



QUALITY MANUALS | FIRST EDITION

IAF SOFTWARE DEFINED VEHICLE AND SOFTWARE QUALITY MANUAL

Verified vehicle software
and controlled factory installation

STABLE RELEASE

Document No. IAF-MAN-SDV-001 | Revision 01

Powertrain and battery and driver assistance software
Secure loading and connected service testing
Defect resolution and vehicle release evidence

International Automotive Federation

English master text | 15 September 2026

iaf.com

Publication identity and use

IAF Software Defined Vehicle and Software Quality Manual

This manual defines software quality controls for vehicle functions, factory installation and connected service testing. It covers powertrain, battery and driver assistance software, with traceable releases, secure programming, controlled defect resolution and vehicle specific delivery evidence.

Control	Publication record
Document	IAF-MAN-SDV-001 IAF Software Defined Vehicle and Software Quality Manual
Edition / revision	First Edition Revision 01 Stable Release
Text issue	15 September 2026 English master text
Document owner	IAF Quality function with the relevant automotive technical committee
Custodian	IAF Secretariat / Document Controller
Institutional authority	Competent authority under IAF-CON-001; publication does not amend the Constitution.
Site adoption	Accountable operating director and technical leads record the actual approval reference, scope and operational effective date.
Classification	Public core manual. Completed operational records follow their assigned access and retention controls.

Reading and applying requirements

“Shall” identifies a requirement when adopted by a site, programme or agreement. “Should” identifies a recommendation. An example is illustrative; it is not a machine setting, test acceptance limit or completed operating record. Annex worksheets may be reproduced for controlled internal use.

Controlled implementation

Stable Release identifies the completed publication text. Site approval, process validation, competence authorization and equipment release are recorded when performed. A missing safety limit, test criterion or release authority prevents activation of the affected operation. Mandatory law, product requirements and validated equipment instructions remain applicable.

Relationship to IAF recognition

Use of this manual does not by itself confer membership, Corporate Recognised status, accreditation, certification or a licence to use IAF marks. Those decisions follow the applicable IAF guides, independent evaluation and recorded scope.

Contents

Every entry links to its section. Page numbers include the cover.

1 Purpose, scope and operating boundaries	5
2 Governance and release responsibilities	6
3 Requirements, hazards and acceptance criteria	7
4 Vehicle configuration and compatibility management	8
5 Architecture, interfaces and resource budgets	9
6 Source control, builds and dependency integrity	10
7 Supplier software and externally sourced components	11
8 Artifact signing, trust and credential control	12
9 Verification strategy and test environment control	13
10 Powertrain control software quality	14
11 Battery management and charging software quality	15
12 Driver assistance software, models and calibration	16
13 Diagnostics, connected interfaces and privacy	17
14 Procedure: approve a software release candidate	18
15 EOL programming station readiness	19
16 Procedure: securely install vehicle software at EOL	20
17 Multi-controller activation and recovery	21
18 Post-installation diagnostics and configuration checks	22

Contents - continued

Every entry links to its section. Page numbers include the cover.

19 Cloud test planning and environment separation	23
20 Procedure: verify connected vehicle services	24
21 EOL functional tests and physical validation boundaries	25
22 Defect intake, severity and reproducibility	26
23 Procedure: correct a defect and verify regression	27
24 Release holds, concessions and residual issues	28
25 Procedure: release a programmed vehicle for delivery	29
26 Post-delivery updates, service and incident feedback	30
27 Competence, metrics and independent assurance	31
28 Documents, retained evidence and IAF interfaces	32
Annex A - Release baseline and compatibility record	33
Annex B - Requirements and verification matrix	34
Annex C - EOL station readiness checklist	35
Annex D - Vehicle programming and recovery traveller	36
Annex E - Connected service verification record	37
Annex F - Defect, correction and regression record	38
Annex G - Vehicle software release passport	39
Annex H - Performance and assurance review worksheet	40

Using the annexes

Enter actual values, evidence references, names and dates in the worksheets. A blank, unsigned or illustrative record is not proof of completion. Retain the record with its governing instruction and revision.

1 Purpose, scope and operating boundaries

1.1 This manual establishes quality controls for software defined vehicles from engineering release through factory installation, connected service verification and delivery. It applies to executable code, boot software, calibrations, configuration data, security credentials, diagnostic content and learned model assets that determine vehicle behaviour. It covers combustion and electric powertrains, battery management, body and chassis controllers, gateways, infotainment and driver assistance functions within the adopted programme scope.

1.2 A software defined vehicle uses software and controlled configuration to deliver or change functions over its operating life. An electronic control unit is identified as an ECU; end of line is identified as EOL. Advanced driver assistance systems are identified as ADAS. The description ADAS shall not imply autonomous operation or remove the driver responsibilities defined for the particular feature. Feature names shall match the actual released capability.

1.3 The programme shall identify which activities occur in development laboratories, on guarded production equipment, on closed test facilities and after customer delivery. Development tools, test certificates and engineering images shall not be treated as production releases. A successful factory flash or cloud connection establishes only the checks actually performed; it does not demonstrate every driving scenario or the complete safety of a vehicle function.

1.4 The requirements apply to vehicle manufacturers, software suppliers, integration partners, factory programming providers and authorised service interfaces through their agreed responsibilities. Each operating site shall adopt a controlled implementation plan identifying its vehicle variants, equipment, release authorities, test limits and retained evidence. Missing information that affects safe programming, vehicle movement or release shall place the affected operation on hold.

1.5 This manual provides process requirements rather than vehicle tuning values or an authorisation to alter protected systems. Mandatory obligations, approved product requirements and validated equipment instructions remain applicable. Technical examples illustrate decision logic only. The operating organisation shall establish actual acceptance limits through its product engineering and safety processes before activating the corresponding tests or production operations.

2 Governance and release responsibilities

2.1 The programme director shall assign an accountable software release authority, a vehicle integration owner and a factory quality owner. Product engineering owns functional requirements and compatibility. Safety and security specialists define their respective acceptance conditions. Manufacturing engineering owns station capability and recovery instructions. Production executes released work, while Quality independently verifies that the evidence required for vehicle release is complete.

2.2 The software release authority shall approve an identified software baseline for an identified vehicle population and use. The factory release authority shall approve installation at a capable station. The vehicle release authority shall confirm the actual configuration and test results of each delivered vehicle. These decisions may be recorded in one controlled system, but their distinct scopes and required approvals shall remain visible.

2.3 No person shall approve their own unresolved critical deviation or silently change a failed acceptance criterion. The site shall define separation between code authoring, artifact promotion, production signing and release approval in proportion to risk. Where staffing requires combined roles, an independent competent reviewer shall verify the critical evidence and record the compensating control before release.

2.4 Anyone observing an unsafe response, unexpected vehicle actuation, compromised software identity or a loss of configuration traceability shall be able to stop the affected operation. The supervisor shall secure the vehicle and preserve evidence. Restart requires the named technical authority and Quality to confirm the cause, containment and applicable recovery checks; schedule pressure shall not serve as an approval basis.

2.5 IAF technical committees may develop guidance and review recurring quality issues within their assigned scope. Publication ownership does not replace the manufacturer or operating site responsibilities for product release. External assessors shall disclose conflicts of interest and access only the information needed for their assignment. Decisions, delegated authorities and competence records shall be retained through the controlled document system.

3 Requirements, hazards and acceptance criteria

3.1 Each software function shall have an approved requirement set describing intended behaviour, prohibited behaviour, operating conditions, inputs, outputs and fault responses. Requirements shall identify the affected hardware, vehicle variants, calibrations and connected services. Measurable acceptance criteria shall be established before formal verification and linked to a requirement identifier, responsible owner and test method.

3.2 The programme shall assess the consequences of incorrect torque, braking, steering, charging, thermal control, driver information and diagnostic behaviour. The assessment shall include interactions between functions and common dependencies such as time, power, communication, sensors and shared computing resources. Safety related requirements shall identify the safe response and the assumptions that must hold for that response to be effective.

3.3 Security requirements shall address unauthorised software installation, altered configuration, misuse of diagnostics, compromised credentials and untrusted connected inputs. Privacy requirements shall identify data collected, the purpose, access and retention. A security mechanism shall not be assumed to satisfy a functional safety requirement, and a functional test shall not be presented as evidence that an unauthorised update is prevented.

3.4 Acceptance limits shall distinguish development exploration from release testing. Boundary values, tolerances, timing budgets, environmental conditions and measurement uncertainty shall be stated where they affect the decision. A test with an undefined expected result is exploratory evidence; it cannot close a release requirement until the appropriate criterion has been approved independently of the observed outcome.

3.5 The requirements owner shall maintain traceability from each release requirement to design elements, verification results and unresolved anomalies. Changes shall trigger an impact review covering dependent functions, variants, factory tests and service behaviour. A requirement shall not be marked complete solely because a test script ran; its result, configuration, coverage and deviations shall support the recorded conclusion.

4 Vehicle configuration and compatibility management

4.1 Every releasable baseline shall identify executable images, boot components, calibrations, vehicle coding, diagnostic descriptions, model assets and relevant connected service interfaces. The baseline shall specify hardware part numbers and revisions, memory constraints, network compatibility and required companion ECU versions. A filename, marketing model year or latest version label is insufficient to establish compatibility.

4.2 A compatibility matrix shall map each authorised vehicle variant to its permitted component combination. The matrix shall include optional equipment, regional configuration, sensor and actuator variants, battery and propulsion variants and feature entitlements where applicable. Unsupported combinations shall be rejected before programming begins, with a clear hold reason and an approved route for resolving incorrect master data.

4.3 Each artifact shall carry a unique identifier, version, integrity value and release provenance. The manifest shall identify required predecessors, installation order, activation conditions and constraints on reversal. Software and calibration shall be controlled together when either changes functional behaviour. A calibration-only change shall receive the same impact assessment principles as an executable change.

4.4 The actual installed configuration shall be read from the vehicle after programming using a validated method. The process shall reconcile intended and reported identifiers, including controllers that were skipped, replaced or recovered. Where a controller cannot report the required identity directly, the programme shall approve a compensating verification method and disclose its limitations rather than infer completion from the station command log alone.

4.5 Engineering shall maintain a controlled rule for component replacement and mixed production lots. A replacement ECU shall be checked against the complete vehicle baseline and its credential state before use. The vehicle passport shall record the as-delivered combination and subsequent authorised changes, allowing an affected population to be identified without relying on incomplete operator notes.

5 Architecture, interfaces and resource budgets

5.1 The software architecture shall define functional boundaries, trust boundaries, network interfaces and dependencies between embedded controllers, central computing and cloud services. Safety relevant control paths shall be assessed for interference from other functions, including resource exhaustion and shared service failure. Design evidence shall explain which failures are contained and which require a coordinated vehicle response.

5.2 Each interface shall define signal meaning, units, range, quality status, update rate, freshness and invalid-data handling. Receiving components shall not treat absent, stale or invalid data as an ordinary valid value. Versioned interface descriptions shall identify behaviour during startup, sleep, wakeup, reset, degraded operation and loss of communication.

5.3 The programme shall allocate and verify processor, memory, storage, communication and timing budgets under representative peak conditions. Average utilisation alone shall not demonstrate adequate margin. Verification shall consider concurrent diagnostics, logging, updates, thermal throttling and connected services where these may affect the intended function or the ability to detect and respond to faults.

5.4 The architecture shall identify required separation of diagnostic, development, production and customer functions. Debug paths and development features shall have an explicit production disposition. A hidden engineering command or an undocumented configuration switch shall not be accepted as a recovery method or a substitute for a controlled service procedure.

5.5 Architecture changes shall be reviewed against existing verification evidence and vehicle compatibility. The review shall consider whether partitioning, shared libraries, message routing or computing allocation changes invalidate earlier results. The integration owner shall define the regression scope and any physical vehicle tests needed before the changed architecture can enter a production baseline.

6 Source control, builds and dependency integrity

6.1 Source code, build scripts, tool configurations, calibration sources and model generation assets shall be held in controlled repositories with recorded access and change history. Each change shall identify its purpose, linked requirement or defect, author and reviewer. Release branches shall have a defined promotion process and shall prevent unreviewed changes from entering a production build.

6.2 The build record shall identify source revisions, compiler and tool versions, dependencies, configuration options and build environment. Dependencies shall be retrieved from approved locations and checked for identity and integrity. The programme shall maintain a component inventory sufficient to locate affected software when a defect or security issue is discovered in a shared library or supplied binary.

6.3 The organisation shall seek reproducible builds and record the method used to compare outputs. Where exact binary reproduction is prevented by approved variable metadata or proprietary tooling, the release record shall identify that limitation and the alternative controls for provenance and integrity. An unexplained difference between intended and rebuilt artifacts shall be investigated before release.

6.4 Build automation shall enforce the required review, analysis and test gates. Failed checks shall remain visible with their disposition; disabling a check requires controlled approval and an impact assessment. Production artifacts shall be promoted from an identified verified build rather than rebuilt informally at the factory or copied from an individual workstation.

6.5 Credentials and signing material shall not be embedded in source repositories, test scripts or unrestricted build logs. Build access shall be reviewed when roles change. The organisation shall retain sufficient build evidence and approved tools or recovery arrangements to reproduce, investigate and support the delivered baseline throughout its defined support period.

7 Supplier software and externally sourced components

7.1 Software purchasing and integration agreements shall define deliverables, supported hardware, interfaces, diagnostic access, change notification, defect reporting and support responsibilities. Acceptance shall require evidence appropriate to the function, including version identity, known limitations, verification scope and installation constraints. A supplier declaration alone shall not close the integrator requirements for vehicle compatibility and intended use.

7.2 Supplied binaries, libraries and model assets shall enter a controlled intake process. The receiver shall check provenance, integrity, licence and permitted use, component inventory and the availability of vulnerability or defect information. Missing source code does not remove the obligation to assess the component; the programme shall establish suitable test, assurance and support evidence for the supplied form.

7.3 The programme shall assess the effect of a supplier change on vehicle behaviour, build reproducibility, factory programming and service recovery. Changes to packaging, signing, dependencies or calibration may be significant even when the supplier reports no functional change. Unannounced replacement of a binary under the same version identifier shall trigger containment and reconciliation.

7.4 Openly distributed components shall be governed by the same quality and configuration principles as purchased components. The organisation shall identify maintenance responsibility, supported versions, licence obligations and the route for receiving and resolving security notices. A publicly available component shall not be presumed suitable for vehicle control merely because it is widely used elsewhere.

7.5 Supplier performance reviews shall consider escaped defects, evidence completeness, response times and the quality of corrective action. Agreements shall preserve access to information needed for incident investigation and affected population identification. Proprietary information shall be protected through controlled access without allowing confidentiality to conceal a release-blocking defect from the responsible authority.

8 Artifact signing, trust and credential control

8.1 The production release process shall distinguish artifact integrity, authorised origin, secure transport and runtime trust. A cryptographic signature can support origin and integrity checks; it does not establish that the software meets functional requirements. Encrypted transfer protects a communication path but does not replace verification of the received release artifact or the intended vehicle compatibility.

8.2 Production signing shall use an approved service with restricted access, protected key material, audit records and separation from development credentials. Where supported by the risk assessment and architecture, protected cryptographic hardware shall hold production keys. Export, backup, rotation and recovery of key material shall follow a controlled procedure that prevents uncontrolled copies and preserves operational recovery.

8.3 The release manifest shall bind the approved artifact identity to its version, target configuration and installation conditions. Verification shall occur at the appropriate trusted points before installation or activation, according to the implemented architecture. A failed signature, altered artifact, untrusted signer or incompatible target shall stop the transaction and produce a recorded hold rather than a manual bypass option.

8.4 The programme shall define certificate and key validity, revocation, replacement and compromise response. Production stations shall handle unavailable or uncertain trust services through an approved bounded mode or a hold condition. Clock validity shall be considered where it affects credential decisions. Expiry shall not be resolved by casually changing a station clock or disabling certificate checking.

8.5 Development identities and production identities shall be segregated. Vehicle specific credentials shall be provisioned through an approved process and shall not appear in ordinary traceability exports or screenshots. The vehicle record shall retain non-secret identifiers and provisioning status. Discovery of exposed credentials shall trigger containment, scope assessment and controlled replacement before affected vehicles are released.

9 Verification strategy and test environment control

9.1 The verification plan shall combine appropriate code analysis, unit testing, component integration, simulated plant testing, hardware testing and physical vehicle testing. Each level shall state the behaviour it can demonstrate and its limitations. In this manual, software in the loop means executable software tested against a simulated environment; hardware in the loop adds actual controller hardware but still depends on the fidelity of the simulated plant.

9.2 Test environments shall have identified hardware, software, models, signal mappings, time bases and tool configurations. Test data and expected results shall be controlled. The team shall verify the test equipment itself with known inputs, seeded faults or reference cases as appropriate. A defective test oracle or incorrect signal mapping can produce a false pass and shall be treated as an assurance risk.

9.3 Coverage shall include normal operation, boundaries, invalid inputs, communication loss, reset, interrupted power, degraded states and recovery relevant to the function. Fault injection shall occur in a controlled laboratory or an expressly approved safe setup. Test commands capable of unintended actuation shall not be sent to ordinary production vehicles or networks as an exploratory shortcut.

9.4 The team shall retain raw results, observed deviations and the exact tested configuration. Repeating a failed test shall not erase the original failure. The reason for repetition, any changed condition and the disposition of inconsistent results shall be recorded. A flaky or non-deterministic test shall be investigated rather than repeatedly rerun until it produces a convenient pass.

9.5 Test completion shall be assessed against approved coverage and acceptance criteria, not solely the number of tests executed. Physical checks remain necessary where simulation cannot adequately represent vehicle dynamics, sensors, electrical behaviour or environmental effects. Evidence from another variant may be reused only after a documented equivalence assessment identifies the shared assumptions and remaining differences.

10 Powertrain control software quality

10.1 Powertrain verification shall cover commanded and actual torque behaviour, operating state transitions, interlocks, sensor plausibility, thermal constraints and the response to relevant faults. The responsible engineering team shall define the approved operating envelope and safe test method for each propulsion variant. This manual does not prescribe torque, speed, current or temperature settings.

10.2 Calibrations affecting propulsion shall have controlled identity, approved limits and traceability to their supporting evidence. A calibration used to improve a single test result shall be reviewed for effects on other operating conditions, durability, energy use, drivability and protection functions. Temporary engineering calibrations shall be clearly segregated and blocked from ordinary customer release.

10.3 Integration tests shall examine communication between propulsion controllers, braking and stability functions, battery management and driver demand interfaces where applicable. The test plan shall include stale messages, conflicting requests, loss of expected data and restart sequences. The intended priority and degraded response shall be defined before tests are run.

10.4 Factory functional tests that can create motion or energise rotating equipment shall use a validated guarded setup, suitable restraints and trained personnel. Programming success shall not authorise propulsion activation. The station shall verify the vehicle state and the required interlocks before a test and shall return the vehicle to an identified safe state afterward.

10.5 Unexpected torque, incorrect direction, uncontrolled movement, defeated protection or unexplained control instability shall block release of the affected configuration and population. Investigation shall preserve software and calibration identity, logs, test conditions and physical findings. The corrective action shall include appropriate regression across interacting functions rather than only the condition that first revealed the defect.

11 Battery management and charging software quality

11.1 Battery management verification shall address measurement plausibility, state estimation, balancing, contactor control, charging communication, thermal management and protection responses within the approved battery architecture. The plan shall identify cell and pack variants, sensor arrangements and relevant hardware tolerances. Software assumptions about the battery shall be supported by the actual hardware configuration and product evidence.

11.2 State of charge and state of health estimates shall be assessed against defined reference methods and operating conditions. The acceptance plan shall cover uncertainty, initialisation, ageing and recovery from interrupted or inconsistent data where relevant. A displayed percentage alone shall not demonstrate adequate estimation quality or prove that a protection function operates correctly.

11.3 Charging tests shall consider authorised operating states, communication loss, incompatible requests, interrupted sessions, restart and limits imposed by the vehicle or charging equipment. Dangerous fault conditions shall be represented using approved test rigs or other controlled methods. Deliberately stressing a production battery beyond its validated envelope is not an acceptable routine software verification technique.

11.4 Factory loading shall follow the approved low voltage supply and high voltage state requirements for the particular vehicle and equipment. The engineering team shall define the permissible contactor state, charging connection state and isolation controls. The station shall not infer electrical safety from a dashboard indication or from the fact that a software programming session has started.

11.5 Incorrect protection thresholds, unintended contactor operation, invalid thermal control or unexplained battery safety diagnostics shall trigger a release hold and the applicable technical response. A fault shall not be closed by disabling a monitor, clearing its evidence or substituting an unvalidated limit. Physical battery concerns shall transfer to the site battery safety and incident procedures as well as software investigation.

12 Driver assistance software, models and calibration

12.1 Each driver assistance feature shall have a defined intended use, operating domain, driver role, activation conditions and limitations. The operating domain shall identify relevant road, speed, environment, visibility and infrastructure assumptions as appropriate. A feature shall not be described or released beyond the capability supported by its evidence and approved customer information.

12.2 The configuration baseline shall include sensor hardware, mounting and alignment data, perception model versions, preprocessing, decision logic and calibration. The team shall assess the effect of sensor replacement, body repair, lens contamination, changed mounting or software updates on performance. EOL calibration shall use an approved target arrangement and controlled conditions appropriate to the actual sensor system.

12.3 Model verification shall use traceable datasets and scenarios with defined coverage, labels and acceptance criteria. Training, tuning and independent evaluation data shall be separated to prevent optimistic results from data leakage. Review shall consider uncommon but consequential scenarios, different environments and changes in sensor characteristics; a single aggregate accuracy figure shall not close the feature requirements.

12.4 Simulation and replay testing shall be correlated with appropriate physical evidence, with limitations recorded. Connectivity tests and factory calibration checks do not demonstrate performance across the driving domain. Tests involving moving vehicles or automated control shall occur only under an approved plan with trained personnel, controlled access and an appropriate intervention and recovery arrangement.

12.5 Incorrect intervention, missed critical detection, misleading driver status or operation outside the approved conditions shall receive a severity assessment based on potential consequence and exposure. A model update shall be treated as a controlled software change, including regression and compatibility review. Delivered vehicles shall retain the exact feature and model baseline needed for investigation and authorised service.

13 Diagnostics, connected interfaces and privacy

13.1 Diagnostic access shall be limited to approved identities, tools, functions and vehicle states. The architecture shall protect programming and privileged configuration from unauthorised access. Production diagnostics shall be separated from unrestricted engineering capability, with logging sufficient to attribute significant actions without exposing credentials or unnecessary personal data.

13.2 Connected interfaces shall define authentication, authorisation, message validation, replay resistance, freshness and failure handling appropriate to the function. A cloud connection shall not provide unrestricted control over torque, braking, steering or other critical actuation. Any remotely requested action shall pass the vehicle architecture controls, state checks and functional constraints established for that feature.

13.3 The programme shall define what happens during network loss, excessive latency, duplicate messages, out of order delivery, stale data and unavailable services. The response shall be feature specific and compatible with the vehicle safety concept. A universal rule to continue indefinitely or stop immediately is inappropriate where functions have different operating consequences.

13.4 Cloud and factory tests shall use approved test accounts and synthetic or suitably controlled data. Production customer credentials shall not be copied into development scripts. Logs shall collect the data necessary for diagnosis, with role based access and defined retention. Sensitive vehicle identifiers shall be pseudonymised where practical for analytical use, while preserving authorised traceability.

13.5 Security findings shall enter a controlled assessment and remediation process with restricted technical detail where necessary. The organisation shall evaluate affected releases and vehicle populations, contain exposure and verify corrective action. Tests shall remain within authorised systems and approved methods; access control bypasses or unapproved scanning of live production networks are outside routine quality verification.

14 Procedure: approve a software release candidate

Use this procedure when a baseline is proposed for production installation. Approval identifies the permitted vehicle population and use; it is separate from the later release of each programmed vehicle.

Step / owner	Required action and evidence
1 Release owner	Freeze the proposed baseline and record every image, calibration, model asset, configuration rule and dependency. Identify the target hardware, vehicle variants, build provenance and intended factory or service use.
2 Verification lead	Reconcile the requirement matrix with completed results. Confirm that test environments and physical evidence support the claimed scope. Record incomplete coverage, inconsistent results and restrictions without deleting failed attempts.
3 Integration lead	Review multi-controller compatibility, startup and recovery behaviour, cloud interface dependencies and service replacement paths. Confirm that installation instructions and supported recovery versions match the candidate baseline.
4 Safety / security	Assess open findings and the effect of the change. Confirm required protection, trust and privacy evidence. Identify release-blocking issues and any eligible residual issues with explicit conditions and accountable acceptance.
5 Manufacturing / Quality	Verify station readiness, programming time and power assumptions, post-load tests, traceability and population hold controls. Demonstrate that an incompatible or failed vehicle is prevented from ordinary delivery.
6 Release authority	Approve or reject the named baseline with scope, conditions and actual signatures. Promote only the approved artifacts and manifest. Notify affected sites and retain the complete evidence index and revision history.

A conditional approval shall identify the exact permitted activity and shall not be interpreted as unrestricted customer release. Missing critical evidence or an unresolved release-blocking issue keeps the candidate on hold. Annex A and Annex B support the decision record.

15 EOL programming station readiness

15.1 The station owner shall maintain an approved equipment configuration covering programming interfaces, network paths, local storage, power support, test instruments and operator software. Station software shall be controlled independently of the vehicle release it installs. A station change shall receive an impact assessment and verification before it is used for unrestricted production.

15.2 The station shall positively identify the vehicle and reconcile its build configuration with the authorised release manifest. It shall detect an incorrect or duplicate identity and prevent an operator from casually substituting another vehicle record. Any manual identity correction shall preserve the original entry, the reason, supporting evidence and approval by an authorised role.

15.3 The validated instruction shall define low voltage support capacity, permitted supply conditions, connection sequence and the required high voltage state for the specific operation. It shall address interruption, overheating, connector damage and loss of communication. Generic voltage values or an assumption that the traction battery will maintain programming power shall not replace equipment and vehicle specific engineering requirements.

15.4 The station shall verify required guarding, vehicle immobilisation, ventilation and access controls for any functional tests included in the cycle. Tool self-checks, measuring equipment status, clock synchronisation and storage capacity shall be checked as relevant to the record. A station unable to preserve reliable results or apply a mandatory interlock shall be unavailable for production release.

15.5 Readiness verification shall include controlled negative tests such as a wrong variant, corrupt test artifact, unavailable credential service or simulated loss of a required connection. These tests shall use approved fixtures or safely isolated arrangements. The expected result is a controlled rejection or recovery state with preserved evidence, not continued operation through an undocumented bypass.

16 Procedure: securely install vehicle software at EOL

The approved vehicle and station instructions govern the exact connection and programming sequence. This procedure establishes the quality gates and records that shall surround that sequence.

Step / owner	Required action and evidence
1 Operator / station	Identify the vehicle, work order, hardware and required baseline. Confirm the approved vehicle state, power support, access controls and station readiness. Reject a configuration mismatch before beginning transfer.
2 Station service	Retrieve the authorised manifest and artifacts through the approved path. Verify their integrity, trusted origin, target compatibility and release status. Record the identity of the verified package without exporting secret credentials.
3 Programming controller	Enter the approved programming state and execute the versioned installation plan. Monitor power, communication and required interlocks. Capture start time, controller identity, progress and error events against the actual vehicle record.
4 Programming controller	Verify transferred content and activate it only under the permitted conditions. Coordinate dependent controllers as specified. Do not infer activation or successful execution solely from completion of a data transfer.
5 Test station	Read back installed identities and perform the required startup, diagnostic and functional checks. Reconcile all planned controllers and calibrations. Preserve failures, retries and recovery actions as part of the same vehicle history.
6 Quality / release	Assign pass or hold based on the complete criteria. Secure any failed vehicle for authorised recovery. Release only when the as-installed baseline and required results are complete and the vehicle record is linked to the production identity.

An interruption shall invoke the approved recovery instruction for that controller and state. Operators shall not improvise cable disconnection, power cycling, image substitution or security bypasses. Annex C and Annex D provide readiness and vehicle programming records.

17 Multi-controller activation and recovery

17.1 The integration owner shall define the dependency graph for controllers that must operate as a compatible group. The installation plan shall specify ordering, staging, activation and the conditions under which mixed versions may exist temporarily. A temporary installation state shall not be assumed suitable for driving, charging or customer delivery.

17.2 Where the architecture supports coordinated or atomic activation, the team shall verify its actual guarantees and failure cases. Where it does not, the plan shall provide controlled intermediate states and recovery actions. A partial update that leaves an unsupported combination shall create a vehicle hold, even if each individual controller reports a successful local programming result.

17.3 Dual-bank or A/B update arrangements may support recovery where the hardware and software implement them. Their availability shall not be assumed for every ECU. Tests shall verify selection of the active image, health checks, interrupted activation and preservation of essential data using a safe test setup representative of the production configuration.

17.4 Recovery shall respect the product security floor and compatibility requirements. Returning to a previous approved image is permitted only when that image remains authorised, compatible and allowed by the implemented rollback protections. An arbitrary downgrade to an older version shall not be used to bypass a failed update or a security restriction.

17.5 The approved recovery record shall identify the failed stage, observed controller state, permitted action and required retests. If the state cannot be established reliably, the vehicle shall remain secured for specialist diagnosis. Recovery success shall include a reconciled complete vehicle baseline and functional checks; merely restoring communication with one controller is insufficient.

18 Post-installation diagnostics and configuration checks

18.1 Post-installation verification shall confirm the identity and operational state of all required controllers, calibrations and feature configurations. The test shall detect a skipped controller, unintended default coding, wrong regional configuration or missing model asset where relevant. Results shall be associated with the installed baseline rather than only the work order target.

18.2 Diagnostic evaluation shall distinguish expected transient records created by an approved programming sequence from unexplained, recurring or safety relevant faults. The instruction shall define which records may be cleared, when they must be read again and which evidence must be preserved. Clearing diagnostic trouble codes shall not itself constitute a repair or a passing result.

18.3 Configuration checks shall include required commissioning routines, sensor calibration states, network communication and feature availability. The programme shall define the conditions for checking sleep, wakeup, reset and retained data where these affect delivery quality. A routine completion flag shall be supported by a validated routine and its required preconditions.

18.4 The station shall verify the production disposition of development functions, temporary accounts, test certificates and debug access. Required production credentials shall be confirmed without exposing their secret content. Test data and simulated customer profiles shall be removed or isolated according to the approved delivery process, with evidence that the intended production state has been established.

18.5 Any contradiction between the vehicle response, controller report and station result shall be investigated. The system shall not select the most favourable source automatically. Quality shall define the hold scope, preserve relevant logs and require a corrected test or technical disposition before the affected vehicle can proceed to final release.

19 Cloud test planning and environment separation

19.1 The connected service owner shall define the scope of cloud testing, including vehicle enrolment, identity, data exchange, service discovery, commands and user-facing status applicable to the release. Each test shall specify whether it exercises a development environment, a production-like environment or an approved production verification path. Environment names shall be visible in the test record.

19.2 Development and production identities, endpoints and credentials shall be separated. Production connectivity checks shall use controlled accounts and authorised services with a defined cleanup process. Test vehicles shall not be accidentally enrolled to a real customer or left associated with a temporary operator account at delivery.

19.3 The plan shall define expected behaviour for connection establishment, authentication, authorisation, time validity, message acknowledgement and state synchronisation. It shall distinguish a network connection from successful application processing. A service response shall be checked against the intended vehicle identity and request context, not simply against receipt of any successful response code.

19.4 Network impairment and service fault tests shall include relevant latency, interruption, duplicate delivery and stale data scenarios. Their severity and duration shall be chosen from the feature requirements and controlled test capability. Disruptive scenarios shall run in isolated environments or specifically approved windows with containment; ordinary production services shall not be intentionally degraded without authorisation.

19.5 The test owner shall define privacy controls, permitted logging and data deletion or retention. Vehicle location, identifiers and diagnostic details shall be collected only to the extent needed for the test and authorised purpose. The evidence shall prove the required behaviour while avoiding unnecessary copies of sensitive data across engineering, factory and supplier systems.

20 Procedure: verify connected vehicle services

Use the approved cloud test plan and a vehicle or rig in a defined safe state. This procedure evaluates connected service behaviour within its stated scope and does not replace physical validation of vehicle functions.

Step / owner	Required action and evidence
1 Test owner	Confirm environment, vehicle identity, software baseline, account ownership and approved test scope. Verify safe vehicle state and permission for each requested function. Identify the expected response and allowable timing before execution.
2 Test system	Establish the authorised connection and verify endpoint trust and identity binding. Record non-secret credential identifiers, service versions and time basis. Reject an identity mismatch or unexpected environment.
3 Test engineer	Exercise approved normal exchanges and compare vehicle, cloud and application states. Verify message content, acknowledgement, freshness and completion. Confirm that a reported success corresponds to the intended operation.
4 Controlled environment	Execute authorised interruption, delay, duplicate and stale-message scenarios. Verify the defined degraded response and recovery. Preserve observations showing that invalid or unauthorised requests do not gain unintended capability.
5 Integration owner	Reconcile logs across systems and investigate contradictory states or missing events. Restore the approved connection and account state. Repeat only the justified scope while retaining the original failure record.
6 Quality / service owner	Approve the scoped result or assign a hold. Remove temporary accounts, test data and unneeded privileges as instructed. Link evidence to the release or vehicle record and document any remaining service restriction.

An unavailable service shall not be recorded as a pass. A specifically approved deferral may be used only when the release criteria permit it, the affected feature is identified and completion or customer communication is controlled. Annex E records the test and cleanup evidence.

21 EOL functional tests and physical validation boundaries

21.1 The EOL test plan shall identify which functions can be verified safely and repeatably within the factory cycle. It shall define equipment, vehicle state, preconditions, measured outputs and acceptance limits. Tests shall be selected to detect relevant installation, configuration and assembly defects while preserving the separate product validation evidence for the full operating domain.

21.2 Any test that may move the vehicle, rotate equipment, energise high voltage or activate actuators shall require an approved controlled setup. The test instruction shall specify guarding, restraints, exclusion zones, competent personnel and safe termination. An operator software prompt shall not be treated as the sole protective measure for a hazardous physical test.

21.3 Sensor and actuator checks shall consider the complete measurement chain and whether the test stimulus represents the intended physical condition. Simulated messages can verify software paths but may bypass a damaged sensor, wiring fault or mechanical misalignment. The test owner shall identify these limitations and provide complementary checks where the defect risk requires them.

21.4 Test limits shall account for equipment capability and repeatability. Borderline results shall follow a defined decision rule and escalation route. Repeatedly retesting until a result enters tolerance shall not be permitted without a documented cause and disposition. Station correlation and maintenance shall be reviewed when results drift or disagree across otherwise equivalent equipment.

21.5 A successful EOL cycle shall not be presented as complete ADAS driving validation, long-term battery durability evidence or proof of every powertrain operating condition. The delivery record shall combine the appropriate product baseline approval with the vehicle-specific factory checks. Where an essential physical test remains incomplete, the vehicle release status shall clearly reflect the resulting hold or permitted restricted use.

22 Defect intake, severity and reproducibility

22.1 Every observed software anomaly shall receive a unique record containing the affected configuration, source of discovery, expected and actual behaviour, test conditions and available evidence. The report shall identify whether vehicle safety, security, privacy, regulatory obligations, core function or production continuity may be affected. Uncertainty about consequence shall trigger assessment, not automatic assignment to a minor category.

22.2 Severity shall describe potential consequence; priority shall describe the planned order of work. The programme shall define severity classes and release rules before using them to close defects. A rare occurrence may still be critical. A production inconvenience may be urgent without having the same safety consequence. Both dimensions shall remain visible in the record.

22.3 The investigation shall seek a reproducible case using a controlled environment and retained configuration. Capture shall include relevant logs, timing, network state, power state, input sequence and physical observations. Sensitive data shall be restricted. An inability to reproduce the issue immediately shall not erase the original evidence or justify closing a credible consequential defect as no fault found.

22.4 Triage shall determine containment and affected population while the root cause is investigated. The team shall consider shared components, common calibrations, hardware variants and delivered vehicles. Where reliable population boundaries are unavailable, the hold shall cover the reasonably affected scope until traceability or evidence supports a narrower decision.

22.5 The record shall distinguish suspected cause, confirmed cause, corrective change and verified result. A workaround shall be identified as such with conditions and expiry. Reports submitted through service, complaints or protected reporting channels shall enter the appropriate technical process without retaliation or pressure to conceal the finding.

23 Procedure: correct a defect and verify regression

The defect owner shall coordinate a controlled correction. A successful reproduction or a code change is an intermediate result; closure requires evidence that the issue is resolved without unacceptable effects on dependent functions.

Step / owner	Required action and evidence
1 Triage team	Confirm the defect record, severity, affected baseline and containment. Preserve the original evidence and define the expected corrected behaviour. Escalate potential safety or security consequences to the responsible specialists.
2 Engineering	Determine and document the root cause or the best supported causal explanation. Identify related code, calibration, interfaces, hardware assumptions and tests. Record uncertainties requiring further investigation.
3 Change owner	Implement the reviewed correction under configuration control. Add or improve a test that meaningfully detects the failure where feasible. Assess effects on timing, resources, compatibility, protection and connected services.
4 Verification lead	Reproduce the original failure on the appropriate baseline where safe, then verify the correction. Execute the justified regression scope, including affected variants and physical tests. Retain failed attempts and changed test conditions.
5 Independent reviewer	Review evidence, remaining anomalies and the impact assessment. Confirm that a monitor was not simply disabled and that acceptance criteria were not weakened to produce a pass. Approve closure or return the issue for further work.
6 Release / Quality	Promote the corrected baseline through release approval. Define factory rework, service or update actions for the affected population. Close containment only after implementation and effectiveness evidence support the decision.

A defect shall be reopened when recurrence or new evidence invalidates the closure. Annex F supports the defect, correction and verification record; configuration changes shall also update the applicable release manifest and vehicle history.

24 Release holds, concessions and residual issues

24.1 The programme shall define release-blocking conditions, including unresolved critical safety or security issues, unauthorised artifacts, incompatible controller combinations, missing required verification and unreliable vehicle traceability. These conditions shall prevent ordinary delivery through the production control system and a visible physical or equivalent controlled hold arrangement.

24.2 A concession may address an eligible, understood and bounded noncritical deviation only through the designated authority. The record shall identify affected vehicles, permitted use, technical rationale, risk assessment, conditions, expiry and completion plan. No concession shall waive mandatory obligations, conceal a critical defect or substitute for missing essential protection.

24.3 Residual issues accepted for a release shall remain in an accessible register linked to the baseline. Acceptance shall state why the intended use remains acceptable, what monitoring or restrictions apply and who owns resolution. The existence of an open issue shall not be hidden by changing its label from defect to enhancement without a supported reassessment.

24.4 Hold controls shall address vehicles already programmed, vehicles awaiting delivery and affected units at other facilities. Production and logistics systems shall reconcile status so that a blocked vehicle cannot leave through an alternative route. Removing a hold requires documented completion of the required action and confirmation by the authorised release role.

24.5 Where a production or customer issue is discovered after release, the organisation shall assess potential consequences and population promptly. Applicable incident, service and communication processes shall be activated by their responsible authorities. A technical manual does not itself determine notification duties; the organisation shall evaluate and fulfil the requirements relevant to the actual event and jurisdiction.

25 Procedure: release a programmed vehicle for delivery

This procedure joins the approved product baseline to the actual vehicle evidence. It shall be performed after all mandatory software, configuration, assembly and final inspection gates applicable to the vehicle are complete.

Step / owner	Required action and evidence
1 Production record	Reconcile the vehicle identity, build variant, hardware and installed software baseline. Confirm that replacements, recovered controllers and rework are included. Investigate missing or contradictory identifiers.
2 Quality system	Confirm required programming, post-load diagnostics, calibration and functional test results. Check completeness of connected service verification where required for release. Preserve links to the original results and any justified retests.
3 Release controller	Check open defects, concessions, campaigns and vehicle holds against the actual configuration. Confirm that no release-blocking condition remains and that any permitted residual issue has an applicable, unexpired approval.
4 Delivery preparation	Verify production account and credential state, removal of temporary test data and required customer feature information. Confirm that development functions and temporary engineering configuration have their approved disposition.
5 Authorised reviewer	Approve or reject the individual vehicle using the defined evidence set. Record identity, date, baseline and release decision. Do not substitute an aggregate batch pass for a missing vehicle-specific mandatory check.
6 Records / service	Lock the as-delivered passport against untracked edits and make the necessary information available to authorised service functions. Retain recovery and support references, while protecting sensitive security and personal information.

If a record is corrected after release, retain the original, reason, supporting evidence and approving identity. A correction shall not retrospectively assert that an unperformed test occurred. Annex G provides the vehicle release passport fields.

26 Post-delivery updates, service and incident feedback

26.1 The software quality lifecycle continues after delivery. The programme shall maintain a support plan covering defect intake, security information, service compatibility, update eligibility and retirement of connected dependencies. The plan shall identify the supported vehicle population and the organisation responsible for each software component and customer-facing function.

26.2 Updates delivered remotely or through authorised service shall pass the applicable release, compatibility, trust and verification gates. The update plan shall define vehicle preconditions, user information where relevant, interruption handling, permitted recovery and confirmation of the installed result. Factory approval of an image does not automatically prove that its remote installation process is suitable.

26.3 Rollout monitoring shall distinguish attempted, successful, failed, deferred and unknown outcomes. The organisation shall define pause conditions and investigate unexpected vehicle behaviour or excessive failure rates before expanding deployment. A lost reporting connection shall not be assumed to mean either successful installation or a safe failure state without the required supporting evidence.

26.4 Service replacement and repair shall reconcile the complete vehicle configuration and relevant calibration requirements. Technicians shall use approved tools and instructions, preserve useful diagnostic evidence and record the resulting baseline. A workshop workaround shall not silently become a fleet software change or an alternative route around production release controls.

26.5 Field findings shall feed requirements, test coverage, factory controls and supplier corrective action. The organisation shall periodically review whether the original assumptions remain valid as hardware ages, services change or new operating conditions emerge. Incident investigation shall preserve records and provide the technical evidence needed by the responsible safety, security, privacy and customer response functions.

27 Competence, metrics and independent assurance

27.1 Role authorisation shall match the task and its consequences. Competence requirements shall cover software configuration, programming equipment, vehicle electrical and movement hazards, diagnostics, data handling and escalation as relevant. Practical demonstration shall supplement awareness training for tasks such as station recovery, release review and physical functional testing.

27.2 The site shall monitor first-pass programming yield, recovery frequency, configuration mismatch rate, test escape findings, traceability completeness and time to contain significant defects. Each metric shall define its population, denominator, exclusions and observation period. Reworked vehicles and repeated attempts shall remain visible rather than being counted as new independent successful vehicles.

27.3 For illustration, if 200 vehicles enter programming and 190 complete all required programming checks on their first attempt, first-pass yield is $190 / 200 \times 100 = 95\%$. If eight of the remaining vehicles later pass approved recovery and two remain on hold, eventual pass rate is $198 / 200 \times 100 = 99\%$. The recovery success does not change the original first-pass result.

27.4 Independent audits shall sample the chain from approved baseline to artifact, station record, installed vehicle identity and release decision. Auditors shall challenge whether a failed test can be bypassed, an expired concession reused or a missing controller result concealed. Safe demonstrations shall use controlled test records or fixtures rather than deliberately creating unsafe live vehicle states.

27.5 Management review shall assess recurring failures, supplier performance, audit results, support risks and the effectiveness of corrective action. Numeric targets shall not encourage suppression of defects or premature closure. Improvement actions shall have owners, dates and evidence of effect on vehicle quality and reliable release decisions. Annex H provides a review worksheet.

28 Documents, retained evidence and IAF interfaces

28.1 Documents and records shall follow the IAF Documents and Records Guide for ownership, identification, revision, access, retention, archival and controlled disposal. The site shall maintain a retention schedule appropriate to vehicle support, contractual duties and mandatory obligations. This manual does not prescribe a universal retention period for every record or jurisdiction.

28.2 The minimum evidence set shall include adopted instructions, requirements, architecture and compatibility baselines, source and build provenance, release approvals, test results, signing and provisioning audit references, station readiness, programming transactions, defect dispositions and vehicle passports. Security secrets shall be held in their approved protected systems rather than copied into general quality files.

28.3 Records shall identify who performed or approved an action, when it occurred, the configuration involved and the outcome. Time bases shall be controlled where events from different systems are correlated. Amendments shall preserve the original information and reason for change. Backup, restoration and long-term readability shall be tested in proportion to the importance and retention period of the evidence.

28.4 The manual interfaces with IAF-MAN-DTV-001 for virtual test environments, IAF-MAN-NPI-001 for prototype and launch evidence, IAF-MAN-OTC-001 for factory operational technology controls, IAF-MAN-GAA-001 for relevant EV assembly activities and IAF-MAN-ASM-001 for authorised service. The applicable IAF Quality Manual, confidentiality, privacy, complaints and conflict of interest controls also remain relevant.

28.5 Membership, Corporate Recognised status, accreditation and mark permissions shall follow their respective IAF processes and approved scopes. Software quality records shall not be represented as proof of a broader recognition that has not been granted. Revisions to this manual shall be issued and communicated through the authorised IAF document process; sites shall assess impacts before changing active operating instructions.

Annex A - Release baseline and compatibility record

Purpose: establish the exact software combination proposed for a defined vehicle population. Attach controlled lists where the number of components exceeds the worksheet. Enter actual evidence references; an empty field is not an acceptance.

Field	Required entry / verification
Record identity	Release record ID; programme; owner; date; revision; intended factory or service use.
Vehicle population	Models and variants; hardware part numbers and revisions; equipment options; regional configuration; explicit exclusions.
Component manifest	ECU identity; executable and boot versions; calibration; model assets; configuration rules; integrity and provenance references.
Dependencies	Permitted companion versions; interface versions; cloud dependencies; installation order; temporary mixed-state restrictions.
Build evidence	Source and toolchain identity; dependency inventory; verified build result; reproducibility evidence or approved limitation.
Trust controls	Authorised signing reference; credential policy; verification method; security floor and approved recovery constraints. Do not enter secrets.
Verification summary	Requirements coverage; test environment identities; physical evidence; unresolved anomalies; accepted restrictions.
Factory / service	Approved installation instruction; station capability; recovery method; post-installation checks; support responsibility.
Decision	Approved / restricted / rejected; exact scope; conditions; release authority; independent reviews; actual signature references.

Decision check

Confirm that every target variant has a permitted complete combination and that the actual promoted artifacts match the approved manifest. A supplier version statement or successful signature check alone does not establish release readiness.

Annex B - Requirements and verification matrix

Purpose: demonstrate that each claimed requirement has suitable evidence. Repeat the requirement row structure for the full scope and maintain links to the original results, including failures and justified retests.

Field	Required entry / verification
Requirement identity	Unique ID; approved revision; intended function; source within the programme; accountable owner.
Operating conditions	Target variants; hardware and software assumptions; valid range; prohibited behaviour; fault and recovery conditions.
Acceptance rule	Measured or observed outcome; limits and timing; uncertainty treatment where relevant; decision rule approved before execution.
Verification method	Analysis, unit, integration, simulation, hardware or physical vehicle method; rationale; limitations and complementary evidence.
Environment	Rig or vehicle ID; models; tools; signal mapping; time basis; data and expected-result revisions; equipment status.
Coverage	Normal and boundary cases; invalid inputs; degraded states; relevant fault scenarios; omitted cases and their justification.
Result	Execution ID and date; actual outcome; raw evidence; pass / fail / incomplete; repeat history and changed conditions.
Issue linkage	Defects and concessions; containment; effect on related requirements; regression evidence after correction.
Conclusion	Satisfied / open / not applicable with rationale; reviewer; approval date; claim scope and residual limitations.

Review question

Could the evidence support the same conclusion if the test outcome had been unfavourable? Check that expected results and acceptance criteria were not revised after observation merely to convert a failure into a pass.

Annex C - EOL station readiness checklist

Purpose: authorise a station for a defined vehicle and release family. Use at initial qualification and after changes according to the approved impact assessment; shift checks may reference the applicable subset.

Checkpoint	Required entry / verification
Identification	Station and location; equipment configuration; operator interface revision; approved vehicle and release families.
Vehicle identity	Scan and reconciliation method; duplicate and mismatch rejection; controlled manual correction route.
Power / vehicle state	Validated support equipment and instruction; connection condition; required high voltage state; interruption response.
Physical protection	Guarding and immobilisation where required; access controls; safe test termination; relevant competence authorisations.
Artifact control	Approved retrieval path; manifest verification; version and compatibility rejection; local cache integrity and release status.
Credentials / network	Environment separation; approved identities; credential validity; protected access; clock and service availability checks.
Results / traceability	Vehicle-linked records; readback verification; required checks; failed-attempt preservation; hold enforcement; storage and recovery.
Challenge tests	Controlled wrong-variant and invalid-artifact cases; approved interruption or service-failure tests; expected and actual rejection behaviour.
Release decision	Open findings; restrictions; maintenance or calibration evidence; station owner and Quality approval; next review trigger.

Stop conditions

Do not authorise production release when the station cannot identify the vehicle, verify the authorised package, maintain required safe conditions, preserve results or prevent delivery after a mandatory failure. Record the owner and action needed to restore readiness.

Annex D - Vehicle programming and recovery traveller

Purpose: retain the actual history of a vehicle programming transaction. Repeated attempts and recovery remain linked to the same vehicle and shall not overwrite the original failure.

Field	Required entry / verification
Vehicle / order	Vehicle identity; work order; build variant; relevant hardware; station; operator or automated service identity.
Target baseline	Approved manifest ID; required controllers, images, calibrations and model assets; compatibility check result.
Preconditions	Readiness record; vehicle state; power support; access and physical safety checks; start time and time basis.
Programming events	Controller and artifact identity; transfer, verification and activation results; relevant timestamps; recorded errors.
Installed readback	Reported versions and configuration; reconciliation with the target; missing or inconsistent identities and disposition.
Required tests	Startup; diagnostics; calibration; functional checks; connected service checks where required; result references.
Recovery history	Failed stage; observed state; approved instruction; responsible specialist; action; replacement parts; repeated checks.
Outcome	First-attempt pass / recovered pass / hold; open issue or concession; restrictions; vehicle release record link.
Authentication	Record creation identity; review and approval references; amendment history; protected storage location.

Evidence integrity

Retain non-secret credential identifiers where needed for traceability, but keep private keys and sensitive access material out of the traveller. A completed transfer without activation and required post-load evidence shall not be recorded as a complete programming pass.

Annex E - Connected service verification record

Purpose: record a scoped connected service test and the restored delivery state. The worksheet shall distinguish network availability, application processing and actual vehicle response.

Field	Required entry / verification
Test identity	Plan and case revisions; owner; execution date; intended release or vehicle decision; approved scope.
Environment	Development, production-like or authorised production path; endpoint identity; service version; vehicle or rig baseline.
Identity / privacy	Approved test account; vehicle binding; non-secret credential reference; authorised data collection and retention.
Preconditions	Safe vehicle state; permitted functions; clock validity; connection conditions; temporary privileges and limits.
Normal case	Request and expected response; timing rule; actual vehicle, cloud and application state; evidence references.
Impaired cases	Approved delay, interruption, duplicate or stale-message scenario; expected degraded behaviour; actual response and recovery.
Reconciliation	Cross-system log correlation; missing or contradictory events; defects; repeats; effect on release.
Cleanup	Temporary account removal; data disposition; privilege removal; production enrolment and delivery state confirmation.
Decision	Pass / fail / incomplete; permitted deferral if applicable; scope limitations; owner and reviewer approval.

Acceptance boundary

Record unavailable tests as incomplete unless an approved requirement explicitly defines another disposition. A passing cloud exchange cannot substitute for a missing physical function test, and synthetic data shall not be presented as an actual vehicle measurement.

Annex F - Defect, correction and regression record

Purpose: maintain a reviewable chain from observed anomaly to containment, correction and verified effectiveness. Separate known facts from hypotheses and retain the original report.

Field	Required entry / verification
Issue identity	Unique ID; reporting channel; date; affected function; observed and expected behaviour; supporting evidence.
Configuration	Vehicle or rig; hardware; complete software and calibration baseline; environment; relevant input and event sequence.
Assessment	Severity and priority with rationale; safety, security or privacy review; uncertainty; immediate escalation.
Containment	Affected or potentially affected population; holds; delivery or service actions; owner; evidence supporting boundaries.
Cause / correction	Reproduction status; confirmed cause or supported hypothesis; reviewed change; related components and assumptions.
Verification	Original failure evidence; correction test; regression scope and rationale; variants; physical evidence; remaining anomalies.
Release action	Approved corrected baseline; factory rework, service or update plan; compatibility and recovery implications.
Closure	Independent review; residual issues; effectiveness evidence; containment removal authority; date and reopening triggers.
Record protection	Controlled evidence location; privacy and confidential access; retained failed attempts; amendment history.

Closure challenge

Confirm that the corrective action addresses the cause and that the observed failure was not concealed by disabling diagnostics, weakening a limit or suppressing a test. A workaround shall carry its own restrictions and shall not be described as a permanent verified correction.

Annex G - Vehicle software release passport

Purpose: bind the approved product configuration to the actual software state and release decision for an individual vehicle. The passport may be an electronic record with controlled links rather than a printed form.

Field	Required entry / verification
Vehicle identity	Production identifier; model and variant; relevant hardware and options; manufacturing site and completion date.
As-delivered baseline	Complete controller, executable, calibration, model and configuration identity; approved manifest; readback evidence.
Installation history	Programming station and transaction; replacements; retries; recovery; links to original and final results.
Acceptance evidence	Required diagnostics, calibrations, functional tests and connected checks; status of each mandatory gate.
Trust / account state	Production provisioning status; non-secret identity references; development access disposition; test account cleanup.
Open items	Defects, holds, concessions or restrictions; applicability and expiry; confirmation that no release blocker remains.
Delivery information	Approved feature scope and limitations; required customer or service information; support and recovery references.
Decision	Released / restricted / held; accountable authority; actual approval date; signature or electronic approval reference.
Record lifecycle	Custodian; access; retention rule; protected history; subsequent authorised update and service linkage.

Release rule

A baseline approval does not replace vehicle-specific evidence. No blank mandatory field shall be treated as a pass, and a later administrative correction shall not claim that an omitted test was performed. Preserve the distinction between intended and confirmed installed configuration.

Annex H - Performance and assurance review worksheet

Purpose: review software quality and factory installation using defined populations and reliable evidence. Set site targets through management approval; the worksheet does not impose universal performance thresholds.

Measure / topic	Required entry / verification
Review scope	Period; vehicle populations; releases; sites; owners; relevant changes and limitations of the data.
First-pass yield	Unique vehicles passing every required first-attempt programming check / unique vehicles entering programming; exclusions disclosed.
Recovery / holds	Vehicles requiring recovery; causes; eventual pass and unresolved hold counts; repeated attempts separately identified.
Configuration quality	Mismatch and incomplete-readback cases; affected variants; master data causes; effectiveness of prevention controls.
Escaped defects	Confirmed findings after the defined release gate; population and observation period; severity; containment and trend.
Traceability	Sampled vehicles with complete mandatory evidence / sampled vehicles; missing fields; retrieval and restoration findings.
Assurance / competence	Audit findings; safe challenge-test results; role authorisations; training gaps; supplier evidence and support risks.
Actions	Root causes; responsible owners; due dates; approved resources; verification method and effectiveness evidence.
Management decision	Required changes to release gates, tests or capacity; accepted residual risks within authority; next review and escalation triggers.

Interpretation check

Compare like populations and report uncertainty where the sample is small or observation is incomplete. A lower reported defect count is not improvement if reporting has weakened. Use the results to improve controls, while preserving candid escalation and independent release decisions.