evolution	23
Annex A Required evidence register	25
Annex B Minimum verification catalogue	27
Annex C Acceptance parameters and response limits	34
Annex D Worked risk and scope examples	37
Annex E Example implementation records	38
Annex F Forward technology scenarios	40

1 Scope and intended outcomes

This standard specifies organizational, engineering, operational and assessment requirements for the integrity of automotive digital systems from concept to final decommissioning. Integrity in this document includes authorized behaviour, authenticity, confidentiality, availability, recoverability, accountability and appropriate handling of personal data.

The scope includes passenger and commercial vehicles, buses, powered two-wheelers, trailers with digital functions, specialized road vehicles and their components. It also includes associated cloud and edge services, mobile applications, remote support, diagnostic tools, update distribution, charging interfaces, vehicle communications, automated driving interfaces and digital manufacturing processes that can influence a released product.

DSI-01-01. The organization shall demonstrate that digital assets perform only authorized functions within the declared operating conditions and that security controls do not introduce unacceptable hazards. A valid signature, authenticated connection or successful test alone shall not be treated as evidence that an action is safe or its content is correct.

DSI-01-02. The lifecycle shall include concept, sourcing, design, development, verification, production, release, deployment, operation, repair, ownership transfer, repurposing, support termination and disposal. For existing products, unavailable historical evidence shall be identified and addressed through reconstruction and verification; it shall not be presumed to exist.

DSI-01-03. The organization shall identify applicable market obligations and contractual duties separately and reconcile them with the engineering controls. A conformity claim under this standard shall not be represented as vehicle market authorization, comprehensive functional safety approval, or a guarantee against all attacks.

Mechanical crashworthiness, general driving performance and overall environmental performance are outside the assessment except where digital behaviour influences them. Artificial intelligence integrity requirements address controlled development and use; they do not by themselves establish that an automated driving function is safe in all conditions.

2 Interpretation and mandatory rules

“Shall” establishes a requirement. “Shall not” establishes a prohibition. “Should” expresses a recommendation. “May” expresses permission. “Can” describes a capability or possibility. Requirements identified by DSI numbers and Annexes A, B and C are normative. Annexes D, E and F are informative; their examples do not establish additional conformance obligations.

DSI-02-01. The organization shall maintain a clause-level applicability statement covering every numbered requirement and every applicable test in Annex B. Each entry shall state applicable or not applicable, the responsible owner, the implementation, the evidence identifier and the assessment result.

DSI-02-02. A not-applicable decision shall identify the absent function, interface or activity and the evidence establishing its absence. Outsourcing, supplier confidentiality, low production volume, cost and lack of evidence shall not alone justify non-applicability. The assessor shall challenge omissions against actual architecture and behaviour.

DSI-02-03. An alternative implementation shall satisfy the same mandatory outcome and acceptance criteria with equivalent or stronger evidence. It shall be justified, reviewed independently of its design author, and recorded before release. This provision shall not waive a numerical minimum, prohibited behaviour, release gate or independent review requirement.

DSI-02-04. Every organization-selected limit shall be recorded in the parameter declaration of Annex C before testing. The declaration shall include units, operating conditions, uncertainty, justification, owner and approval. A value shall not be relaxed after a failed test without an engineering change assessment and repetition of affected tests.

DSI-02-05. “All” and “100 percent” shall apply to the documented in-scope population, whose completeness shall be verified. Sampling shall not silently redefine the population. An unresolved applicability decision or missing mandatory evidence shall prevent a conformant decision for the affected scope.

3 Terms and abbreviations

Term	Meaning in this standard
Accountable organization	Entity making the conformity claim and controlling the declared scope or accepting integration responsibility.
Digital asset	Hardware, executable software, model, data, identity, key, configuration or service whose compromise can affect the scope.
Integrity envelope	Documented limits within which a function is authorized, validated and able to respond safely to faults or hostile inputs.
Essential function	Function needed to maintain a justified minimum level of physical safety or safe recovery in the current operating state.
Safe degraded state	Validated reduced capability appropriate to the situation; it may require controlled stopping rather than continued travel.
Evidence baseline	Identified set of requirements, versions, tests, findings and approvals supporting a particular decision.
Threat scenario	Credible sequence involving an actor or hostile condition, an entry point, affected assets and a harmful outcome.
Residual risk	Risk remaining after implemented controls and their demonstrated limitations are considered.
Trust boundary	Interface across which authority, identity, confidentiality or assumed integrity changes.
Blast radius	Maximum population, services or functions affected by a defined compromise before independent controls contain it.
OTA	Over-the-air delivery of software, firmware, models, calibration, configuration or credentials.
SDLC	Software development lifecycle, including requirements, design, implementation, verification and maintenance.
SBOM	Machine-processable inventory of software components and their dependency relationships.

Term	Meaning in this standard
AI	Artificial intelligence, including learned models, generative models and agents able to invoke tools or services.
ECU	Electronic control unit, including consolidated or virtualized implementations.
API	Application programming interface between software components or services.
V2X	Communication between a vehicle and other vehicles, infrastructure, people, networks or services.
Integrity passport	Controlled record linking a declared product or platform to its assessed digital baseline and support status.
Material change	Change that can invalidate an assumption, risk decision, control, test result, support commitment or scope statement.
Credible awareness	Earliest recorded receipt or observation of sufficiently specific information to require technical triage.
Independent review	Review by a competent person who did not produce the item and has authority to reject it.
Security epoch	Protected ordering value used to prevent acceptance of superseded security states.

4 Scope declaration and integrity profiles

DSI-04-01. The scope declaration shall identify legal entity, engineering sites, operational responsibilities, product families, hardware variants, software releases, regions, deployment environments, associated services and supported lifecycle stages. It shall show all external dependencies capable of affecting an in-scope claim.

DSI-04-02. The organization shall identify the claim as a complete vehicle platform, defined subsystem, component, service, or organizational process. A component or process result shall not be promoted as complete vehicle conformity. Integration assumptions shall be delivered with every partial-scope result.

DSI-04-03. Integrity profiles shall be assigned using the criteria below. All profiles shall implement applicable baseline requirements. A higher profile increases assurance depth; it does not imply that another profile may omit necessary controls.

Profile	Assignment criteria	Additional assurance
IP1	No credible route to essential-function interference, high-impact privacy harm or fleet propagation; boundaries are demonstrated.	Independent internal review and baseline verification.
IP2	Connected services, remote functions, valuable credentials or sensitive personal data; compromise can cause material harm without meeting IP3 criteria.	Assessment team independent of the delivery team; adversarial integration tests.

Profile	Assignment criteria	Additional assurance
IP3	Credible influence on essential functions, remote actuation, automated driving authority, release-signing roots or fleet-wide privileged operations.	Organizationally independent technical assessment; all relevant high-consequence attack paths exercised; recovery and fleet containment exercises.

DSI-04-04. The highest applicable profile shall govern a shared trust boundary or common control unless isolation is demonstrated. A gateway, build service or identity system that can undermine an IP3 function shall receive IP3 assurance for that dependency even if it is located outside the vehicle.

DSI-04-05. The scope shall declare whether OTA, AI, V2X, charging control, remote driving, biometrics, third-party applications, digital keys and continuous learning are present. The corresponding conditional requirements shall apply whenever their triggering capability exists, including dormant capabilities activatable after sale.

DSI-04-06. The organization shall reassess scope and profile after every material change. An integration supplier shall receive the assumptions needed to reassess its own risk, including support limitations and known residual vulnerabilities.

5 Governance and engineering accountability

DSI-05-01. Senior management shall appoint an accountable digital integrity owner with authority to stop release or deployment and obtain remediation resources. Product security, safety, privacy, software release and operations responsibilities shall be assigned with named deputies and escalation routes.

DSI-05-02. The organization shall maintain a lifecycle integrity plan defining deliverables, review gates, staffing, competence, supplier responsibilities, test environments, operating resources and support funding. Release pressure shall not override unresolved mandatory gates.

DSI-05-03. Personnel performing threat analysis, secure development, cryptography, privacy assessment or adversarial testing shall demonstrate competence appropriate to their tasks through assessed work, supervised practice or relevant experience. Competence shall be reviewed when duties or technologies materially change.

DSI-05-04. Authoring, approval and deployment authority shall be separated for production signing, trust-root changes and fleet-wide commands. At least two independently authenticated persons shall approve these actions, except for pre-authorized automated actions restricted by tested policy and independent limits.

DSI-05-05. Risk acceptance shall state affected assets, consequences, alternatives, constraints, owner, review date and invalidating triggers. No individual shall approve their own unreviewed risk analysis. Risk acceptance shall not authorize noncompliance with a mandatory prohibition.

DSI-05-06. Evidence shall be protected against unauthorized alteration, deletion and backdating. Access shall follow least privilege, with recorded changes and a retention schedule covering the support period and any longer applicable duty. Personal data within evidence shall be minimized and managed separately from technical retention needs.

DSI-05-07. Internal audits shall examine implementation and actual product behaviour at least once per 12 months. IP3 operations shall additionally review privileged access, exposure and open risks at least once per 6 months. Management shall track corrective actions to verified closure.

6 Threat analysis and risk decisions

DSI-06-01. Threat analysis shall begin before architecture approval and cover assets, users, attackers, interfaces, data flows, dependencies, privileges, physical access and credible misuse throughout the lifecycle. Assumptions about connectivity, trust, vehicle state and access duration shall be explicit.

DSI-06-02. Analysis shall consider remote and local attackers, malicious insiders, compromised suppliers, stolen service tools, hostile tenants, compromised authorized accounts and attacks using valid credentials. It shall include simultaneous failures, common dependencies and loss of trusted time or revocation services.

DSI-06-03. Consequences shall be rated separately for physical safety, privacy, operation, financial harm and fleet propagation. The highest justified consequence shall drive treatment. Low financial impact shall not offset serious physical or privacy harm.

Impact	Decision meaning
I1 Limited	Reversible inconvenience with no meaningful essential-function, sensitive-data or fleet effect.
I2 Material	Recoverable service disruption, limited data harm or material repair and financial consequences.
I3 Severe	Potential serious injury contribution, severe personal-data harm, sustained essential-service disruption or substantial fleet propagation.
I4 Extreme	Potential fatal or multiple serious injuries, systemic fleet loss of control, or irreversible and widespread severe harm.

Feasibility	Required reasoning
F1 Constrained	Several demonstrated independent barriers and demanding access or resources; assumptions remain defensible.
F2 Plausible	Specialist capabilities or restricted access are required and reasonably obtainable.
F3 Accessible	A motivated attacker can obtain the required access and resources with limited barriers.
F4 Demonstrated	Reproducible exploitation exists or credible active exploitation affects the relevant configuration.

DSI-06-04. The initial priority shall be the impact number multiplied by the feasibility number: 1 to 3 Low, 4 to 7 Moderate, 8 to 11 High, and 12 to 16 Critical. I4 scenarios shall be at least High. An actively exploited path to essential-function control, production signing or uncontrolled privileged fleet actions shall be Critical regardless of the product. These categories are treatment priorities, not quantitative probabilities.

DSI-06-05. Uncertainty shall be recorded and investigated. Where an uncertain assumption can conceal I3 or I4 harm, the assessment shall use the more conservative credible case until evidence resolves it. Absence of public exploitation shall not establish infeasibility.

DSI-06-06. Treatment shall define preventive, detective, containment and recovery controls; link each control to verification evidence; and re-evaluate the complete attack path after implementation. Reducing exposure by disabling a feature shall include checks that it cannot be reactivated without authorization.

DSI-06-07. A release shall contain no known Critical residual scenario and no uncontained, credibly exploitable High residual scenario. Other High residual scenarios shall require demonstrated independent barriers, a time-limited treatment plan and independent approval. A safety or privacy prohibition elsewhere in this standard shall still prevail.

DSI-06-08. Threat analysis shall be updated before material changes, after relevant incidents and when assumptions or attack capabilities change. A periodic review shall occur at least every 12 months, and every 6 months for IP3 scopes.

7 Asset identity and digital configuration

DSI-07-01. The organization shall maintain a controlled inventory of in-scope hardware, software, firmware, models, datasets, calibrations, keys, certificates, services and externally reachable interfaces. Each item shall have an identifier, owner, version or configuration, dependency links and lifecycle status.

DSI-07-02. Each release shall include a machine-processable software inventory reconciled with the delivered executable content. Unknown components, binary-only dependencies and incomplete dependency depth shall be explicitly recorded and investigated; they shall not disappear from the inventory because source code is unavailable.

DSI-07-03. The inventory shall link executable artifacts to their origin, intended function, supported versions, known vulnerability disposition and deployment population. Cryptographic and AI inventories shall capture the additional fields required by Clauses 9 and 19.

DSI-07-04. Released software, policy, model and configuration states shall be identifiable on the product or through a protected service interface. A vehicle identifier shall not be treated as an authentication secret. Publicly readable identifiers shall not grant remote access.

DSI-07-05. Unauthorized configuration drift shall be detected at boot, update or a justified runtime checkpoint. The response shall be compatible with the current safety state; immediate shutdown shall not be assumed to be safe.

DSI-07-06. Inventory coverage shall include 100 percent of in-scope executable deployment units and production signing identities. The organization shall reconcile build records, deployment manifests and observed instances before release and after material changes.

DSI-07-07. Each software inventory shall identify its author, generation time, format and version, generation context, generation tool and version, product baseline, component names, producers, versions, identifiers, digests with algorithm names, license information and dependency relationships. It shall state coverage and unknown values explicitly and shall be authenticated against unauthorized alteration. Changes to the inventory shall be versioned and reconciled with the actual delivered content.

8 Architecture and trust boundaries

DSI-08-01. The architecture shall document trust domains and allowed flows among external interfaces, infotainment, diagnostics, body functions, energy management, motion control, safety functions and backend services. Undocumented cross-domain access shall be denied by default.

DSI-08-02. A less trusted domain shall not directly authorize essential-function actuation. Commands crossing the boundary shall be authenticated where technically applicable, explicitly authorized, checked for freshness and constrained by a local integrity envelope independent of the requesting service.

DSI-08-03. Every shared compute platform shall enforce separation of privileges, memory, storage, communications and resource consumption. Resource exhaustion and malicious tenants shall be tested against the scheduling and timing limits of essential functions.

DSI-08-04. Externally supplied data shall be validated for size, structure, range, sequencing, freshness and semantic plausibility before use. Validation shall account for malformed, authenticated-but-false and inconsistent inputs.

DSI-08-05. Development ports, diagnostic functions and unused services shall be removed, disabled or access-controlled in production. A production debug session shall require specific authorization, bounded scope and duration, and a durable activity record.

DSI-08-06. Safety-related fallback and containment shall not share a single unmitigated compromise path with the control they supervise. Common power, timing, memory, identity and update dependencies shall be analyzed and tested.

DSI-08-07. A single compromised user account, service credential or externally connected component shall not permit unrestricted commands across the entire declared fleet. Fleet segmentation and independent authorization boundaries shall limit the declared blast radius.

DSI-08-08. Executable boot stages and security-relevant startup configuration shall be verified against authorized integrity evidence before use. The chain of verification shall begin from a protected trust basis and shall include recovery paths. Runtime loading of privileged code shall apply equivalent authorization and integrity checks; verification failure shall invoke the validated state-aware response.

9 Identity cryptography and trust renewal

DSI-09-01. Devices, workloads, service personnel and privileged users shall have distinct authenticated identities appropriate to their function. Production devices shall not use a fleet-wide shared authentication secret. Public trust anchors may be shared where their compromise and renewal are controlled.

DSI-09-02. Keys shall be generated using demonstrably adequate randomness, assigned to defined purposes, protected in storage and use, rotated or renewed as needed, and destroyed when retired. Export of high-value private keys shall be prevented or subject to an independently approved and tested protection mechanism.

DSI-09-03. The organization shall maintain a cryptographic profile containing algorithms, parameter strengths, purposes, libraries, implementation versions, key locations, validity periods, trust chains,

revocation behaviour and known limitations. Secrecy of an algorithm shall not be the basis of its claimed strength.

DSI-09-04. Privileged remote administration shall use phishing-resistant multifactor authentication or a demonstrated equivalent protecting against credential replay and origin impersonation. Machine identities shall use short-lived or equivalently controlled credentials with narrow permissions.

DSI-09-05. Interfaces shall prevent unauthorized downgrade, identity substitution and replay. Nonces, sequence values and trusted freshness mechanisms shall remain sound through reboot, sleep, clock correction and power loss.

DSI-09-06. Trust-root compromise shall have a documented recovery path that does not rely solely on the compromised signing authority. Recovery shall authenticate a replacement authority, limit affected scope, prevent replay and preserve a recoverable product state.

DSI-09-07. The organization shall assess long-lived confidentiality and signature trust against foreseeable changes in computational capability, including quantum computation. The assessment shall distinguish data collected now for future decryption from future forgery of software and identity credentials.

DSI-09-08. IP2 and IP3 designs shall provide and test a migration path for cryptographic algorithms, key formats and trust anchors. Testing shall include larger messages, memory and timing effects, mixed-fleet interoperability, refusal of downgrade and interrupted migration. Where replacement is physically impossible, a declared compensating architecture and lifecycle replacement plan shall be required.

DSI-09-09. Experimental cryptography shall not become the sole production protection of an IP3 boundary without independent analysis, implementation validation and operational recovery evidence. A claim of quantum readiness shall identify the exact tested migration capability and remaining limitations.

DSI-09-10. Sensitive data and security-relevant communications shall use confidentiality and integrity protection appropriate to their threat exposure in transit and at rest. Key material shall be separated from protected content, and secrets shall not appear in ordinary logs or diagnostic output. Designs that cannot encrypt a legacy link shall enforce independently verified access and integrity boundaries and shall document the remaining exposure.

DSI-09-11. For high-value hardware trust boundaries, the threat model shall consider physical extraction, fault injection, side-channel leakage and unauthorized debug access according to credible attacker access. Applicable protection claims shall have representative hardware testing or independent evaluation evidence covering the actual implementation and operating conditions.

10 Secure software development

DSI-10-01. Each security, privacy and resilience requirement shall be traceable to design decisions, implementation items, verification cases and release approval. Requirements affecting essential functions shall also link to the relevant hazard analysis.

DSI-10-02. Source repositories shall enforce authenticated access, protected branches, review before integration and recorded changes. Security-sensitive code and policy changes shall receive review by a competent person other than the author.

DSI-10-03. The organization shall maintain coding rules covering memory safety, input handling, concurrency, integer behaviour, error handling, privilege use and secret handling. New externally exposed or IP3 code shall use memory-safe implementation where practicable; exceptions shall identify the constrained code, reason, compensating controls and specific tests.

DSI-10-04. Development shall include automated source analysis, dependency analysis, secret detection and appropriate dynamic tests. Tool limitations and false-negative risks shall be documented. Unresolved findings shall be dispositioned using Clause 6 rather than hidden through tool exclusions.

DSI-10-05. Test strategy shall include negative, boundary, misuse, fault-injection and adversarial scenarios alongside correct operation. Security testing shall cover generated code, configurations, scripts and infrastructure definitions, not only compiled application code.

DSI-10-06. AI-assisted code shall be subject to the same ownership, review, origin checks and verification gates as other code. Untrusted generated instructions shall not receive privileged build or deployment authority merely because they originate from an assistant.

DSI-10-07. Production secrets and identifiable customer records shall not be placed in development data or model prompts without a specific approved need and equivalent protection. Test datasets shall minimize exposure and shall be access-controlled and deleted according to their declared retention.

DSI-10-08. Every discovered defect with a security effect shall be assessed for root cause, related components and regression risk. Confirmed defects shall generate regression checks where repeatable testing is possible.

11 Build and release provenance

DSI-11-01. The build process shall bind source versions, dependencies, build instructions, toolchain versions, configuration and resulting artifacts into an integrity-protected provenance record. Only approved inputs shall enter a production build.

DSI-11-02. Build workers shall be isolated from untrusted submissions and production signing authority. Temporary access shall expire, environments shall be reset between trust contexts, and unauthorized outbound access shall be restricted.

DSI-11-03. Release signing shall occur only after the recorded gates are satisfied. The signing service shall verify the artifact identity and approval state itself; it shall not rely solely on a caller-supplied assertion that testing passed.

DSI-11-04. IP3 release artifacts shall be independently rebuilt or independently verified against protected provenance, approved inputs and executable content. Where reproducible output is not feasible, the reason and an alternative content-verification method shall be recorded and tested.

DSI-11-05. Artifact stores shall prevent substitution, unreviewed overwrite and unauthorized deletion. Distribution shall preserve the approved artifact digest and metadata from signing to installation.

DSI-11-06. The organization shall test compromise of a build worker, dependency source and ordinary release account. The tests shall demonstrate that these compromises alone cannot authorize an unrestricted IP3 release.

DSI-11-07. Emergency releases shall preserve identity, authorization, integrity, essential regression and recovery checks. Deferred nonessential tests shall be recorded with deadlines and completed before the release is treated as fully verified.

12 Supplier and service dependencies

DSI-12-01. Procurement shall assign requirements for secure development, asset transparency, vulnerability notification, update delivery, support duration, incident cooperation, evidence access and retirement. Responsibilities shall extend to relevant subcontractors.

DSI-12-02. The integrator shall assess supplier evidence for the delivered version, configuration and use conditions. Supplier attestations shall not replace integration tests or transfer accountability for the complete vehicle claim.

DSI-12-03. Dependency inventories shall include executable components, hosted services, model providers, remote administration, signing services and infrastructure control planes. A supplier replacement or service relocation shall trigger a material-change assessment.

DSI-12-04. The organization shall establish an actionable response to supplier discontinuation, insolvency, loss of access, signing compromise and support termination. Options shall include replacement, escrow where suitable, service migration, constrained operation or controlled retirement; feasibility shall be demonstrated before dependency acceptance.

DSI-12-05. Confidential evidence may be examined under controlled access, but insufficient assessor access shall be recorded as an evidence gap. The assessor shall not infer conformity from inaccessible claims.

DSI-12-06. Shared or reused components shall be tracked across affected vehicle families. A relevant vulnerability shall trigger population analysis and coordinated remediation across all affected releases, including branches maintained by different suppliers.

13 OTA and other update integrity

DSI-13-01. Every change delivered to a product shall be governed as an update when it can alter behaviour, authorization, privacy or a risk assumption. This shall include firmware, applications, AI models, calibrations, feature flags, policy, maps used for control and trust credentials, regardless of delivery channel.

DSI-13-02. An integrity-protected update manifest shall identify the artifact, digest, authorized signer, target hardware, allowed source states, resulting state, dependencies, security epoch, validity constraints, installation conditions, recovery method and release approval. Ambiguous targets shall be rejected.

DSI-13-03. Before installation, the receiving system shall verify authenticity, authorization, completeness, freshness, compatibility, available energy, storage and required operating conditions. A package that passes signature verification but fails any required check shall not be activated.

DSI-13-04. Essential-function software shall not be activated during an unsafe vehicle state. Concurrent installation while driving shall be permitted only where isolation, scheduling, power effects and activation controls have been validated for that operating state.

DSI-13-05. Multi-component updates shall maintain a defined compatible state across interruption, restart and partial completion. The update design shall implement transactional activation or an equivalent validated mechanism preventing incompatible component combinations from controlling the vehicle.

DSI-13-06. A failed update shall preserve a validated recoverable state. Recovery may restore a previously approved compatible version or use an approved recovery image. Recovery shall not silently cross below the security epoch or reactivate a known prohibited state.

DSI-13-07. The organization shall test energy interruption, communication loss, storage exhaustion, corrupted packages, stale metadata, wrong targets, revoked authority, incomplete dependencies and failure during each state transition. Annex B defines minimum acceptance evidence.

DSI-13-08. Fleet deployment shall use staged cohorts, predeclared monitoring criteria and automatic or independently authorized pause controls. Cohort size, expansion conditions, observation duration and acceptable failures shall be justified before rollout. A laboratory success shall not alone authorize immediate deployment to the entire fleet.

DSI-13-09. The user or operator shall receive understandable information on purpose, expected duration, vehicle availability, necessary actions, effects on functions and applicable scheduling choices. Changes to optional data use shall require renewed choice where that choice is the processing basis.

DSI-13-10. Deployment records shall distinguish offered, downloaded, verified, installed, activated, failed, recovered and unreachable devices. “Delivered” shall not be counted as “successfully activated.” Unreachable devices shall remain visible in the outstanding-risk population.

DSI-13-11. Update refusal, subscription expiry or loss of connectivity shall not secretly disable essential functions. Where continued use becomes unsafe, the organization shall communicate and implement a validated risk response appropriate to vehicle state.

DSI-13-12. Workshop, removable-media and emergency updates shall satisfy the same authorization, target verification, integrity and recovery outcomes as OTA. Physical access shall not itself authorize arbitrary firmware installation.

14 Cloud mobile applications and remote operations

DSI-14-01. Backend services and mobile applications able to read vehicle data or issue commands shall be included in the platform threat model. Authorization shall be checked for each object, vehicle, tenant and operation; possession of an identifier or a valid session shall not grant unrestricted access.

DSI-14-02. Remote commands shall be restricted by function, vehicle, operating state, duration and requester role. Commands shall expire, resist replay and be rejected when sequence or state makes execution unsafe. The vehicle shall enforce its local integrity envelope even when the backend is authenticated.

DSI-14-03. Tenant and fleet isolation shall be verified using hostile requests from ordinary users, compromised support accounts and service identities. Rate limits shall protect both service availability and vehicle-side resources.

DSI-14-04. Mobile applications shall protect credentials and sensitive local records, bind enrollment to verified authority, and revoke access when devices are lost or accounts are transferred. An application update shall not silently broaden vehicle permissions.

DSI-14-05. Administrative access shall be time-bounded, logged and periodically reviewed. Break-glass access shall require a defined emergency reason, minimum scope, prompt independent review and revocation when the emergency ends.

DSI-14-06. Cloud configuration changes, infrastructure deployments and remote feature activations shall pass change control. Separate approval and fleet limits shall apply to commands with common-mode consequences, including immobilization, unlocking and energy dispatch.

DSI-14-07. Loss of a region, identity provider, communication carrier, time source or payment service shall be analyzed as a dependency failure. Recovery tests shall establish that essential vehicle behaviour is not dependent on restoring a commercial account or optional subscription.

15 Privacy and responsible data use

DSI-15-01. Every personal-data flow shall have a specified purpose, data categories, affected persons, justified processing basis, recipients, access rules, retention limit and deletion method. Linkable vehicle identifiers, location histories, recordings and inferred behaviour shall be treated as personal data where they can relate to a person.

DSI-15-02. Collection shall be limited to what is necessary for the stated purpose. The design shall evaluate local processing, lower precision, shorter retention and derived features before transmitting raw location, audio, video or biometric information.

DSI-15-03. Optional analytics, advertising, profiling and secondary model training shall be disabled by default until the required affirmative choice or other demonstrated applicable authority exists. A choice for an optional purpose shall not be bundled with access to an unrelated essential function.

DSI-15-04. Information shall be accessible to drivers, passengers, rental users and other affected persons through means appropriate to the interaction. Notices and controls shall identify material sensor activity, data sharing and changes in purpose without relying solely on a lengthy account document.

DSI-15-05. Where processing relies on consent, withdrawal shall be as easy as granting it and shall stop future optional processing at the next applicable processing point. Withdrawal shall be propagated to recipients and offline devices through a controlled mechanism. Data retention on another justified basis shall be explained and restricted.

DSI-15-06. Access, correction, export, restriction and deletion requests shall be authenticated proportionately and processed through a tracked workflow within applicable deadlines. Identity verification shall not collect excessive additional data. Backup restoration shall reapply deletion and restriction records before renewed use.

DSI-15-07. Occupant monitoring and biometric systems shall restrict raw recordings, templates and inferred sensitive attributes. Children, incidental passengers and bystanders shall be considered in the impact assessment. Safety monitoring shall not automatically justify commercial reuse.

DSI-15-08. Ownership transfer, return of a rented vehicle and removal of a shared driver shall revoke prior digital keys, remote access, pairing and personal profiles. Reset shall be verified in the vehicle, applications and relevant backend services; the former owner shall not retain location access.

DSI-15-09. Precise location and remote access features shall be assessed for stalking, coercive control and unauthorized household access. Removal of a shared user shall prevent covert continued access. Notifications shall be designed so they do not expose a vulnerable person's new location or create additional foreseeable harm.

DSI-15-10. Data processors and onward recipients shall receive purpose and retention restrictions. Cross-border hosting and access shall be evaluated against applicable duties, and material changes shall trigger renewed assessment. This standard shall not be used to presume that a transfer is permitted.

DSI-15-11. Claims of anonymity shall be supported by reidentification analysis using realistic auxiliary information. Pseudonymous data shall not be presented as anonymous merely because direct names are removed.

DSI-15-12. Privacy verification shall trace seeded test data through collection, transmission, access, retention, export and deletion. Privacy settings shown to users shall match observed traffic and stored records under connected, disconnected and reset conditions.

16 Cyber resilience and safe recovery

DSI-16-01. For each essential function, the organization shall define its authorized operating envelope, tolerated disruption, failure-detection needs, fallback behaviour and maximum safe response time. These parameters shall be derived from hazard and operational analysis rather than a universal network timeout.

DSI-16-02. The product shall retain the essential capability needed to reach or maintain a justified safe state during loss of cloud, network, positioning, identity or payment services. A remote-dependent automated service shall locally perform its validated contingency response; continued autonomous travel shall not be assumed safe.

DSI-16-03. Security controls shall not cause an unsafe reboot, sudden loss of steering or braking, unsafe energy interruption, trapping of occupants or uncontrolled actuator command. Containment shall be state-aware and verified with the relevant engineering disciplines.

DSI-16-04. The architecture shall bound resource starvation, repeated reconnection, crash loops, malicious event floods and corrupted stored states. Failure of optional services shall not exhaust resources reserved for essential functions.

DSI-16-05. Recovery assets shall have protected integrity, appropriate separation and a tested restoration path. Recovery shall re-establish trusted software, configuration, identity and restrictions; simply restarting a compromised state shall not count as recovery.

DSI-16-06. Fleet exercises shall test simultaneous credential revocation, control-plane outage and compromised update distribution. Measured containment shall remain within the predeclared blast radius and shall not require unsafe commands to unaffected vehicles.

DSI-16-07. The organization shall define detection, containment, restoration and evidence-preservation times in Annex C. Safety response shall complete within its engineered time budget. Administrative incident deadlines shall not be used as permissible delay for an immediate vehicle safety response.

DSI-16-08. Resilience testing shall include degraded power, temperature and communication conditions within the declared product limits. A design that only recovers with ideal power and uninterrupted connectivity shall not support a broader claim.

17 Vulnerability handling and corrective updates

DSI-17-01. A publicly accessible vulnerability reporting channel shall remain available throughout support. Reports shall receive an identifier, secure handling, acknowledgement and a stated coordination process. The organization should support responsible research through clear testing boundaries and constructive communication.

DSI-17-02. Every credible report shall be triaged against deployed and supported configurations, including reachability, required privileges, compensating controls and fleet scope. A generic severity label or component name match shall not replace product-specific analysis.

DSI-17-03. Response clocks shall begin at credible awareness, including actionable supplier notice or internal detection. Classification and clock-start decisions shall be recorded. Reclassification shall not reset elapsed time or conceal a missed deadline.

DSI-17-04. The organization shall meet the triage, interim-control and correction-plan deadlines in Annex C. When no safe interim control is available, the condition shall remain unresolved and shall be escalated immediately; a documented explanation shall not convert a failed requirement into conformity.

DSI-17-05. A correction shall undergo proportionate regression, compatibility, security and recovery testing. Remediation priority shall consider the danger of both exploitation and deployment. An unsafe patch shall not be installed merely to meet an administrative deadline.

DSI-17-06. Advisory information shall identify affected products, practical mitigations, available updates, user actions and remaining limitations without unnecessarily enabling exploitation. Disclosure timing shall consider active harm, remediation availability and applicable reporting duties.

DSI-17-07. Closure shall require evidence that the affected state is removed or effectively contained in the relevant population. Unreachable vehicles, declined installations and unsupported branches shall be separately reported with their residual exposure.

DSI-17-08. Recurring vulnerabilities shall trigger root-cause improvement in architecture, development or supplier controls. A successful patch shall not close a systemic process failure without evidence of corrective action.

18 Monitoring incident response and evidence

DSI-18-01. Monitoring shall cover threats relevant to the scope, including unauthorized commands, identity anomalies, boot integrity failures, update rejection, cross-domain access and abnormal fleet activity. Collected telemetry shall be proportionate and shall not depend on continuous raw cabin recording.

DSI-18-02. Security events shall have reliable ordering, source identity, integrity protection and access controls. Where trusted clock time is unavailable, the system shall record clock uncertainty and preserve event sequence rather than fabricate precise timing.

DSI-18-03. Monitoring pipelines shall detect their own loss of coverage and resist forged, suppressed or duplicated events. The organization shall test alert delivery under service failure and shall distinguish “no event observed” from “no monitoring available.”

DSI-18-04. An incident plan shall assign technical command, safety decisions, privacy decisions, communications, supplier coordination and operational recovery. IP3 scopes shall maintain an on-call response capability able to act at any time.

DSI-18-05. Response actions shall preserve essential functions, restrict further compromise and protect necessary evidence. Collection tools shall not overwrite relevant records or expose unrelated personal information without a justified need.

DSI-18-06. Notification workflows shall identify affected users, partners and competent authorities where applicable, record the basis and deadline, and preserve the content sent. The standard's engineering deadlines shall not replace shorter applicable notification duties.

DSI-18-07. The organization shall exercise a complete incident scenario at least every 12 months, and every 6 months for IP3 scopes. Exercises shall include an unavailable primary responder, a supplier handoff, a safety-sensitive decision and recovery verification.

DSI-18-08. A post-incident review shall reconstruct events and assumptions, assess containment performance and assign improvements with owners and due dates. Public or customer statements shall distinguish confirmed facts, current uncertainty and planned actions.

19 Artificial intelligence and adaptive software integrity

DSI-19-01. Each deployed model shall have an identified owner, version, intended function, authority, operating limits, input assumptions, dependencies and monitoring plan. The model record shall distinguish development data, evaluation data and live operational inputs.

DSI-19-02. Training and evaluation assets shall have documented provenance, authorization for use, transformation history and access controls. Data contamination, duplicate evaluation items and dependence between training and testing shall be investigated before performance evidence is accepted.

DSI-19-03. The organization shall evaluate poisoning, adversarial inputs, model substitution, extraction, privacy leakage and manipulation of external content according to the model's role. Results shall include unsuccessful and inconclusive cases, relevant limitations and the defended operating envelope.

DSI-19-04. A generative model or agent shall not have direct unrestricted authority over motion control, safety settings, production signing or fleet-wide commands. A separate policy enforcement mechanism shall validate identity, intent, permissions, command parameters and operating state before any authorized action.

DSI-19-05. External text, retrieved content, diagnostic files and sensor-derived instructions shall be treated as untrusted data. Tests shall establish that such content cannot grant new permissions, reveal protected credentials or override the independent action boundary.

DSI-19-06. A model update, prompt-policy change, retrieval-source change or tool-permission change shall undergo impact analysis and applicable release gates. Model drift shall not be used as an explanation for unapproved changes to safety or privacy authority.

DSI-19-07. Continuous or federated learning shall be limited to a prevalidated adaptation envelope with protected provenance, participant controls, poisoning defenses, monitoring and a tested rollback or freeze capability. Adaptation outside that envelope shall be treated as a new release. IP3 actuation policy shall not self-expand its authority in service.

DSI-19-08. AI performance and robustness limits shall be declared by scenario and relevant operating conditions before testing. A single average accuracy shall not conceal failure in a safety-relevant subgroup, rare condition or hostile-input category.

DSI-19-09. When uncertainty, drift or input conditions exceed the approved envelope, the system shall use its validated fallback, request appropriate human involvement or stop the affected function safely. Human intervention shall not be credited unless the person has sufficient information, competence and response time.

DSI-19-10. Reproducing a decision shall use the available model version, relevant configuration and minimum necessary input record. Claims of explanation shall state their limits and shall not substitute for evidence that prohibited actions are prevented.

20 Connected interfaces and automated mobility

DSI-20-01. Each external mobility interface shall document its trust assumptions, authorized operations, message limits and failure response. Scope shall include charging, V2X, positioning, digital keys, remote assistance, teleoperation and third-party applications where present.

DSI-20-02. Authenticated V2X messages shall be checked for freshness, location consistency and plausibility before they influence driving. A valid sender credential shall not establish that a claimed road event is true. Essential decisions shall use corroboration or a validated conservative response.

DSI-20-03. Positioning and time-dependent functions shall detect or tolerate spoofed, delayed, conflicting or unavailable signals within declared limits. The organization shall test behaviour when the apparent position remains plausible but slowly diverges.

DSI-20-04. Charging and bidirectional energy functions shall authenticate relevant parties, separate payment from physical protection, bound power requests and validate command freshness. A compromised charging service shall not override local thermal, electrical or vehicle-state limits.

DSI-20-05. Digital keys shall support verified enrollment, role-limited sharing, expiration, revocation and ownership transfer. Proximity-based access shall consider relay and ranging manipulation. Emergency entry and occupant egress shall remain compatible with safety needs.

DSI-20-06. Remote driving or assistance shall distinguish advice from control authority, identify the responsible operator, define latency and link-quality limits, and record authority transfer. Loss of link or uncertain authority shall trigger the locally executable validated contingency response.

DSI-20-07. Cooperative manoeuvres, platooning and shared perception shall not permit a compromised participant to issue unchecked motion commands to peers. Membership change, conflicting messages and abrupt participant withdrawal shall be tested.

DSI-20-08. Third-party applications and aftermarket devices shall receive the minimum permitted data and functions. Installation, permission changes, removal and revocation shall preserve domain isolation and shall not bypass update control.

DSI-20-09. Satellite and future communication services shall remain external dependencies subject to the same identity, freshness, denial-of-service and outage analysis. A new communication technology shall not be presumed trusted because it is novel or has greater bandwidth.

21 Production diagnostics repair and transfer

DSI-21-01. Production processes shall provision device identities and approved software through controlled stations with authenticated operators, protected credentials and traceable records. Production and engineering test identities shall be separated.

DSI-21-02. End-of-line checks shall verify approved executable state, unique device credentials, production access settings and required security functions. Any repair to provisioning shall be logged and reverified before release.

DSI-21-03. Service tools shall authenticate the tool and authorized operator as appropriate, limit functions to the job, and expire access. Service credentials shall not become transferable master keys for all vehicles.

DSI-21-04. Replacement components shall be checked for identity, compatibility, approved state and key handling. Reused or remanufactured modules shall undergo data sanitization, secure enrollment and removal of previous ownership links.

DSI-21-05. Authorized independent repair shall have a controlled access route appropriate to the operation and applicable duties. Security restrictions shall be technically justified, proportionate and documented; repair access shall not grant unrelated personal data or unrestricted remote control.

DSI-21-06. Resale, lease return, fleet reassignment and export shall trigger a documented handover process covering profiles, remote permissions, digital keys, installed state and support information. Security defects shall not be hidden by resetting visible notifications.

DSI-21-07. Field modifications and retrofit equipment shall be assessed for new attack paths, electrical effects, data access and update compatibility. The integrity passport shall be updated where the assessed baseline changes.

22 Support continuity and end of life

DSI-22-01. Before supply, the organization shall declare a security support period or end date, covered products and services, update channels, responsible contact and the method for notifying users of changes. The commitment shall be supportable by supplier contracts, capability and resources.

DSI-22-02. Security support for essential functions and previously supplied security protections shall not be conditional solely on purchasing optional entertainment, analytics or convenience services. Any paid service boundary shall be clearly described without undermining the declared product support commitment.

DSI-22-03. End-of-support planning shall assess installed population, expected remaining use, unresolved vulnerabilities, dependency retirement and feasible protective measures. A notice alone shall not resolve a continuing high-consequence technical risk.

DSI-22-04. Support termination notice shall be provided at least 12 months before the declared end date unless an unforeseeable event prevents that notice. An exception shall trigger immediate notification, management escalation and a risk-managed continuity response. An existing commitment shall not be shortened solely by issuing such a notice.

DSI-22-05. The retirement plan shall provide an approved terminal configuration, controlled disconnection, replacement route, restricted mode or other justified protection. Disabling connectivity shall be checked for effects on emergency, safety, energy and recovery functions.

DSI-22-06. Decommissioning shall revoke identities and remote access, erase or cryptographically render inaccessible personal and secret data, close service accounts and update the asset record. Reintroduction into service shall require controlled re-enrollment.

DSI-22-07. Support records and recovery instructions needed by authorized maintainers shall remain accessible for the declared period. Changes of corporate ownership, supplier or service operator shall preserve assigned obligations or establish a documented successor arrangement.

23 Verification and technical assessment

DSI-23-01. The verification plan shall map every applicable mandatory requirement to document review, inspection, analysis, test or a justified combination. Annex B shall be treated as a minimum test catalogue, supplemented by product-specific threat and hazard cases.

DSI-23-02. Test items shall represent the production hardware, software, configuration, access controls and associated services. Differences from production shall be listed with their effect on validity. A disabled security control shall not be used to obtain an otherwise unrepresentative passing result.

DSI-23-03. The plan shall define preconditions, stimuli, environmental limits, expected outcomes, measurement methods, uncertainty, pass criteria, stopping conditions and safe recovery. Adversarial tests shall be authorized and isolated from uncontrolled public-road or customer effects.

DSI-23-04. Interface coverage shall include every distinct exposed interface class and every materially different trust boundary. Sampling of product variants shall be justified by architectural equivalence, with all exceptions and worst-case variants tested. IP3 high-consequence paths shall not be omitted solely because they are difficult to reproduce.

DSI-23-05. Test results shall record exact versions, actual observations, timestamps, tools, configuration, operator, evidence artifacts and deviations. Test procedures shall be repeatable by a competent assessor without relying on undocumented personal knowledge.

DSI-23-06. Simulations shall document model validity and differences from physical systems. Physical timing, energy interruption and hardware isolation claims shall include representative hardware evidence; simulation alone shall not establish them.

DSI-23-07. Failed or inconclusive mandatory cases shall be investigated and rerun after correction. A result shall not be changed to pass by deleting the failed stimulus or excluding a newly discovered attack path without a valid scope change and complete reassessment.

DSI-23-08. Review independence shall match the assigned profile. IP3 assessment shall be conducted by an organizationally independent team with no responsibility for designing or approving the assessed release. A commercial relationship shall be disclosed and managed so it does not control technical conclusions.

DSI-23-09. Competence records shall cover the scope actually assessed, including automotive state behaviour, software, communications, privacy and cryptography as relevant. Specialists shall be involved when a general assessor cannot validate a material claim.

24 Conformity decisions and change control

DSI-24-01. A conformant decision shall require a complete scope and applicability statement, satisfied mandatory requirements, passed applicable mandatory tests, acceptable residual risk, a complete evidence index, required independent review and a signed decision. No weighted score shall compensate for a failed requirement.

DSI-24-02. Findings shall be classified as Critical when they create immediate or uncontrolled severe harm or a prohibited release condition; Major when a required system or control is absent or ineffective; and Minor when a limited required element is deficient without established systemic failure. Severity shall govern response priority, not permission to leave a requirement unmet.

DSI-24-03. Any unresolved mandatory nonconformity shall prevent a new conformant decision. Observations and recommendations that do not establish a failed requirement may remain open if clearly separated from nonconformities.

DSI-24-04. An assessment result shall identify scope, profile, versions, evidence baseline, assessor, decision authority, date, conditions, support status and next planned review. This standard shall not impose a universal fixed certificate term. Continued claims shall depend on maintained conditions and reassessment triggers.

DSI-24-05. A material change shall trigger an impact analysis before deployment. A delta assessment shall identify what changed, what evidence remains valid and what must be repeated. Changes to trust roots, essential-function authority, AI adaptation limits, major suppliers or the support model shall require independent review.

DSI-24-06. An active claim shall be restricted, suspended or withdrawn when a critical condition, material unassessed change, unsupported configuration or evidence failure invalidates it. Affected parties shall be informed without presenting a historical result as the current condition.

DSI-24-07. Restoration shall require verified corrective action, relevant repeat testing and a new recorded decision. Merely submitting an action plan shall not restore a suspended claim.

DSI-24-08. Public claims shall distinguish self-declaration, independently assessed results and certification under a separately approved scheme. Use of an IAF conformity mark shall require explicit authorization under that scheme; preparation of this standard does not grant mark use.

DSI-24-09. Complaints and appeals shall be recorded and reviewed by competent persons independent of the contested decision. Security-sensitive details shall be protected while the reasons for the outcome remain reviewable by authorized parties.

25 Digital integrity passport and transparency

DSI-25-01. A conformity claim shall have a digital integrity passport identifying the accountable organization, assessed object, claim type, scope, profile, baseline versions, decision date, support commitment and current status. The passport may use any machine-processable format satisfying the required semantics.

DSI-25-02. The passport shall link to a controlled evidence index without publicly exposing private keys, exploit details, personal records or confidential architecture. A public view and a restricted technical view shall be separated.

DSI-25-03. Passport updates shall be authenticated and versioned. Historical decisions shall remain distinguishable from the current state. A stale or unverifiable passport shall not be displayed as proof of current conformity.

DSI-25-04. An offline status display shall identify the last verified time and its freshness limit. When that limit is exceeded, status shall be shown as unknown rather than automatically conformant or automatically unsafe.

DSI-25-05. The public view shall state relevant feature dependencies, security contact, available updates, support end and significant restrictions in understandable language. It shall not publish individual vehicle location or personal ownership history.

DSI-25-06. Passport information shall be exportable in a documented format so authorized assessors and successor support providers can interpret it without dependence on one service operator.

26 Performance review and technology evolution

DSI-26-01. The organization shall monitor inventory completeness, critical and high exposure, deployment success, unreachable population, containment performance, recovery outcomes, privacy-control failures and open corrective actions. Metrics shall have defined denominators, observation windows and treatment of missing data.

DSI-26-02. Metrics shall be reported by affected configuration and risk class where aggregation can conceal harm. A high average update success rate shall not conceal an unrecoverable essential-function failure in a small vehicle population.

DSI-26-03. Threat and technology review shall examine changes in compute capability, communication systems, software architecture, autonomous agents, synthetic data, sensing, remote control and energy coordination. It shall occur at least every 12 months and before introducing a materially new capability.

DSI-26-04. A new capability shall be assessed through its actual authority, dependencies, failure modes and evidence needs. Where existing test methods cannot substantiate its integrity envelope, deployment authority shall be constrained until suitable verification exists.

DSI-26-05. The organization shall maintain a forward compatibility and migration plan for cryptography, supported interfaces, recovery tooling and evidence formats. The plan shall identify irreversible hardware constraints and the point at which replacement becomes necessary.

DSI-26-06. Claims such as continuous trust, autonomous resilience or future readiness shall state the measured capability, operating conditions, validated limits and date. Predictions shall not be presented as tested performance, and automated monitoring shall not be presented as proof that no compromise exists.

Annex A Required evidence register

Normative

The accountable organization shall maintain the following evidence for applicable activities. Evidence may be combined in one controlled system if each required content item remains identifiable. Every record shall identify its owner, version, approval state, scope, access classification and retention rule. The register shall link each individual DSI requirement and Annex B test to actual evidence, rather than only to a generic policy folder.

Record	Required content	Principal clauses
A01 Scope statement	Entity, product, services, variants, interfaces, lifecycle stages, claim type and limitations.	1 to 4
A02 Applicability matrix	Every requirement and test, applicability basis, implementation, evidence and outcome.	2 and 23
A03 Profile decision	Consequence and authority analysis, shared dependencies, isolation basis and reviewer.	4
A04 Integrity plan	Roles, competence, gates, resources, suppliers, support funding and review schedule.	5
A05 Risk register	Assets, scenarios, impact, feasibility, uncertainty, controls, residual risk and acceptance.	6
A06 Digital inventory	Hardware, executable units, dependencies, models, configurations, identities and deployed states.	7
A07 Architecture record	Domains, trust boundaries, allowed flows, resource limits and independent containment.	8
A08 Cryptographic record	Algorithms, keys, trust chains, validity, revocation, migration and recovery evidence.	9
A09 Development record	Requirements traceability, source reviews, tool output, tests and defect dispositions.	10
A10 Release provenance	Approved inputs, toolchain, build evidence, artifact digests, signing and release approvals.	11
A11 Supplier assurance	Responsibility contracts, evidence reviews, support arrangements and exit plans.	12
A12 Update campaign	Manifest, preconditions, compatibility, interrupted-update tests, cohorts and outcomes.	13
A13 Service controls	API permissions, tenancy, mobile enrollment, remote commands and administration.	14
A14 Data processing record	Purposes, data flows, user controls, impact assessment, recipients, retention and deletion tests.	15

Record	Required content	Principal clauses
A15 Resilience case	Essential functions, state envelopes, timing budgets, containment and restoration tests.	16
A16 Vulnerability record	Awareness time, triage, affected population, interim controls, correction and closure.	17
A17 Incident record	Monitoring coverage, event integrity, decisions, notifications, exercises and lessons.	18
A18 AI integrity record	Provenance, authority, evaluation sets, hostile-input testing, adaptation and fallback.	19
A19 Interface assurance	V2X, charging, positioning, digital keys, remote control and aftermarket tests.	20
A20 Production and service	Provisioning, end-of-line checks, service access, replacement parts and handover.	21
A21 Support and retirement	Commitments, installed population, continuity response, terminal state and sanitization.	22
A22 Verification dossier	Coverage, representative variants, procedures, uncertainty, observations and retests.	23
A23 Decision record	Findings, closure, residual risk, independent review, scope and signed decision.	24
A24 Change record	Materiality decision, changed assumptions, evidence reuse and reassessment.	24
A25 Integrity passport	Public and restricted views, versions, authenticated status and support information.	25
A26 Performance review	Metric definitions, missing data, trends, management action and technology migration.	26
A27 Parameter declaration	All limits from Annex C, engineering justification, units, approvals and invalidating triggers.	2 and Annex C

Annex B Minimum verification catalogue

Normative

B0 Common execution rules

Every applicable case below shall be translated into an executable product-specific procedure. The procedure shall state exact inputs, topology, versions, permissions, timing, vehicle state, expected observations, instruments and restoration steps. The reviewer shall approve it before execution. A catalogue title alone shall not count as a completed test.

Each case shall cover its stated variants and all materially different implementations identified in the coverage plan. Stateful interruption or race-sensitive sequences shall be repeated at least 10 times per selected configuration for IP1 and IP2, and at least 30 times for IP3. Repeated runs shall vary relevant timing and initial state. Additional runs shall be performed where nondeterminism or observed failures invalidate confidence. Deterministic document inspections do not require artificial repetition.

No unauthorized actuation, cross-boundary authority, acceptance of a prohibited artifact, or exposure of protected test data shall be observed in a passing case. This zero-observed-failure rule concerns the executed test set; it is not proof of zero residual risk. Measurement uncertainty shall be included when comparing an observation with a limit. An observation whose uncertainty crosses the acceptance limit shall be inconclusive until resolved.

Each result shall include the procedure, raw observations, evidence digests, outcome, reviewer, deviations and linked finding identifiers. Where a conditional feature is absent, non-applicability shall be established through the scope statement and implementation inspection.

B01 Scope and inventory reconciliation

Applies to all scopes; verifies Clauses 4 and 7. Reconcile the declared scope with architecture, build outputs, observed services and a representative production configuration. Identify omitted binaries, hidden endpoints, dormant features and differing component versions. Compare each executable deployment unit and signing identity with the inventory.

Acceptance: every observed in-scope executable unit, privileged identity and material interface is identified; discrepancies are resolved; profile assignment reflects actual authority. Preserve reconciliation logs, inventory snapshots and the variant selection rationale.

B02 Boot and runtime integrity

Applies to executable platforms; verifies Clauses 7 to 9. Modify protected boot, executable, configuration and policy artifacts; attempt startup and relevant runtime reloads. Repeat with valid content and with a validly signed but prohibited security state. Observe verification order, execution decisions, alerts and safe recovery.

Acceptance: altered or prohibited content does not gain unauthorized execution; the approved state starts correctly; recovery meets its declared envelope. Preserve artifact identifiers, verification results and hardware-observed state transitions.

B03 Domain and resource isolation

Applies to shared platforms and gateways; verifies Clauses 8 and 16. From a compromised less trusted domain, attempt unauthorized memory, storage and network access. Exhaust its allocated compute, communication and event capacity while exercising essential functions at declared worst-case workload.

Acceptance: cross-domain authority remains constrained and essential deadlines, data integrity and fallback behaviour remain within approved limits. Record timing distributions and worst observed values, not only averages.

B04 Identity enrollment and revocation

Applies to identity-controlled access; verifies Clauses 9, 14 and 21. Enroll a legitimate identity; then test stolen credentials, unauthorized enrollment, role escalation, expired credentials and revoked access. Repeat through offline operation, clock uncertainty and later reconnection.

Acceptance: only authorized roles act; revocation reaches connected enforcement points within Annex C limits; offline behaviour follows the bounded declared policy. Record issuance, use, refusal and revocation propagation events.

B05 Trust root recovery and cryptographic migration

Applies to IP2 and IP3 trust systems and any claimed migration capability; verifies Clause 9. Simulate compromise of the normal authority and exercise the independent recovery path. Migrate a representative component and service to the approved alternative algorithm or trust format. Test downgrade, mixed versions, interruption and resource effects.

Acceptance: unauthorized recovery and downgrade fail; legitimate migration preserves compatibility, essential timing and recoverability. The evidence identifies exactly which algorithms, formats and product variants were exercised.

B06 Build provenance and release authority

Applies to software producers and integrators; verifies Clauses 10 to 12. Introduce an unapproved dependency, substitute a stored artifact and impersonate an ordinary build worker. Attempt production signing without completed approvals. Verify an approved release against its provenance using the declared independent method.

Acceptance: unauthorized content cannot acquire an approved release identity; provenance resolves to the delivered content; independent approvals cannot be fabricated by the tested single compromised account.

B07 Update authenticity and target binding

Applies to updateable products; verifies Clause 13. Present a valid package and packages with altered bytes, missing content, stale metadata, incorrect target hardware, unauthorized signer and revoked signing authority. Include a package whose signature is valid but whose dependencies or target state are wrong.

Acceptance: only the intended authorized compatible package reaches activation. Rejections preserve approved operation and create actionable records without exposing secrets.

B08 Interrupted update and recovery

Applies to updateable products; verifies Clauses 13 and 16. Enumerate the update state machine and interrupt power or communications during download, verification, preparation, writing, activation and confirmation where each interruption is physically meaningful. Repeat at boundary timings and low declared energy.

Acceptance: each interruption leaves or restores a validated state within the declared recovery limit. No unapproved image executes, no incompatible essential-function state activates, and recovery does not cross below the allowed security epoch.

B09 Multi component compatibility and rollback

Applies to interdependent updates; verifies Clause 13. Execute updates in incorrect order, with one component unavailable, with a stale component state and with a failed activation acknowledgement. Attempt replay of a prior valid update and unauthorized rollback.

Acceptance: dependency rules are enforced, partial activation cannot authorize incompatible essential behaviour, and only explicitly approved compatible recovery states are reachable. Preserve the compatibility matrix and observed component states.

B10 Fleet rollout and emergency pause

Applies to fleet distribution; verifies Clauses 8, 13 and 16. In an isolated fleet representation, trigger declared failure thresholds during a staged campaign and compromise an ordinary rollout account. Include unreachable vehicles and delayed acknowledgements. Exercise pause and recovery authority.

Acceptance: expansion stops at the approved trigger; the tested account cannot exceed its cohort authority; observed affected population remains within the declared blast radius. Unreachable and failed vehicles remain in the denominator and action register.

B11 Safe installation conditions

Applies to updates affecting operating state; verifies Clause 13. Attempt activation during motion, charging, low energy, occupied service mode and other disallowed states identified by the hazard analysis. Test false or stale indications of safe state.

Acceptance: essential-function activation occurs only under validated conditions; a spoofed state cannot bypass controls; user information matches actual unavailability and recovery behaviour.

B12 API object and tenant authorization

Applies to connected services; verifies Clause 14. Using ordinary, elevated and revoked accounts, request another vehicle's records, issue commands to another tenant and invoke privileged endpoints. Include altered identifiers, batch operations, alternate request forms and concurrent authorization changes.

Acceptance: no cross-vehicle or cross-tenant access or command execution occurs outside the approved role model. Errors and logs do not disclose protected records or reusable secrets.

B13 Remote command freshness and safety envelope

Applies to remote functions; verifies Clauses 8, 14 and 20. Replay, delay, reorder and duplicate commands; submit authorized commands with unsafe parameters or in an invalid vehicle state. Simulate a compromised authenticated backend.

Acceptance: stale or unsafe commands are rejected or constrained locally, and no single remote principal bypasses the essential-function envelope. Record both the server decision and the vehicle's actual response.

B14 Parser and stateful protocol robustness

Applies to exposed parsers and message handlers; verifies Clauses 8, 10 and 20. Exercise a corpus covering valid traffic, malformed lengths, invalid encodings, extreme values, invalid state sequences and resource exhaustion. Execute at least 100000 distinct mutated inputs per exposed parser class, supplemented by relevant stateful sequences and justified additional exploration for IP3.

Acceptance: no unauthorized execution, protected-data disclosure or unsafe loss of essential function occurs; crashes and hangs are analyzed and corrected where they violate requirements. The input count is a minimum exercise size, not a sufficient security argument by itself.

B15 Cloud and dependency outage

Applies where external services support the product; verifies Clauses 14 and 16. Remove connectivity, identity, trusted time, positioning or primary cloud service singly and in credible common-failure combinations. Restore dependencies with stale sessions and conflicting state.

Acceptance: the product reaches or maintains its declared safe state, reconnects without replaying stale authority and meets recovery limits. Preserve vehicle-state evidence and service restoration records.

B16 Ransomware and destructive recovery exercise

Applies to recovery-dependent scopes; verifies Clauses 11, 16 and 18. Use an isolated environment to deny normal operational access and corrupt representative mutable state. Assume one administrative domain is compromised. Restore from protected recovery assets and re-establish trust.

Acceptance: the tested compromise cannot destroy all required recovery paths; restored software, identities and data restrictions match an approved baseline. Restoration time is measured from declared exercise onset to verified service readiness.

B17 Privacy defaults and data flow

Applies to personal-data processing; verifies Clause 15. Use seeded identities and distinctive synthetic records to trace collection and transmission with default settings, optional consent enabled, consent withdrawn and network access interrupted. Inspect actual destinations and stored content.

Acceptance: observed processing matches declared purpose and settings; disabled optional purposes do not receive new data; queued data follows the current valid policy before transmission. Preserve traffic and storage evidence with controlled access.

B18 Deletion and backup restoration

Applies to retained personal data; verifies Clause 15. Request deletion through an authenticated test identity and follow the record across active storage, caches, processors and backups. Restore a backup that contains the previously deleted record.

Acceptance: the declared deadlines are met; restricted or deleted information does not re-enter ordinary processing after restoration; justified retained evidence remains segregated. The test records any storage where immediate physical overwrite is not feasible and verifies the approved alternative.

B19 Ownership transfer and digital keys

Applies to user or owner-linked access; verifies Clauses 15, 20 and 21. Transfer a test vehicle or rental session and attempt access using former accounts, mobile devices, shared keys, service sessions and offline credentials. Include later reconnection of an old device.

Acceptance: previous users cannot locate, unlock, command or retrieve new personal records without fresh authorization; the new authorized user can complete intended enrollment; occupant egress remains available.

B20 AI provenance and model substitution

Applies to AI functions; verifies Clause 19. Reconcile the deployed model with its record and substitute model weights, configuration, retrieval data or tool policy. Include a signed model outside the declared compatibility or authority limits.

Acceptance: unauthorized substitutions and incompatible authority changes are blocked; the approved model remains traceable to its evaluated baseline and production restrictions. Record both model identity and the effective runtime policy.

B21 AI hostile content and action boundaries

Applies to AI or agents processing untrusted content; verifies Clause 19. Submit instructions embedded in retrieved text, diagnostic files and relevant input channels that attempt to override policy, access another user's data or invoke prohibited vehicle and backend functions. Include indirect and multi-step attempts.

Acceptance: independent enforcement prevents prohibited tool use, secret disclosure and unauthorized actuation in the defined test suite. Refusal wording from the model alone is insufficient evidence if a tool call can still execute.

B22 AI drift poisoning and adaptation limits

Applies to adaptive, learned or federated systems; verifies Clause 19. Introduce representative distribution shifts, manipulated contributions and adaptation outside the approved envelope. Exercise monitoring, isolation of suspect contributions, freeze and recovery.

Acceptance: approved scenario-specific limits are maintained or the validated fallback activates; adaptation cannot broaden authority; integrity and provenance survive rollback. Record scenario-level results and uncertainty, including the weakest performing relevant condition.

B23 V2X and cooperative message integrity

Applies to V2X and cooperative driving; verifies Clause 20. Send stale, forged, duplicated and authenticated-but-false messages; simulate conflicting participants, false events, implausible position and sudden withdrawal. Use controlled simulation plus hardware where physical behaviour is claimed.

Acceptance: origin trust does not bypass plausibility and local safety constraints; malformed or misleading cooperation does not create unauthorized actuation. Preserve the basis for corroboration or conservative fallback.

B24 Charging and bidirectional energy authority

Applies to connected energy functions; verifies Clause 20. Emulate a compromised charger or dispatch service, stale authorization, excessive power requests, interrupted sessions and mismatched payment state. Test commands near approved electrical and thermal boundaries.

Acceptance: local physical limits remain effective; payment or remote authorization failure cannot override protection; power changes and session termination follow validated vehicle-state behaviour.

B25 Positioning time and remote driving

Applies to functions relying on positioning, trusted time or remote driving; verifies Clauses 9, 16 and 20. Inject drift, abrupt jumps, delayed commands, link degradation, clock rollback and conflicting operator authority. Test at the declared worst-case reaction boundary.

Acceptance: the product detects or tolerates the condition within its approved envelope and performs the local contingency response before the safe-response budget is exceeded. Record measured latency, loss patterns and actual control authority.

B26 Manufacturing provisioning and service access

Applies to production and maintenance; verifies Clause 21. Inspect representative provisioning records and attempt duplicate device credentials, use of engineering keys, expired workshop sessions, unauthorized replacement modules and excessive diagnostic permissions.

Acceptance: production identity and state are controlled; service authority remains job-limited; incompatible or unauthorized replacements cannot gain privileged operation. Preserve end-of-line and reenrollment evidence.

B27 Logging and monitoring continuity

Applies to monitored scopes; verifies Clause 18. Suppress, forge, reorder and duplicate security events; remove the primary logging endpoint and introduce clock uncertainty. Generate known detectable security events during each condition.

Acceptance: relevant detection objectives and coverage-loss alerts are met; source integrity and event ordering remain interpretable; absence of monitoring is not represented as absence of attacks.

B28 Vulnerability response clock and coordination

Applies to supported products; verifies Clause 17 and Annex C. Inject a time-stamped credible report affecting a shared component and trace acknowledgement, triage, population discovery, escalation, interim controls and the correction plan. Include an unavailable primary supplier contact.

Acceptance: required deadlines are met without resetting the awareness clock; affected variants and unreachable devices remain visible; closure requires technical evidence rather than an unanswered supplier request.

B29 End of support and decommissioning

Applies to products with support or retirement obligations; verifies Clause 22. Exercise the terminal-configuration plan on a representative item, remove an external dependency and attempt reuse of revoked credentials and erased test data. Inspect notice and successor-support arrangements.

Acceptance: the declared support commitment and safe terminal state are demonstrable; retired identities cannot retain ordinary access; sanitization prevents authorized test recovery of protected content through the defined access methods.

B30 Passport status and material change

Applies to conformity claims; verifies Clauses 24 and 25. Alter passport data, replay an older status, expire its freshness period and introduce an unassessed material change. Exercise restriction, suspension and restoration workflows.

Acceptance: tampering and stale status are recognizable; current claims track the assessed baseline; restoration requires a recorded new decision. The public view discloses no restricted personal or exploit information.

B31 Fleet compromise and independent containment

Applies to IP3 and any shared privileged fleet service; verifies Clauses 8, 14, 16 and 18. Assume compromise of a fleet operations principal and attempt commands, credential changes or update actions beyond its authorized segment. Exercise the independent containment channel with the ordinary control plane unavailable.

Acceptance: affected scope stays within its approved quantitative limit, unaffected segments preserve essential behaviour, and containment meets its declared timing. A limit equal to the entire fleet fails unless the scope is a single vehicle with no shared control plane.

B32 Supplier exit and replacement integration

Applies to a critical external dependency; verifies Clauses 12 and 22. Select a supplier whose failure can undermine an essential or privileged function. Exercise the documented exit route using representative artifacts, alternative support or constrained operation. Test identity handover and evidence availability.

Acceptance: the organization demonstrates a technically feasible continuity or controlled-retirement route, with maintained trust and declared limits. A contractual promise with no executable recovery or replacement method does not pass.

Annex C Acceptance parameters and response limits

Normative

C1 Parameter declaration

Before design verification, the organization shall create a signed parameter declaration containing every applicable field below. Product-specific values shall be justified from threat, hazard, dependency and operational analysis. Blank values, “as soon as possible” and values chosen only after seeing test outcomes shall not be accepted.

Parameter	Required declaration	Binding decision rule
Essential-function timing	Detection and safe-response budget per function and operating state, in suitable time units.	Observed response including uncertainty shall not exceed the safe budget.
Recovery	Maximum time to each defined safe state and restored service; power and link conditions.	All applicable recovery tests shall meet the declared time and state limits.
Fleet blast radius	Maximum number and proportion of vehicles, identities and services affected per defined compromise.	Limits shall be below the whole fleet for shared control planes and met in B10 and B31.
Update cohorts	Size, sequence, observation period, expansion authority and stop thresholds.	No cohort expansion before its approved evidence and observation conditions are met.
Privileged revocation	Time from approved revocation to enforcement; connected and offline cases.	Connected backend privileged enforcement shall complete within 15 minutes; safety-sensitive device actions shall also follow the local envelope.
Offline authority	Maximum credential age, command lifetime and permitted offline functions.	Expired optional remote authority shall fail closed; essential functions shall use their validated state-aware response.
Parser coverage	Interface classes, corpus, state sequences, input count and stopping rule.	At least 100000 distinct mutated inputs per applicable parser class; risk-based additional coverage remains required.
Update interruption	State transitions, timing variation, selected hardware variants and repetitions.	At least 10 repetitions per stateful sequence for IP1 and IP2; at least 30 for IP3.
AI evaluation	Scenario-level limits, hostile-input cases, relevant populations, sample rationale and uncertainty.	Every safety-relevant declared limit shall pass or the affected authority shall be constrained and reassessed.
Data retention	Maximum duration by purpose, storage, cache, backup and recipient.	Expiry and deletion shall be verified; any mandatory retention exception shall be segregated and justified.
Monitoring	Events, coverage, alert latency and response routing by threat class.	Missing coverage shall be detectable; engineered safety deadlines take precedence.

Parameter	Required declaration	Binding decision rule
Passport freshness	Maximum age of a displayed verified status and offline treatment.	Expired status shall be unknown until reverified, without implying that the vehicle is necessarily unsafe.
Support	Start basis, end date or calculable duration, components and services covered.	Delivered commitment shall be maintained; announced changes shall not silently shorten it.

C2 Vulnerability workflow deadlines

The following are maximum elapsed calendar times from credible awareness. They are proposed IAF process limits. They are not general patch-installation deadlines and do not authorize delay in responding to immediate harm. Any shorter applicable duty or engineered safety-response time shall take precedence.

Priority	Technical triage completed	Effective interim protection or verified existing containment	Dated permanent-correction plan approved
Critical	24 hours	72 hours	7 calendar days
High	72 hours	14 calendar days	30 calendar days
Moderate	7 calendar days	Need assessed and dispositioned within 30 calendar days	60 calendar days
Low	14 calendar days	Need assessed and dispositioned within 60 calendar days	90 calendar days

Reports through the public channel shall be acknowledged within 2 calendar days; urgent technical action shall not wait for acknowledgement. For initially unclassified reports, triage shall prioritize the highest credible consequence. An indication of active essential-function compromise shall trigger immediate escalation at receipt.

An effective interim protection shall remove or contain the relevant attack path in the affected environment and shall have evidence that it does not create unacceptable safety or privacy harm. A press statement, planned update, customer notice alone or disabled alert shall not count as technical containment. Operational restriction may count only where its actual enforcement and safe consequences are demonstrated.

Each permanent-correction plan shall state a justified delivery deadline, owner, affected population, validation activities and deployment strategy. Progress shall be reviewed at least weekly for Critical and High items until permanent correction or validated long-term treatment. A missed interim deadline is a nonconformity; a missed correction commitment shall trigger escalation, renewed risk assessment and claim review. Neither shall be erased by issuing a replacement plan.

Where an interim control has been verified and the resulting risk no longer meets Critical or uncontained exploitable High criteria, a new conformity decision may consider the updated residual risk and evidence. The original finding, duration and affected population shall remain in the historical record. Without that verification, the release and claim restrictions remain in force.

C3 Periodic review minima

Activity	IP1 and IP2	IP3
Complete threat review	At least every 12 months	At least every 6 months
Internal implementation audit	At least every 12 months	At least every 12 months with privileged-operation review every 6 months
Incident exercise	At least every 12 months	At least every 6 months
Review of assurance baseline and targeted technical retest	At least every 12 months	At least every 6 months
New-technology and migration review	At least every 12 months	At least every 12 months and after material capability change

Periodic intervals shall not postpone reviews required by an incident, relevant vulnerability, material change or invalidated assumption. Targeted retesting shall cover changed or newly exposed attack paths; the assessor shall justify any unchanged evidence retained. This table sets assurance activities, not a universal certificate validity period.

C4 Release decision checklist

Before an initial or materially changed release is approved, the decision authority shall verify all of the following: the scope and inventory are complete; all applicable mandatory requirements are met; required tests pass; independent reviews are complete; known Critical residual risks and uncontained exploitable High residual risks are absent; any other High residual risk meets Clause 6; update and recovery routes are verified; privacy settings match observed behaviour; support responsibilities are funded and assigned; and the evidence baseline identifies the actual release.

An administrative signature without these conditions shall not authorize a conformant claim. A recommendation for improvement may remain open only if it is not a failed requirement and does not invalidate risk acceptance.

Annex D Worked risk and scope examples

Informative

D1 Remote cabin command crossing into motion control

Consider an authenticated mobile service that changes cabin temperature. Analysis reveals that a shared backend credential also reaches a gateway permitting motion-related commands. The nominal cabin function cannot remain IP1 merely because its user interface appears low risk. The shared authority path warrants IP3 assurance until isolation is demonstrated.

A credible I4 and F3 scenario has a priority value of 12 and is Critical. Appropriate treatment could combine removal of excessive backend authority, independent local command checks, gateway restrictions and segmented service credentials. A residual rating is reconsidered only after tests show the complete path is broken. A lower rating for the mobile application alone would not establish platform integrity.

D2 Personal data in a vehicle resale

A former owner retains a paired application after resale. The vehicle reset removes visible contacts but a backend association still allows location queries. The defect may cause severe privacy harm even when driving behaviour is unaffected. Testing follows the old identity across the vehicle, application and backend, including an offline phone reconnecting after transfer.

A valid remedy revokes the old authority at every relevant enforcement point and prevents silent restoration from cached relationships. Deleting the vehicle's screen history alone would not address the scenario.

D3 A signed AI model with unsafe authority

A properly signed model update expands an assistant from answering maintenance questions to invoking vehicle service functions. Signature verification establishes provenance, while the new tool permissions change authority. This is a material change requiring permission analysis, hostile-content testing and independent verification of the action boundary.

A constrained design routes proposed actions through a separate policy mechanism and validates the vehicle's state. The model's assurance statement cannot replace the enforcement mechanism or its tests.

D4 Updating a supplier library without changing a vehicle binary

A hosted service changes a dependency that validates fleet command requests. The vehicle firmware stays the same, but the platform's trust boundary changes. The scope therefore includes a change assessment, new service provenance and relevant API, replay and fleet containment tests.

Evidence reuse is possible for unaffected vehicle hardware. It does not eliminate verification of the changed service or justify displaying an unchanged baseline without recording the dependency change.

Annex E Example implementation records

Informative

These examples show record content rather than a mandated data format. A real implementation would replace descriptive entries with controlled values and evidence identifiers. A cryptographic signature binds actual bytes according to the selected documented encoding; the example fields do not themselves constitute a signature scheme.

E1 Update manifest fields

Field	Example content or interpretation
Manifest identity	Unique campaign manifest with version and issuance time.
Artifact	Update package identity, byte length, digest and digest algorithm.
Authorized target	Product family, hardware variants and permitted installation population.
Source conditions	Allowed currently installed software, model, policy and security epoch.
Resulting state	Exact software, model and configuration identities after activation.
Dependencies	Required peer-component versions and ordering or transactional conditions.
Operating conditions	Approved motion state, energy reserve, temperature and storage availability.
Authority	Signer identity, authorization scope and trusted verification path.
Freshness	Validity conditions, campaign ordering and anti-replay state.
Recovery	Approved compatible recovery state and minimum allowed security epoch.
Release evidence	Baseline identifier and independent release approval records.
Rollout control	Cohort policy, observation conditions, pause authority and stop criteria.
User effect	Expected availability, affected functions and necessary operator actions.

E2 Integrity passport fields

Field	Example content or interpretation
Standard	IAF Digital Systems Integrity First Edition.
Claim type	Complete platform, subsystem, component, service or process.
Accountable entity	Legal entity accepting responsibility for the declared scope.
Product baseline	Hardware, software, service, model and configuration identifiers.
Integrity profile	IP1, IP2 or IP3 with a link to the approved scope statement.
Assessment basis	Self-declaration, independent assessment or authorized scheme certification.
Current status	Conformant, restricted, suspended, withdrawn or unknown.
Decision record	Decision date, authority and protected evidence-baseline reference.
Support	Covered components, security contact and declared support end.
Freshness	Last verification time, permitted age and offline presentation rule.
Limitations	Supported environments, dependencies and explicit scope exclusions.
Change history	Authenticated version history and superseded decision identifiers.

E3 Nonconformity record fields

A useful record identifies the failed requirement, affected baseline, observed evidence, severity, immediate action, root cause, correction, corrective action owner, deadline and retest outcome. It also records claim restrictions, independent closure approval and whether other product families share the defect.

“Correction” repairs the identified defect. “Corrective action” changes the process or architecture that allowed it. Both may be necessary, and their evidence can differ.

Annex F Forward technology scenarios

Informative

The following scenarios are planning hypotheses, not forecasts with guaranteed dates. The normative requirements apply when the corresponding authority or dependency is introduced. The aim is to make new technology reviewable without assuming that an unknown future implementation is already safe.

Scenario	Potential integrity failure	Capability to prepare and demonstrate
Autonomous maintenance agents	An agent translates untrusted diagnostic content into privileged fleet action.	Independent action policy, scoped credentials, simulated approval paths and recoverable changes.
Software defined vehicle marketplaces	A downloaded feature changes permissions or timing on shared compute.	Signed capability declarations, sandboxing, resource budgets and revocable permissions.
Continuous fleet learning	Poisoned contributions alter shared driving behaviour or reveal training participants.	Provenance, contribution screening, bounded adaptation, privacy tests and freeze capability.
Quantum-related trust transition	Recorded data becomes decryptable or long-lived signing trust becomes forgeable.	Inventory of exposure horizons, tested migration and independent trust renewal.
Cooperative perception	Authenticated peers create convincing but false shared situational awareness.	Plausibility checks, source diversity and local conservative decision boundaries.
Digital twins connected to live vehicles	A simulation environment acquires unintended write authority to operational systems.	Separate identities, explicit direction of data flow and validated actuation gates.
Large-scale bidirectional charging	Compromised dispatch creates correlated unsafe energy behaviour.	Local electrical protection, bounded cohorts and independent fleet containment.
Satellite and future mobile networks	New connectivity introduces credential, timing or long-outage assumptions.	Technology-neutral trust checks, bounded authority and verified disconnected behaviour.
Remanufactured compute modules	Reused hardware retains identities, data or unsupported trust anchors.	Sanitization, re-enrollment, compatibility evidence and renewed support commitment.
Provider disappearance	A connected vehicle loses an essential service or usable update route.	Tested support succession, exportable evidence and a safe terminal configuration.

The long-term ambition of this standard is a vehicle ecosystem in which authorized behaviour, recoverability and responsible data use remain demonstrable as technology changes. Future capability claims become meaningful when they identify the tested scope, the boundary that contains failure, and the evidence supporting continued operation.