

Software Requirements Specification

for

Federation Architecture for
Composed Infrastructure Services
(FACIS)

Convoy Demonstrator

FACIS.CD

Version 1.0 (October 2026)

Published by

eco – Association of the Internet Industry (eco – Verband der Internetwirtschaft e.V.)

Lichtstrasse 43h

50825 Cologne, Germany

Copyright © eco Association of the Internet Industry (eco – Verband der Internetwirtschaft e.V.)

This work is licensed under the Creative Commons Attribution 4.0 International License. To view a copy of this license, visit <http://creativecommons.org/licenses/by/4.0/> or send a letter to Creative Commons, PO Box 1866, Mountain View, CA 94042, USA

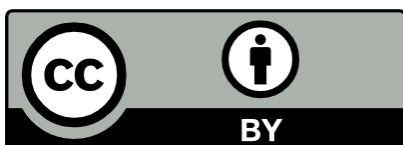


Table of Contents

1. Purpose and exit criteria	1
1.1 Purpose	1
1.2 Exit criteria	1
2. Scope	2
2.1 In scope	2
2.2 Out of scope	2
2.3 Optional positions	3
3. Integration with the XFSC/FACIS tool stack	3
4. Assumptions, constraints and external dependencies	4
5. Functional Requirements	4
5.1 Federation gateway: admission and status (FR-GW)	5
5.2 Geofinder: queue discovery (FR-GEO)	9
5.3 STS: reservation, session and token lifecycle (FR-STS)	11
5.4 Vehicle software: agent, drive logic and protective stop (FR-VEH)	15
5.5 World service and fault injection (FR-SIM)	19
5.6 Dashboard, console, emergency stop and reset (FR-OPS)	20
5.7 Business interface, events and codes (FR-IF)	22
5.8 Configuration profile and fixtures (FR-CFG)	23
5.9 Traffic light, T0 and coordinated release (FR-TL)	24
6. Non-functional requirements	25
6.1 Security and trust (NFR-SEC)	25
6.2 Deployment (NFR-DEP)	26
6.3 Timing (NFR-TIM)	27
6.4 Event log and demonstration evidence (NFR-EVD)	28
6.5 Configuration and repository (NFR-CFG)	28
6.6 Delivery and documentation (NFR-DEL)	29
6.7 Start-delay indicators (NFR-KPI)	30
7. Data and interface definitions	31
8. Architecture and implementation approach	39
8.1 Component overview	39
8.2 Design decisions	40
8.3 Dependencies and licences	40
9. Repository and delivery	40
10. Demonstration and verification	40
10.1 Environment and fixtures	40
10.2 Demonstration scenarios	41
10.3 Edge checks	41
10.4 Unit tests in CI	42
11. Delivery, acceptance and scope control	42
11.1 Change control	42
11.2 Client acceptance	42

12. Storyline traceability	42
13. Glossary	43

1. Purpose and exit criteria

1.1 Purpose

The FACIS Convoy Demonstrator (CD) reproduces an authorised convoy start as software: simulated vehicles of different virtual OEM¹ tenants are admitted through the federation gateway on the basis of verifiable credentials issued by the XFSC OCM W-Stack² and held in PCM Cloud³ (FR-GW-001 ... 004), discovered as a queue by the cloud from their authenticated position reports (FR-GEO-001 ... 005), started as a coordinated wave by one smart-traffic service (STS; FR-STs-001 ... 015), and stopped – on credential invalidation, on loss of a required service or on an injected fault – solely by the local expiry of short-lived release tokens, with authenticated STOP and TOKEN_CLEAR as accelerators only (FR-STs-013, FR-VEH-016).

A simulated traffic light is admitted through the same gateway with its own infrastructure credential and publishes authenticated signal-phase messages with the green-onset time T0 (FR-TL-001). The STS supports two release modes: in motion-proof (default) every follower receives GO only after its wave predecessor has demonstrably moved (FR-STs-006); in coordinated the STS issues follower GO tokens at T0 plus a fixed offset per rank (FR-TL-003). In both modes a follower's approach is bounded by the local distance gate and protective stop (FR-VEH-007, FR-VEH-011).

The Demonstrator shows that a federation decision (admission, invalidation, unavailability) is sufficient to authorise and to withdraw convoy motion end to end without any withdrawal message reaching the vehicle. All components are built on the mandatory XFSC tool stack and deployed in the FACIS cloud environment.

1.2 Exit criteria

The exit criteria are demonstration goals. Each is met when the named scenarios of Section 10.2 have been executed once in the FACIS cloud environment, have shown the described behaviour and are recorded in the demonstration protocol witnessed by the client, and when the named edge checks of Section 10.3 are met in their stated form: T-04, T-05 and T-10 pass in the CI report of the tagged release (NFR-CFG-004); T-12 is shown within M5.

ID	Criterion	Scenarios
E1	Vehicles and the traffic light are admitted with credentials issued by the OCM W-Stack and held in PCM Cloud; invalid, revoked, identity-forged and role-violating requests are rejected; revocation and recovery work through the OCM W-Stack status list.	M1
E2	The reference and the origin-shifted formation are discovered with the correct order and roles; the wave starts in release mode motion-proof (console) and in release mode coordinated (traffic-light T0); the FOLLOW_GAP vehicle stops before the dummy by the protective stop; the session ends in DONE.	M2, M3(a), M3(b), T-05, T-10
E3	Revocation of a rolling vehicle's credential blocks further issuance and the vehicle stops by local token expiry while its business downlink is blocked; unaffected participants complete.	M4
E4	For each demonstrated fault (uplink off, STS stop, convoy-layer stop, sensor invalid, emergency stop with reachable and blocked downlink) every affected vehicle reaches standstill; a reset restores the demo-ready state.	M5, T-04, T-12
E5	The tagged release is deployed with Helm into the FACIS cloud environment on the mandatory tool stack, the runbook is followed by a client operator, and the demonstration recorded by the client.	R

¹ Original Equipment Manufacturer

² <https://github.com/eclipse-xfsc/deployment/tree/main/OCM%20W-Stack>

³ <https://github.com/eclipse-xfsc/deployment/tree/main/PCM%20Cloud>

2. Scope

2.1 In scope

Item	Deliverables
Convoy layer – federation gateway	ORCE flows and custom nodes for admission, verification and status via OCM W-Stack, access tokens and the issuance block (FR-GW-001 ... 015).
Convoy layer – geofinder and STS	One ORCE instance with the geofinder (FR-GEO-001 ... 005) and the single STS with both release modes and the token lifecycle (FR-STS-001 ... 015, FR-TL-002, FR-TL-003).
Convoy layer – business broker	A dedicated MQTT broker over TLS with ACLs (FR-IF-001, NFR-SEC-001, NFR-SEC-004).
Dashboard, console and lab control	Built with the FACIS UI Builder package: operations screen and system-identification screen, console with fault injection, emergency stop and reset (FR-OPS-001 ... 007).
Vehicle software	Three vehicle services, each one ORCE instance with agent and drive logic (FR-VEH-001 ... 017).
World service	Closed 2D track, kinematics, front-distance model and position noise, on a transport independent of the business broker (FR-SIM-001 ... 004).
Simulated traffic light	One ORCE instance admitted with its own OCM W-Stack infrastructure credential (FR-TL-001).
Event log	Structured events shown in the dashboard (NFR-EVD-001, NFR-EVD-004).
Configuration profile and fixtures	One versioned profile with schema and consistency checks, three fixtures and the discovery reference vectors of Table 5g (FR-CFG-001 ... 003).
Deployment	Helm charts for the FACIS cloud environment (NFR-DEP-001 ... 003).
Demonstration and handover	Demonstration script M1–M5 and R, runbook and README (NFR-DEL-001, NFR-DEL-005).

2.2 Out of scope

Item	Reason
Physical vehicles, positioning hardware, embedded boards, a trial day	The HAL and position-source interfaces (FR-VEH-015) are kept so that hardware can be attached later. The traffic light is simulated (FR-TL-001).
Modifying, re-hosting or reimplementing XFSC services	FR-GW-013: OCM W-Stack and PCM Cloud are consumed as provided.
A second STS, a dispatcher, a variable number of participants, more than one intersection	Fixed scope: three participants, one reference dummy, one STS, one traffic light (Table 5).
Following-speed or distance control between vehicles, sensor-assisted convoy mode	FR-VEH-011: distance is only a start gate and a stopping condition.
Any withdrawal message as a precondition for stopping	FR-STS-013, FR-VEH-016.
A physical emergency-stop function	FR-OPS-003: the emergency stop is the laboratory abort of the convoy layer.
Driver or other personal credentials	FR-GW-015.
ETSI ITS PKI certificates, ETSI CAM/SPaT/MAP mappings	Participants are identified with FACIS federation credentials only.
Gaia-X / GXDCH compliance, XFSC Federated Catalogue registration, FACIS Digital Contracting Service, federation-based operator sign-on	No contribution to E1–E5.
Calibration, qualification freeze, repeated acceptance runs, statistical	Not required for a TRL 4 laboratory demonstrator; the witnessed demonstration is the acceptance (NFR-DEL-005).

Item	Reason
KPI and latency evidence, independent evidence re-analysis, safety argument	
Operational QoS targets, availability, endurance	Not required for a laboratory demonstrator.
Operation of the OCM W-Stack, PCM Cloud and the FACIS cloud environment; initial issuance of the test credentials at kick-off	Client conditions precedent (Section 4). Suspension, revocation, recovery and re-issuance during the demonstration and the reset are performed by the CD through the OCM W-Stack (FR-GW-005, Table 5e).

2.3 Optional positions

Options are offered separately from the core scope. An option is delivered only if the client orders it. Requirements that belong to an option carry the priority **OPTION**. An ordered option is accepted separately on the demonstration protocol against the acceptance criteria stated for it (O-1: this table and FR-GW-014; O-2: FR-OPS-010, NFR-KPI-001); its outcome does not affect acceptance of the core scope.

Option	Content
O-1 Dedicated PCM Cloud instance per vehicle	The client provides one PCM Cloud instance per simulated vehicle when it orders O-1 and issues the test credentials into it (condition precedent applies to these instances from the order). After the M1 run of the core scope, the contractor binds each vehicle agent to its own instance, records the holder arrangement and runs M1 a second time with this arrangement, recorded separately in the demonstration protocol (extends FR-GW-014). Acceptance: inspection shows one PCM Cloud instance per vehicle and no shared instance; the second M1 run passes.
O-2 Release-mode comparison and start-delay indicators	Comparison view of the last run of each release mode and start-delay indicators per rank (FR-OPS-010, NFR-KPI-001).

3. Integration with the XFSC/FACIS tool stack

Integration Note (NFR-DEL-002)

The contractor records the credential profile currently supported by FACIS (format, flow, issuer), the OCM W-Stack, PCM Cloud, ORCE and FACIS UI Builder versions, the MQTT broker product, the FACIS trust list used for verification, the holder arrangement per vehicle, whether the OCM W-Stack distinguishes verification sub-reasons, and any client-approved mock.

Native first

Issuance, presentation verification and the status list are consumed from the OCM W-Stack; holders are provided by PCM Cloud (FR-GW-001, FR-GW-003, FR-GW-005, FR-GW-014). A mock may only add a check the OCM W-Stack demonstrably does not provide, never replace a native result, and only with written client approval; it is recorded in the Integration Note and shown with its own **MOCK** label on the dashboard. The admission path of E1 and the invalidation path of E3 always rely on native OCM W-Stack results (FR-GW-003, FR-GW-013, FR-OPS-006).

No silent fallback.

An unreachable OCM W-Stack function produces **SERVICE_UNAVAILABLE**; there is no automatic switch to a mock (FR-GW-010).

Identity scheme

Vehicles and the traffic light are identified with DID-based verifiable credentials issued via the OCM W-Stack (FR-GW-001, FR-TL-001); convoy-layer services hold separate service identities (NFR-SEC-003); no driver or personal credential is used (FR-GW-015).

Environments

The Demonstrator is deployed into and demonstrated in the FACIS cloud Kubernetes environment with Helm (NFR-DEP-001, NFR-DEP-002); all components use the cluster's synchronised clock (NFR-TIM-

006). Development and unit tests may run on contractor systems with a local broker and test doubles of the OCM W-Stack adapters; test doubles are never deployed (FR-GW-013).

4. Assumptions, constraints and external dependencies

Mandatory tool stack

ORCE, OCM W-Stack, PCM Cloud, FACIS UI Builder package, Helm on the FACIS cloud Kubernetes environment (NFR-DEL-002). One STS, three participants, one reference dummy and one traffic light (Table 5). TLS on every network endpoint (NFR-SEC-001); private keys stay with their owner and issuer keys remain with the OCM W-Stack (NFR-SEC-002). Control messages are not retained on the business broker (FR-IF-001). The world service and the vehicles use a transport independent of the business broker (FR-VEH-015). All code under Apache-2.0 in the client-designated repository (NFR-DEL-003, NFR-CFG-003).

The client provides after project start:

- (1) the OCM W-Stack issuance, verification and status list functions, PCM Cloud and the ORCE base images running and supported in the FACIS cloud environment;
- (2) test credentials for CD-V1 ... CD-V3 and the traffic light, issued through the OCM W-Stack into their PCM Cloud holders, and the OCM W-Stack authorisation the federation gateway needs to request issuance, suspension and revocation for these participants;
- (3) a FACIS cloud namespace with ingress, TLS certificates, Helm deployment rights and a namespace-scoped service account that lets lab control scale the CD deployments for fault injection and reset (Table 5d, NFR-DEP-002);
- (4) the FACIS UI Builder package with its documentation;
- (5) access to the client-designated repository and to the FACIS trust list.

Hazard note

Nothing moves physically; the laboratory cannot produce real-world effects. The emergency stop of the CD is the laboratory abort of the convoy layer, not a physical emergency-stop function (FR-OPS-003). The local protective stop, the token logic and the degradation to standstill are specified so that a physical vehicle at a later stage can inherit them; this specification derives no requirement on a physical platform.

Assumptions

- A-1 The reference placement of Table 5f reproduces the roles LEAD, FOLLOW and FOLLOW_GAP with the Table 5 defaults (gap threshold, lane threshold, noise).
- A-2 The stopping-distance relation $d_{\min} > v_{\max} \times (\text{sensor_max_age} + \text{delta_local}) + v_{\max}^2 / (2 \times a_{\text{brake}}) + \text{margin}$ holds with the Table 5 defaults (about 0.85 m headroom, noise-free); it is checked for the loaded profile at start (FR-CFG-002).
- A-3 The ARMED and ROLLING timeouts of Table 5 exceed the durations of the demonstration scenarios, including $T_0 + 2 \times \text{offset}$ for coordinated mode.
- A-4 The status-list propagation time of the OCM W-Stack is short compared with the token TTL; it is shown in the event log, not qualified.

5. Functional Requirements

Every requirement is stated with identifier, name, priority (MUST HAVE / OPTION), group, requirement text and acceptance criteria. Requirement text uses MUST / MUST NOT / SHOULD / MAY in their RFC 2119⁴ sense. Acceptance criteria name the scenario (M1 ... M5, R), edge check (T-04, T-05, T-10, T-12), integration test (Section 11.1), unit test that provides the evidence. A criterion that names none of these is evidenced by the scenario named in another criterion of the same requirement; where there is none, by inspection of the tagged release or of the demonstration event log, recorded in the demonstration protocol.

⁴ <https://rfc-editor.org/rfc/rfc2119>

Overview of the 9 groups (67 requirements):

Group	Identifiers (numbers)	MUST	OPTION
Federation gateway (FR-GW)	001, 002, 003, 004, 005, 006, 007, 008, 009, 010, 011, 012, 013, 014, 015	15	0
Geofinder (FR-GEO)	001, 002, 003, 004, 005	5	0
STS (FR-STS)	001, 002, 004, 005, 006, 007, 008, 009, 010, 012, 013, 014, 015	13	0
Vehicle software (FR-VEH)	001, 002, 004, 006, 007, 008, 009, 010, 011, 012, 013, 014, 015, 016, 017	15	0
World service (FR-SIM)	001, 002, 003, 004	4	0
Dashboard, console, emergency stop, reset (FR-OPS)	001, 002, 003, 004, 006, 007, 010	6	1
Business interface (FR-IF)	001, 002	2	0
Configuration profile and fixtures (FR-CFG)	001, 002, 003	3	0
Traffic light, T0, coordinated release (FR-TL)	001, 002, 003	3	0
Total		66	1

5.1 Federation gateway: admission and status (FR-GW)

ID	Name	Priority
FR-GW-001	Credential profile via OCM W-Stack and PCM Cloud	MUST HAVE
FR-GW-002	Access-token identity binding	MUST HAVE
FR-GW-003	Presentation verification via OCM W-Stack	MUST HAVE
FR-GW-004	Admission decision and typed rejection	MUST HAVE
FR-GW-005	Invalidation and recovery via the status list	MUST HAVE
FR-GW-006	Status polling	MUST HAVE
FR-GW-007	Status age rule	MUST HAVE
FR-GW-008	Issuance block on known invalidation	MUST HAVE
FR-GW-009	Recovery requires fresh status and admission	MUST HAVE
FR-GW-010	Reachability and no silent fallback	MUST HAVE
FR-GW-011	Status decision rule	MUST HAVE
FR-GW-012	Recovery after connectivity return	MUST HAVE
FR-GW-013	Mandatory XFSC tools	MUST HAVE
FR-GW-014	Separate holder per vehicle	MUST HAVE
FR-GW-015	No driver identity	MUST HAVE

[FR-GW-001] Credential profile via OCM W-Stack and PCM Cloud		MUST HAVE
Priority: MUST HAVE Group: Federation gateway		
Requirement	The federation gateway MUST admit a vehicle or the traffic light only with verifiable credentials (DID-based) issued through the XFSC OCM W-Stack in the credential profile currently supported by FACIS, as recorded in the Integration Note. Holders MUST be provided by PCM Cloud in the arrangement of FR-GW-014; no alternative credential ecosystem is used.	
Acceptance criteria	The Integration Note records credential format, flow, issuer and the OCM W-Stack and PCM Cloud versions used.	
	M1 shows that every credential used was issued exclusively through the OCM W-Stack into PCM Cloud, including any credential re-issued by the CD after a revocation	
	A presentation outside the recorded profile is rejected with VP_INVALID	

[FR-GW-002] Access-token identity binding		MUST HAVE
Priority: MUST HAVE Group: Federation gateway		
Requirement	The federation gateway MUST bind each access token to stationId, tenant and the OEM/vehicle credential identifiers taken from the OCM W-Stack verification result and controlled provisioning data. Identity fields requested by the client MUST NOT be used for the binding.	
Acceptance criteria	Positive admission produces the documented binding (stationId, tenant, credential identifiers) in the issued access token	
	M1: vehicle A cannot obtain or use authority for B; the attempt is rejected with IDENTITY_MISMATCH or ACCESS_TOKEN_INVALID	
	Requested identity fields in the admission request have no influence on the binding	
	An access token past its lifetime (default 10 min, Table 5) is rejected by every request receiver	

[FR-GW-003] Presentation verification via OCM W-Stack		MUST HAVE
Priority: MUST HAVE Group: Federation gateway		
Requirement	The federation gateway MUST verify credential presentations through the verification function of the OCM W-Stack; admission always requires the positive native result (FR-GW-004). A mock MAY only add a check that the OCM W-Stack demonstrably does not provide, only with written client approval, and MUST NOT replace or override a native result. Such a check MUST be recorded in the Integration Note and shown with its own MOCK label wherever its result is shown. Labels are given per capability (issuance, verification, status list) and per check only where the OCM W-Stack reports individual checks or a check is mocked.	
Acceptance criteria	M1 exercises positive and negative presentations (invalid signature or holder binding, revoked credential)	
	The system-identification screen shows NATIVE or MOCK per capability and a separate MOCK label for each mocked check (FR-OPS-006)	
	No mocked result is shown as native verification	

[FR-GW-004] Admission decision and typed rejection		MUST HAVE
Priority: MUST HAVE Group: Federation gateway		
Requirement	Admission MUST require a positive OCM W-Stack verification result and a valid status (Table 5b). A credential whose status is suspended or revoked MUST be rejected with VP_INVALID and sub-reason CREDENTIAL_REVOKED, derived from the status list. Any other invalid presentation MUST produce VP_INVALID; the sub-reasons CHAIN_INVALID and BINDING_INVALID are set only where the OCM W-Stack result distinguishes them (Integration Note), otherwise the OCM W-Stack reason is recorded in the event without secrets. An unavailable or unparseable service MUST produce SERVICE_UNAVAILABLE.	
Acceptance criteria	Admission is rejected while the status of the credential is blocked	
	M1: the revoked credential is rejected with VP_INVALID and sub-reason CREDENTIAL_REVOKED	
	A verification failure or timeout of the OCM W-Stack is reported as SERVICE_UNAVAILABLE and never as a proven invalid credential	
	Each rejection carries exactly one Table 4 code	

[FR-GW-005] Invalidation and recovery via the status list		MUST HAVE
Priority: MUST HAVE Group: Federation gateway		
Requirement	The federation gateway MUST perform credential invalidation (suspension or revocation) and recovery through the status list service of the OCM W-Stack and MUST preserve its semantics: a suspension is lifted; an irreversibly revoked credential is replaced through OCM W-Stack issuance, not reactivated.	
Acceptance criteria	M1 and M4 record operation and affected credential in STATUS_CHANGED events	
	Reset restores valid participation without reversing an irreversible revocation	
	A revoked credential is replaced through issuance, not reactivated	

[FR-GW-006] Status polling		MUST HAVE
Priority: MUST HAVE Group: Federation gateway		
Requirement	The federation gateway MUST read the status of every admitted credential from the OCM W-Stack status list at the configured poll interval (default 1 s, Table 5) and MUST verify the authenticity of the status list as provided by the OCM W-Stack. Every observation records the start time of its request.	
Acceptance criteria	A status list that fails authenticity or integrity checks is treated as blocked	
	Every status change appears as STATUS_CHANGED in the event log with the request start of its observation	

[FR-GW-007] Status age rule		MUST HAVE
Priority: MUST HAVE Group: Federation gateway		
Requirement	A status older than the configured maximum age (default 30 s, Table 5), measured from the request start of the last successful observation, MUST be treated as blocked; a status whose age equals the maximum age is blocked. A failed observation MUST NOT refresh the age. An observation whose request start is not later than that of the last recorded observation MUST be discarded. Without any successful observation the status is blocked.	
Acceptance criteria	Unit test: an age just below, equal to and above the maximum age yields valid, blocked and blocked	
	Unit test: a failed poll leaves the age unchanged	
	Unit test: an observation that completes after a newer one is discarded	
	Unit test: an empty status cache is blocked	

[FR-GW-008] Issuance block on known invalidation		MUST HAVE
Priority: MUST HAVE Group: Federation gateway		
Requirement	A known invalidation MUST block every further token issuance for the affected vehicle, including GO promotion, and MUST remove the vehicle from new discovery and session formation.	
Acceptance criteria	M4: no TOKEN_ISSUED for the affected vehicle after t_disable; RENEWAL_REFUSED carries the disable time	
	M4: the affected vehicle stops by local token expiry; unaffected participants complete	

[FR-GW-009] Recovery requires fresh status and admission		MUST HAVE
Priority: MUST HAVE Group: Federation gateway		
Requirement	Recovery after invalidation MUST require a valid status and renewed admission. An ended session MUST NOT resume, and a vehicle MUST NOT start automatically after recovery.	
Acceptance criteria	After recovery M1 shows standstill and a successful fresh admission	
	Tokens of the ended session remain rejected by the drive module (SESSION_CLOSED)	
	No TOKEN_ISSUED event occurs for the recovered vehicle without a new session	

[FR-GW-010] Reachability and no silent fallback		MUST HAVE
Priority: MUST HAVE Group: Federation gateway		
Requirement	Reachability of the OCM W-Stack verification and status functions MUST be shown per function. An unreachable function MUST produce SERVICE_UNAVAILABLE; the system MUST NOT switch to a mock automatically.	
Acceptance criteria	The dashboard shows reachability per function	
	Inspection: no automatic fallback from OCM W-Stack to a mock exists	

[FR-GW-011] Status decision rule		MUST HAVE
Priority: MUST HAVE Group: Federation gateway		
Requirement	The gateway and the STS MUST apply the decision rule of Table 5b at every admission and issuance decision: with a valid status admission, new sessions, initial ARMED issuance, GO promotion and renewal are allowed; with a blocked status all of them are blocked. The age rule of FR-GW-007 MUST be evaluated at the decision, independently of the polling timer.	
Acceptance criteria	Unit test: no issuance decision is allowed once the status is blocked	
	M4: GO promotion and renewal stop for the invalidated vehicle	

[FR-GW-012] Recovery after connectivity return		MUST HAVE
Priority: MUST HAVE Group: Federation gateway		
Requirement	After the OCM W-Stack becomes reachable again, a fresh valid status MUST restore eligible admission without restart of gateway, geofinder or STS. Recovery MUST NOT reopen ended sessions.	
Acceptance criteria	Integration test: after a blocked connection to the status list is released, admission succeeds again without restart	
	No automatic vehicle motion follows recovery; a new session requires standstill and discovery	

[FR-GW-013] Mandatory XFSC tools		MUST HAVE
Priority: MUST HAVE Group: Federation gateway		
Requirement	The federation gateway MUST consume the OCM W-Stack (issuance, verification, status list) and PCM Cloud in the versions recorded in the Integration Note. No native XFSC service is modified, re-hosted or reimplemented. Each OCM W-Stack function MUST be accessed through one adapter module; test doubles of the adapters are used only in CI and local development and are never part of the deployed container images or Helm charts. A runtime mock requires written client approval and is limited to the supplementing checks recorded under FR-GW-003; issuance, verification and status-list results on the admission (E1) and invalidation (E3) paths always come from the native OCM W-Stack.	
Acceptance criteria	The Integration Note lists tool, version and, where applicable, the recorded gap per capability	
	Inspection: no XFSC service is modified, re-hosted or reimplemented	
	Inspection: the container images and Helm charts of the tagged release contain no test double; every runtime mock has a recorded client approval	

[FR-GW-014] Separate holder per vehicle		MUST HAVE
Priority: MUST HAVE Group: Federation gateway		
Requirement	Each simulated vehicle MUST hold its credentials in a holder of its own; no holder, credential or key is shared between vehicles. The holders MAY be separate holders within one PCM Cloud tenant.; the arrangement is recorded in the Integration Note. A dedicated PCM Cloud instance per vehicle is option O-1 (Section 2.3).	
Acceptance criteria	Inspection: one holder per vehicle; credential identifiers differ per vehicle	
	M1: no cross-vehicle credential use is possible	
	With option O-1 (Section 2.3): the second M1 run and inspection show a dedicated PCM Cloud instance per vehicle	

[FR-GW-015] No driver identity		MUST HAVE
Priority: MUST HAVE Group: Federation gateway		
Requirement	The system MUST NOT depend on any driver or other personal credential. Admission, session and release MUST bind to vehicle/OEM and service identities only, and personal data MUST NOT be processed or stored in the event log.	
Acceptance criteria	Inspection: no schema, credential type or console field references a driver or natural person	
	Admission with vehicle/OEM credentials only succeeds (M1)	

5.2 Geofinder: queue discovery (FR-GEO)

ID	Name	Priority
FR-GEO-001	Position-report authentication	MUST HAVE
FR-GEO-002	Formation eligibility	MUST HAVE
FR-GEO-003	Along-track ordering	MUST HAVE
FR-GEO-004	Gap segmentation and stability	MUST HAVE
FR-GEO-005	Position message schema	MUST HAVE

[FR-GEO-001] Position-report authentication		MUST HAVE
Priority: MUST HAVE Group: Geofinder		
Requirement	The geofinder MUST accept only authenticated, schema-valid position reports that match the current run, stationId, tenant and access token. Reports older than the position-stale threshold (default 3 s, Table 5) MUST be rejected. Per stationId only a report whose measurement timestamp is later than that of the last accepted report MUST be accepted; a duplicate or out-of-order report MUST be discarded without effect.	
Acceptance criteria	Reports with a foreign identity, run or access token are rejected with POSITION_INVALID, ACCESS_TOKEN_INVALID or IDENTITY_MISMATCH	
	A report older than the stale threshold is rejected	
	Unit test: a redelivered report (same measurement timestamp) and an older report are discarded and do not count towards stability (Table 5g, D-08); for the motion proof see FR-STS-006	

[FR-GEO-002] Formation eligibility		MUST HAVE
Priority: MUST HAVE Group: Geofinder		
Requirement	A new formation MUST use only unreserved, in-lane vehicles whose last accepted position report is not older than the position-stale threshold (default 3 s, Table 5) and that meet the standstill criterion (discovery standstill threshold and duration; defaults 0.05 m/s for 3 s, Table 5).	
Acceptance criteria	A vehicle with an active reservation is not included in a new formation	
	A vehicle outside the lane threshold (default 0.30 m) is not included	
	A vehicle moving above the discovery standstill threshold, or standing for less than the required duration, is not included	
	A vehicle whose last accepted position report is older than the stale threshold is not included	
	The dummy is treated as a passive obstacle and never as a participant	
	Unit tests: Table 5g vectors D-05, D-06, D-07 and D-09 produce their expected outcome	

[FR-GEO-003] Along-track ordering		MUST HAVE
Priority: MUST HAVE Group: Geofinder		
Requirement	Participants MUST be ordered along the closed track by cutting the largest free arc; the participant directly before that arc in driving direction is the LEAD. Arcs are measured from front to front in driving direction and compared after rounding to the discovery distance resolution (default 1 mm, Table 5). A formation MUST NOT be reported when it has only one participant, when the two largest arcs differ by less than the cut tolerance (default 0.10 m, Table 5), or when its span from the last participant to the LEAD exceeds half the track perimeter.	
Acceptance criteria	M2 with the reference placement and the origin-shifted placement reproduces the reference order CD-V1, CD-V2, dummy, CD-V3	
	Unit tests: Table 6g vectors D-01, D-02, D-07, D-11 and D-12 produce their expected outcome	

[FR-GEO-004] Gap segmentation and stability		MUST HAVE
Priority: MUST HAVE Group: Geofinder		
Requirement	Two consecutive participants whose arc exceeds the configured gap threshold (default 2.20 m, Table 5) are separated by a gap; an arc equal to the threshold is not a gap. A formation MUST be reported only after participant identities, order and segment boundaries have remained unchanged for the configured number of consecutive geofinder cycles (default 3 cycles of 1 s, Table 5).	
Acceptance criteria	The reference placement yields one gap segment: CD-V3 becomes FOLLOW_GAP behind the dummy (M2)	
	Unit test: no formation is reported before the required stable-cycle count (Table 5g, D-01 and D-10)	
	Unit tests: Table 5g vectors D-03, D-04 and D-10 produce their expected outcome	

[FR-GEO-005] Position message schema		MUST HAVE
Priority: MUST HAVE Group: Geofinder		
Requirement	A position report MUST contain stationId, tenant, run_id, x, y, speed, measurement timestamp and schemaVersion; units and value ranges MUST be fixed in the versioned schema. Speed MUST come from the motion source, not from differences of noisy reports.	
Acceptance criteria	Reports with missing fields or non-finite values are rejected	
	Inspection: speed is taken from the position-source interface, not derived from report differences	

5.3 STS: reservation, session and token lifecycle (FR-STs)

ID	Name	Priority
FR-STs-001	Atomic participant reservation	MUST HAVE
FR-STs-002	No session migration or resumption	MUST HAVE
FR-STs-004	Session protocol	MUST HAVE
FR-STs-005	Role and order binding	MUST HAVE
FR-STs-006	GO release by predecessor motion proof (release mode motion-proof)	MUST HAVE
FR-STs-007	Lead progress, target STOP and DONE	MUST HAVE
FR-STs-008	Lead loss abort	MUST HAVE
FR-STs-009	Release-token signing and sequence	MUST HAVE
FR-STs-010	Issuance checks	MUST HAVE
FR-STs-012	Renewal semantics	MUST HAVE
FR-STs-013	Withdrawal by non-issuance; STOP as accelerator	MUST HAVE
FR-STs-014	Release-token schema	MUST HAVE
FR-STs-015	Composition in the session proposal	MUST HAVE

[FR-ST5-001] Atomic participant reservation		MUST HAVE
Priority: MUST HAVE Group: STS		
Requirement	The single STS MUST atomically reserve every participant of a formation before opening its session. A formation that contains an already reserved vehicle MUST be rejected with SESSION_CONFLICT.	
Acceptance criteria	Conflicting proposals create exactly one active assignment per vehicle (unit test)	
	The accepted session proceeds to PROPOSED; a conflicting one is rejected with SESSION_CONFLICT	

[FR-ST5-002] No session migration or resumption		MUST HAVE
Priority: MUST HAVE Group: STS		
Requirement	An aborted or failed session MUST NOT migrate or resume. Reservations MUST persist until the last issued token has expired plus B_stop; re-participation MUST require fresh standstill and a cleared local fault state. After a start or restart the STS MUST NOT open a session or sign a token until TTL + B_stop have elapsed since its start (start-up hold).	
Acceptance criteria	M5: no participant is reassigned before its last token has expired	
	A vehicle is admitted to discovery again only after standstill and cleared fault state	
	Unit test: no session is opened and no token is signed during the start-up hold	

[FR-ST5-004] Session protocol		MUST HAVE
Priority: MUST HAVE Group: STS		
Requirement	The STS MUST implement the session protocol of Table 5c (PROPOSED, CONFIRMED, TOKENS_ISSUED, ARMED, ROLLING, DONE, ABORTED) with the state timeouts of Table 5 and abort on rejection or timeout with a typed reason naming the state.	
Acceptance criteria	M3 runs through every state up to DONE	
	STATE_TIMEOUT names the state in which the timeout occurred	
	Terminal sessions (DONE, ABORTED) issue no further tokens	

[FR-ST5-005] Role and order binding		MUST HAVE
Priority: MUST HAVE Group: STS		
Requirement	Roles and order MUST be computed before initial token issuance and become binding at ARMED: first participant LEAD/NONE; first participant behind a gap FOLLOW_GAP/GAP; all others FOLLOW with their direct predecessor. The STS MUST separately retain the preceding authorised participant as wave_predecessor.	
Acceptance criteria	M2/M3 show the reference roles: V1 LEAD/NONE, V2 FOLLOW/V1, V3 FOLLOW_GAP/GAP with wave_predecessor V2	
	No role, predecessor or rank changes during a session; a changed claim at the same token_seq is rejected by the drive module (T-05)	

[FR-ST5-006] GO release by predecessor motion proof (release mode motion-proof)		MUST HAVE
Priority: MUST HAVE Group: STS		
Requirement	The LEAD MAY receive GO without predecessor motion. In release mode motion-proof (default) every other participant MUST receive GO only after its wave_predecessor has supplied the configured number of consecutive fresh motion reports (default 2 reports above v_move 0.10 m/s, Table 5) timestamped after that predecessor's GO issuance. Only reports with distinct, strictly increasing measurement timestamps count; a duplicate report does not count. A dummy cannot trigger GO. The release mode coordinated is specified in FR-TL-003.	
Acceptance criteria	M3(a): FOLLOW_GAP starts only after the participant before the gap has moved	
	T-10: predecessor loss before the required motion proof never releases the dependent follower	
	Unit test: a redelivered motion report does not count twice	
	PHASE_CHANGED records the motion report IDs that triggered the promotion	

[FR-ST5-007] Lead progress, target STOP and DONE		MUST HAVE
Priority: MUST HAVE Group: STS		
Requirement	Lead progress MUST be accumulated as unwrapped along-track travel from the initial position. At the scenario target the STS MUST halt issuance and send a run/session-bound STOP; DONE MUST require all participants standing.	
Acceptance criteria	M3 reaches the target and ends in DONE	
	After the target no further TOKEN_ISSUED occurs for the session	
	DONE is entered only after STANDSTILL of every participant	

[FR-ST5-008] Lead loss abort		MUST HAVE
Priority: MUST HAVE Group: STS		
Requirement	Loss of the LEAD before the target (blocked status or stale position) MUST abort the session with LEAD_UNAVAILABLE and halt all issuance for that session.	
Acceptance criteria	A simulated lead loss produces SESSION_ENDED(ABORTED, LEAD_UNAVAILABLE)	
	No token is issued for the session after the abort; followers stop by expiry or STOP	

[FR-ST5-009] Release-token signing and sequence		MUST HAVE
Priority: MUST HAVE Group: STS		
Requirement	The STS MUST sign release tokens with ES256 using the release-token schema of FR-ST5-014, current run/session binding and a strictly increasing token_seq per vehicle-session. nbf MUST equal the issuance time rounded down to whole seconds and exp MUST equal nbf plus TTL (Table 5).	
Acceptance criteria	Unit test: schema and sequence of the issued tokens	
	Release-token keys and type cannot be confused with access-token keys and type	
	TOKEN_ISSUED carries operation type, sequence, phase, nbf/exp and fingerprint	

[FR-STS-010] Issuance checks		MUST HAVE
Priority: MUST HAVE Group: STS		
Requirement	Initial ARMED issuance, GO promotion and renewal MUST be distinct operations. Every operation MUST check session state, halt flag, identity, access token, fresh position (age at most position_stale, Table 5) and status before signing. Session state, halt flag, position freshness and status MUST be evaluated again immediately before the signed token is released; a token whose second evaluation fails MUST be discarded and not sent. TOKEN_ISSUED is emitted only for a released token; a discarded token is logged as RENEWAL_REFUSED with its reason.	
Acceptance criteria	M4/M5: no issuance after invalidation, halt or uplink loss beyond position_stale	
	A failing check results in no signature (unit test)	
	Unit test: a status change, halt, target, session abort or stale position that occurs while a token is being signed prevents its release and produces no TOKEN_ISSUED	
	Each operation type is identifiable in TOKEN_ISSUED	

[FR-STS-012] Renewal semantics		MUST HAVE
Priority: MUST HAVE Group: STS		
Requirement	Renewal MUST preserve role and phase; GO promotion MUST be logged separately. A refused request MUST extend nothing, and a request MUST NOT reopen a closed session.	
Acceptance criteria	Renewals never change role or phase; each promotion appears as PHASE_CHANGED	
	A request for a DONE/ABORTED session is refused	

[FR-STS-013] Withdrawal by non-issuance; STOP as accelerator		MUST HAVE
Priority: MUST HAVE Group: STS		
Requirement	Federation- or status-conditioned withdrawal MUST work solely through non-issuance and local token expiry without requiring any message to reach the vehicle. Regular completion and emergency stop MAY use authenticated STOP/TOKEN_CLEAR as accelerators; expiry MUST remain the independent fallback.	
Acceptance criteria	M4 demonstrates expiry stopping with the business downlink of the affected vehicle blocked	
	Inspection: no code path requires receipt of a message to bring a vehicle to standstill	

[FR-STS-014] Release-token schema		MUST HAVE
Priority: MUST HAVE Group: STS		
Requirement	A release token MUST use ES256, typ=cd-release+jwt, an issuer-bound kid and exactly the claims session_id, sts_instance, station_id, kolonnen_index, rolle (LEAD/FOLLOW/FOLLOW_GAP), vorgaenger (stationId/GAP/NONE), phase (ARMED/GO), nbfc, exp, policy_version, run_id and token_seq. kolonnen_index starts at 0 for the LEAD. No motion-control values are allowed.	
Acceptance criteria	Unit test: exact fields and types; tokens with additional or unknown claims fail validation	
	Access tokens use a distinct type and trust purpose	

[FR-STS-015] Composition in the session proposal		MUST HAVE
Priority: MUST HAVE Group: STS		
Requirement	The session proposal sent in state PROPOSED MUST contain the identities (stationId, tenant) of all participants, the recipient's rank (kolonnen_index), its predecessor and its wave_predecessor, and the release mode of the session.	
Acceptance criteria	The proposal schema contains participant list, rank, predecessor, wave_predecessor and release mode	
	The agent logs the received composition	

5.4 Vehicle software: agent, drive logic and protective stop (FR-VEH)

ID	Name	Priority
FR-VEH-001	Agent credential custody and gateway use	MUST HAVE
FR-VEH-002	Position reporting, renewal and STOP translation	MUST HAVE
FR-VEH-004	Agent failure	MUST HAVE
FR-VEH-006	Token validation	MUST HAVE
FR-VEH-007	Drive state machine	MUST HAVE
FR-VEH-008	Monotonic token deadline	MUST HAVE
FR-VEH-009	Expiry handling and stopping latch	MUST HAVE
FR-VEH-010	Session lock and TOKEN_CLEAR semantics	MUST HAVE
FR-VEH-011	Protective stop on obstacle distance	MUST HAVE
FR-VEH-012	Sensor validity handling	MUST HAVE
FR-VEH-013	Fault latch	MUST HAVE
FR-VEH-014	Agent-to-drive messages	MUST HAVE
FR-VEH-015	HAL and position-source interfaces	MUST HAVE
FR-VEH-016	Termination of convoy authorisation on expiry	MUST HAVE
FR-VEH-017	Degradation behaviour: standstill	MUST HAVE

[FR-VEH-001] Agent credential custody and gateway use		MUST HAVE
Priority: MUST HAVE Group: Vehicle software		
Requirement	The vehicle agent MUST use its PCM Cloud holder for its credentials, MUST hold its own vehicle key and MUST use the federation gateway for all external credential operations.	
Acceptance criteria	M1 shows the provisioning route per vehicle	
	Inspection: all federation traffic of the vehicle passes the gateway	
	The vehicle private key never leaves the vehicle service	

[FR-VEH-002] Position reporting, renewal and STOP translation		MUST HAVE
Priority: MUST HAVE Group: Vehicle software		
Requirement	The vehicle agent MUST publish position reports at the configured interval (default 1 s), request renewal at the configured fraction of token lifetime (default 0.5) and translate only a STOP of the current run and session into TOKEN_CLEAR. A missing reply MUST NOT trigger TOKEN_CLEAR.	
Acceptance criteria	An old or foreign-session STOP is ignored; only a current run/session STOP produces TOKEN_CLEAR	
	After a missing renewal reply the vehicle stops by expiry	

[FR-VEH-004] Agent failure		MUST HAVE
Priority: MUST HAVE Group: Vehicle software		
Requirement	A failure or restart of the agent logic MUST prevent new releases; the drive logic MUST complete its local expiry stop unaffected. After a start or restart the drive logic MUST command stop() and MUST reject every token until it receives a run_id distributed by lab control over the run-control interface (Table 3) at the initial start or in a reset (Table 5e, step 4); lab control does not re-send the current run_id to a drive logic that restarts during a run. Such tokens are rejected with RUN_MISMATCH unless an earlier check of Table 2a fails.	
Acceptance criteria	Integration test: after the agent logic of a rolling vehicle is halted with the agent-stop switch (FR-SIM-004), the vehicle stops by expiry; no old token restarts motion	
	Unit test: after a start the drive logic commands stop() and rejects tokens until a run_id is distributed	
	Unit test: after a restart within a run, a still-valid token of the current run is rejected with RUN_MISMATCH until the next reset	

[FR-VEH-006] Token validation		MUST HAVE
Priority: MUST HAVE Group: Vehicle software		
Requirement	The drive logic MUST check every TOKEN_SET in the order of Table 2a and MUST answer a rejected token with exactly one SM_NACK whose reason is that of the first failing check. The checks cover schema, type and policy_version, ES256 signature and issuer/key assignment, station and run binding, session lock, fault latch, validity window (nbf/exp with nbf_tolerance, Table 5), sequence, phase/state and, for the ARMED-to-ROLLING transition, sensing. An invalid token MUST NOT replace a valid current token. Every requirement and acceptance criterion of this specification that names an SM_NACK reason applies when no earlier check of Table 2a fails.	
Acceptance criteria	T-05: each check of Table 2a failing alone yields its reason; each combined-failure vector of T-05 yields the reason of the earlier check	
	An access token presented as a release token is rejected with TOKEN_SCHEMA_INVALID	
	Unit test: exactly one SM_NACK is sent per rejected TOKEN_SET	
	The current valid token remains in force after any rejection	

[FR-VEH-007] Drive state machine		MUST HAVE
Priority: MUST HAVE Group: Vehicle software		
Requirement	The drive logic MUST implement the state machine of Table 2: from IDLE only ARMED of a new admissible session is accepted; GO requires the same session, a higher token_seq and a valid distance of at least d_min; IDLE, ARMED and FAULT mean standstill.	
Acceptance criteria	Unit tests cover every transition of Table 2	
	A direct GO from IDLE is rejected with SESSION_STATE_INVALID	
	A distance below d_min or an invalid sample prevents the ARMED-to-ROLLING transition	

[FR-VEH-008] Monotonic token deadline		MUST HAVE
Priority: MUST HAVE Group: Vehicle software		
Requirement	An accepted token MUST establish a local deadline = $t_{receipt} + \min(exp - now, exp - nbf)$, evaluated once at acceptance with the synchronised clock and then tracked on the monotonic clock only, so that the remaining validity never exceeds TTL after receipt. An identical redelivery or a wall-clock adjustment MUST NOT extend an existing deadline.	
Acceptance criteria	Unit test: the deadline runs on the monotonic clock; a wall-clock step forward or backward after acceptance does not change it	
	Unit test: an identical redelivery extends nothing	
	TOKEN_ACCEPTED records fingerprint, deadline and current state	

[FR-VEH-009] Expiry handling and stopping latch		MUST HAVE
Priority: MUST HAVE Group: Vehicle software		
Requirement	On deadline expiry the drive logic MUST start braking to standstill within δ_{local} (default 0.10 s, Table 5) (degradation behaviour standstill, FR-VEH-017). An internal stopping latch MUST reject any resumption of convoy motion for the locked session until standstill and then report FAULT(TOKEN_EXPIRED), or IDLE after TOKEN_CLEAR.	
Acceptance criteria	M4/M5: after expiry the vehicle brakes and reaches standstill; BRAKE_STARTED records cause and time	
	Any TOKEN_SET for the locked session while stopping is rejected with SESSION_CLOSED	
	FAULT(TOKEN_EXPIRED) is reported at standstill; IDLE only after TOKEN_CLEAR	

[FR-VEH-010] Session lock and TOKEN_CLEAR semantics		MUST HAVE
Priority: MUST HAVE Group: Vehicle software		
Requirement	Braking, TOKEN_CLEAR or a terminal fault MUST lock the session for the rest of the run; a TOKEN_SET of a locked session is rejected with SESSION_CLOSED unless an earlier check of Table 3a fails. TOKEN_CLEAR MAY clear a fault and change the stopping destination to IDLE but MUST NOT remove the session lock or start motion.	
Acceptance criteria	T-04: a still-valid old ARMED/GO token replayed after clear is rejected; the vehicle stays non-moving	
	TOKEN_CLEAR never produces motion and never unlocks the session	

[FR-VEH-011] Protective stop on obstacle distance		MUST HAVE
Priority: MUST HAVE Group: Vehicle software		
Requirement	During ROLLING a free distance below d_{min} MUST trigger braking within δ_{local} and FAULT(SAFETY_STOP) at standstill. Distance MUST provide only a start-safety gate and a stopping condition, not following-speed control; no following controller is active and none is driven by release tokens.	
Acceptance criteria	M3: the FOLLOW_GAP vehicle stops before the dummy without overlap	
	Inspection: no speed or distance controller acts on the target speed during ROLLING	

[FR-VEH-012] Sensor validity handling		MUST HAVE
Priority: MUST HAVE Group: Vehicle software		
Requirement	A missing, invalid or over-age distance sample (sensor_max_age, default 0.20 s) MUST inhibit start and MUST trigger a protective stop while rolling, reported as SENSOR_FAULT.	
Acceptance criteria	M5: an invalid sample injected while rolling stops the vehicle with FAULT(SENSOR_FAULT)	
	Start with an invalid sample is rejected with SM_NACK(SENSOR_FAULT)	

[FR-VEH-013] Fault latch		MUST HAVE
Priority: MUST HAVE Group: Vehicle software		
Requirement	FAULT MUST remain latched until TOKEN_CLEAR. While latched, a TOKEN_SET of a new session MUST be answered with SM_NACK(FAULT_LATCHED) and a TOKEN_SET of the locked session with SM_NACK(SESSION_CLOSED), unless an earlier check of Table 3a fails.	
Acceptance criteria	Unit test: a GO token of a new session after a fault is rejected with FAULT_LATCHED	
	TOKEN_CLEAR leaves the vehicle standing in IDLE with the old session closed	

[FR-VEH-014] Agent-to-drive messages		MUST HAVE
Priority: MUST HAVE Group: Vehicle software		
Requirement	Agent and drive logic of one vehicle MUST exchange only the messages of Table 1 (TOKEN_SET, TOKEN_CLEAR, SM_ACK, SM_NACK(reason), SM_STATE). Both MAY run in one ORCE instance per vehicle.	
Acceptance criteria	Inspection: only the Table 1 message families are exchanged	
	Unit tests exercise the drive logic only through the Table 1 messages and the run-control input (Table 3)	
	SM_STATE values are IDLE/ARMED/ROLLING/FAULT and conform to actual standstill	

[FR-VEH-015] HAL and position-source interfaces		MUST HAVE
Priority: MUST HAVE Group: Vehicle software		
Requirement	The hardware abstraction layer MUST provide setTargetSpeed(v), stop(), getDistance() -> (metres, valid, timestamp) and getMotionState() -> (speed, valid, timestamp) towards the world service; a position-source interface MUST supply (x, y, speed, timestamp) to the agent. Both MUST use a transport independent of the business broker and be documented.	
Acceptance criteria	Inspection: all motion and sensor access uses these interfaces	
	Stopping the business broker does not interrupt HAL or position-source traffic (T-12)	

[FR-VEH-016] Termination of convoy authorisation on expiry		MUST HAVE
Priority: MUST HAVE Group: Vehicle software		
Requirement	The end of a vehicle's convoy authorisation MUST rest on two independent mechanisms: (1) from the disable instant <code>t_disable</code> (known invalidation, halt flag, session abort or missing fresh position/status) the STS signs no further token for the vehicle (FR-GW-008, FR-STS-010); (2) from the local expiry instant <code>t_exp</code> of the last accepted token the drive logic locks the session, accepts no further GO or renewal for it and emits <code>DEGRADATION_STARTED</code> . Neither mechanism requires a message to reach the vehicle.	
Acceptance criteria	M4: <code>t_disable</code> and <code>t_exp</code> of the affected vehicle are visible in the event log and on the operations screen	
	Unit test: after <code>t_exp</code> every <code>TOKEN_SET</code> for the locked session is answered <code>SESSION_CLOSED</code> (Table 2a, step 5)	
	Convoy authorisation is never restored without fresh admission, discovery and a new session	

[FR-VEH-017] Degradation behaviour: standstill		MUST HAVE
Priority: MUST HAVE Group: Vehicle software		
Requirement	After the end of convoy authorisation (FR-VEH-016) the vehicle MUST brake to standstill (FR-VEH-009). <code>DEGRADATION_STARTED</code> MUST carry the mode standstill.	
Acceptance criteria	M4/M5: every degradation ends in standstill; <code>DEGRADATION_STARTED(mode=standstill)</code> is emitted	

5.5 World service and fault injection (FR-SIM)

ID	Name	Priority
FR-SIM-001	Track and kinematic model	MUST HAVE
FR-SIM-002	World service	MUST HAVE
FR-SIM-003	Independence during convoy-layer faults	MUST HAVE
FR-SIM-004	Fault injection for the demonstration	MUST HAVE

[FR-SIM-001] Track and kinematic model		MUST HAVE
Priority: MUST HAVE Group: World service		
Requirement	The simulator MUST use a closed 2D polyline with one-dimensional along-track motion and occupied vehicle/dummy length intervals. Positions are front points and distance is the front-to-next-rear free path; configured acceleration and braking MUST be integrated to zero without negative speed.	
Acceptance criteria	Unit tests validate distance, acceleration and stopping distance against the model	
	Speed never becomes negative; braking integrates to zero	
	The reference track (12 m perimeter) is delivered	

[FR-SIM-002] World service		MUST HAVE
Priority: MUST HAVE Group: World service		
Requirement	A world service separate from the convoy layer MUST supply timestamped position/speed and distance/motion feedback over a transport independent of the business broker. Position reports MUST carry normally distributed noise (sigma_pos, Table 5); the geofinder MUST receive only agent-published reports, never world ground truth.	
Acceptance criteria	Inspection verifies the separation of world service, vehicles and convoy layer	
	The geofinder receives only agent-published reports	

[FR-SIM-003] Independence during convoy-layer faults		MUST HAVE
Priority: MUST HAVE Group: World service		
Requirement	The world service and the vehicles MUST keep running when the convoy layer is stopped.	
Acceptance criteria	T-12 stops only the convoy layer; world and vehicles continue and the vehicles stop by expiry	

[FR-SIM-004] Fault injection for the demonstration		MUST HAVE
Priority: MUST HAVE Group: World service		
Requirement	Lab control MUST be able to inject the faults of Table 5d (uplink off per vehicle, STS stop, convoy-layer stop, sensor invalid, business downlink block for M4), record each injection as FAULT_INJECTED and keep the listed unaffected components running. For integration tests lab control MUST also provide an agent-stop switch per vehicle (FR-VEH-004) and a block of the connection to the status list (FR-GW-012).	
Acceptance criteria	Each Table 6d fault is injectable from the console	
	FAULT_INJECTED records fault type, onset and affected component	

5.6 Dashboard, console, emergency stop and reset (FR-OPS)

ID	Name	Priority
FR-OPS-001	Dashboard content and freshness	MUST HAVE
FR-OPS-002	Authenticated console	MUST HAVE
FR-OPS-003	Emergency stop (laboratory abort)	MUST HAVE
FR-OPS-004	Reset procedure	MUST HAVE
FR-OPS-006	System-identification screen	MUST HAVE
FR-OPS-007	Operations screen	MUST HAVE
FR-OPS-010	Release-mode comparison view	OPTION

[FR-OPS-001] Dashboard content and freshness		MUST HAVE
Priority: MUST HAVE Group: Dashboard, console, emergency stop, reset		
Requirement	The dashboard MUST be built with the FACIS UI Builder package and consist of the operations screen (FR-OPS-007) and the system-identification screen (FR-OPS-006). It MUST show track and vehicles, tenant, order/gaps/segments, session, roles, phases, remaining TTL, drive state, status and reachability per credential, the active profile and NATIVE/MOCK labels. A stale display MUST be distinguishable from fresh data. Its appearance follows the FAP UI implementation guideline as implemented by the UI Builder package.	
Acceptance criteria	M2–M5 show every listed field and label	
	Remaining TTL, drive state, release mode and degradation state per vehicle are visible during the wave	
	A paused event stream is shown as stale	

[FR-OPS-002] Authenticated console		MUST HAVE
Priority: MUST HAVE Group: Dashboard, console, emergency stop, reset		
Requirement	A separately authenticated console MUST support start, reset, invalidation/recovery and the Table 5d faults. Destructive actions MUST require confirmation, and console access MUST be limited to the client operators.	
Acceptance criteria	Unauthenticated console or lab-control calls fail	
	Confirmation is required for invalidation, STS stop and emergency stop	

[FR-OPS-003] Emergency stop (laboratory abort)		MUST HAVE
Priority: MUST HAVE Group: Dashboard, console, emergency stop, reset		
Requirement	The emergency stop is the laboratory abort of the convoy layer, not a physical emergency-stop function of a vehicle platform. Its effect path MUST be: (1) the STS blocks new sessions and halts every token issuance within halt_budget (default 1 s, Table 5); (2) the STS sends run/session-bound STOP to reachable vehicles as an accelerator; (3) every vehicle stops at the latest by local token expiry, whether or not STOP was received. Confirmation state and standstill count MUST be displayed.	
Acceptance criteria	M5: emergency stop with reachable and with blocked business downlink; all vehicles reach standstill	
	An unconfirmed halt never appears as successful; the standstill count matches the world-observed standstills	

[FR-OPS-004] Reset procedure		MUST HAVE
Priority: MUST HAVE Group: Dashboard, console, emergency stop, reset		
Requirement	Reset MUST follow the steps of Table 6e, restore this run's credential changes through the OCM W-Stack status list and issue a new run_id only after standstill. Any failure MUST produce RESET_INCOMPLETE and never a demo-ready state.	
Acceptance criteria	M5 ends with a reset that reports demo-ready only after health, valid status, free reservations, standstill and the end of the STS start-up hold	
	RESET_COMPLETED is emitted with the new run_id	

[FR-OPS-006] System-identification screen		MUST HAVE
Priority: MUST HAVE Group: Dashboard, console, emergency stop, reset		
Requirement	The dashboard MUST provide a system-identification screen listing every participant (vehicles, traffic light) and every convoy-layer service with its identifier (DID or service identifier), credential status, trust status and NATIVE/MOCK label per capability.	
Acceptance criteria	Each participant and service appears with identifier, credential status and trust status	
	Status changes (STATUS_CHANGED) are reflected on the screen	

[FR-OPS-007] Operations screen		MUST HAVE
Priority: MUST HAVE Group: Dashboard, console, emergency stop, reset		
Requirement	The dashboard MUST provide an operations screen showing the track with all vehicles and the dummy, the sessions of the current run (state, run_id, release mode, result with reason), the connected traffic light with its current phase and, per vehicle, rank, role, predecessor, wave_predecessor, phase (ARMED/GO), remaining TTL, drive state, GO issuance time and, in coordinated mode, the configured GO offset relative to T0.	
Acceptance criteria	All listed fields are visible during M3 (both release modes)	
	A completed run shows DONE/ABORTED per session with reason	

[FR-OPS-010] Release-mode comparison view		OPTION
Priority: OPTION (O-2) Group: Dashboard, console, emergency stop, reset		
Requirement	With option O-2 the operations screen MUST show, for the last run of each release mode, the GO issuance times and start lag per rank side by side (NFR-KPI-001).	
Acceptance criteria	After M3(a) and M3(b) both runs are shown side by side	

5.7 Business interface, events and codes (FR-IF)

ID	Name	Priority
FR-IF-001	Business interface contract	MUST HAVE
FR-IF-002	Codes and events	MUST HAVE

[FR-IF-001] Business interface contract		MUST HAVE
Priority: MUST HAVE Group: Business interface		
Requirement	The contractor MUST deliver versioned schemas, MQTT topics and request correlation for admission, positions, proposals, confirmations, token operations, status, health, console and traffic-light phase messages. Control messages MUST NOT be retained on the business broker.	
Acceptance criteria	Interface description and example messages for every operation	
	Retain is disabled for control topics on the broker	
	Every request carries a correlation identifier and every error a Table 4 code	

[FR-IF-002] Codes and events		MUST HAVE
Priority: MUST HAVE Group: Business interface		
Requirement	The codes of Table 4 and the events of Table 4a MUST cover every emitted error and event. An unknown value MUST NOT be treated as success.	
Acceptance criteria	Inspection of the code and event list against the implementation	
	Unit test: every drive rejection reason of Table 2a is asserted	
	An unknown phase or adapter output fails closed (unit test)	

5.8 Configuration profile and fixtures (FR-CFG)

ID	Name	Priority
FR-CFG-001	Configuration profile	MUST HAVE
FR-CFG-002	Profile consistency checks	MUST HAVE
FR-CFG-003	Shipped fixtures	MUST HAVE

[FR-CFG-001] Configuration profile		MUST HAVE
Priority: MUST HAVE Group: Configuration profile and fixtures		
Requirement	The contractor MUST deliver one versioned configuration profile (JSON with schema) covering the Table 5 parameters, deployment bindings, polyline, direction, placements and scenario targets. Runtime-generated IDs and secrets MUST remain outside the profile.	
Acceptance criteria	Invalid or incomplete profiles are rejected at start with CONFIG_INVALID	
	run_id and secrets are not part of the profile file	

[FR-CFG-002] Profile consistency checks		MUST HAVE
Priority: MUST HAVE Group: Configuration profile and fixtures		
Requirement	Every component MUST load the profile through one shared loader that validates it against the schema and against the following checks before start: (1) the stopping-distance relation of assumption A-2 holds with the loaded values of d_min, v_max, sensor_max_age, delta_local, a_brake and the distance margin; (2) the renewal fraction lies strictly between 0 and 1; (3) the maximum status age exceeds the status poll interval; (4) the ARMED timeout exceeds (number of participants of Table 5 – 1) × coordinated GO offset, whatever release mode the profile selects. A failed check MUST reject the profile with CONFIG_INVALID. The loader MUST log the derived B_stop and the stopping-distance headroom.	
Acceptance criteria	Unit tests: a profile that violates any one of the checks is rejected with CONFIG_INVALID	
	The Table 5 defaults pass all checks; the loader logs B_stop = 0.40 s and a stopping-distance headroom of about 0.85 m	

[FR-CFG-003] Shipped fixtures		MUST HAVE
Priority: MUST HAVE Group: Configuration profile and fixtures		
Requirement	The reference placement (Table 5f), its origin-shifted variant (Table 5g, D-02) and one obstacle-free fixture for M4 and M5 MUST be shipped with the source, each with its expected outcome. The discovery reference vectors of Table 5g MUST be shipped as unit-test data. The obstacle-free fixture MUST allow the M4/M5 observation windows to complete before any participant approaches another one on the closed track.	
Acceptance criteria	M2–M5 run with the shipped fixtures	
	Each fixture states its expected outcome	
	All Table 5g vectors pass in CI	

5.9 Traffic light, T0 and coordinated release (FR-TL)

ID	Name	Priority
FR-TL-001	Federation-identified traffic light	MUST HAVE
FR-TL-002	T0-bound session start	MUST HAVE
FR-TL-003	Coordinated release mode	MUST HAVE

[FR-TL-001] Federation-identified traffic light		MUST HAVE
Priority: MUST HAVE Group: Traffic light, T0, coordinated release		
Requirement	The system MUST include a simulated traffic-light service that is admitted through the federation gateway with its own infrastructure credential issued by the OCM W-Stack and that publishes authenticated signal-phase messages on the business broker. Each phase message MUST carry light_id, intersection_id, a strictly increasing phase_event_id, phase (red/green), the green-onset time T0, validity_until, the stop-line position, a timestamp and schemaVersion.	
Acceptance criteria	The traffic light is admitted with a distinct infrastructure credential (M1) and shown on the system-identification screen	
	Unauthenticated phase messages are rejected	

[FR-TL-002] T0-bound session start		MUST HAVE
Priority: MUST HAVE Group: Traffic light, T0, coordinated release		
Requirement	When the trigger source is traffic-light, the STS MUST issue the LEAD GO of an ARMED session not before the green-onset time T0 of a valid, not yet consumed phase message of the light bound to the session. A phase change to red before the LEAD GO MUST cancel the pending start; a session that is not ARMED at T0 MUST NOT start on that event. With trigger source console the console start applies (FR-OPS-002).	
Acceptance criteria	M3(b): LEAD GO is issued not before T0; T0 and phase_event_id are recorded in TOKEN_ISSUED	
	Unit test: a consumed or not increasing phase_event_id, a phase message of a light not bound to the session, a message past validity_until and a red phase before LEAD GO do not start the session	

[FR-TL-003] Coordinated release mode		MUST HAVE
Priority: MUST HAVE Group: Traffic light, T0, coordinated release		
Requirement	In release mode coordinated the STS MUST issue the follower GO of rank r (kolonnen_index $r \geq 1$) not before $T0 + r \times \text{offset}$ (offset from the profile, Table 5), and only while status and position of that participant are valid (FR-GW-011, FR-STS-010). If the GO of a follower cannot be signed within the ARMED timeout (Table 5) counted from T0, the session is aborted with STATE_TIMEOUT naming ROLLING, the session state at that time (Table 5c). A follower's approach is bounded solely by the $d_{\min}$ gate and protective stop (FR-VEH-007, FR-VEH-011); token schema and deadline handling are the same as in release mode motion-proof.	
Acceptance criteria	M3(b): GO issuance instants per rank follow $T0 + r \times \text{offset}$	
	M3(b): FOLLOW_GAP stops before the dummy by the protective stop	

6. Non-functional requirements

Overview of the 7 groups (23 requirements):

Group	Identifiers (numbers)	MUST	OPTION
Security and trust (NFR-SEC)	001, 002, 003, 004, 005	5	0
Deployment (NFR-DEP)	001, 002, 003	3	0
Timing (NFR-TIM)	001, 002, 004, 005, 006	5	0
Event log and demonstration evidence (NFR-EVD)	001, 004	2	0
Configuration and repository (NFR-CFG)	001, 003, 004	3	0
Delivery and documentation (NFR-DEL)	001, 002, 003, 005	4	0
Start-delay indicators (NFR-KPI)	001	0	1
Total		22	1

6.1 Security and trust (NFR-SEC)

ID	Name	Priority
NFR-SEC-001	Transport security	MUST HAVE
NFR-SEC-002	Key custody	MUST HAVE
NFR-SEC-003	Identity separation	MUST HAVE
NFR-SEC-004	Broker ACLs and request authorisation	MUST HAVE
NFR-SEC-005	Secret-free logs and data minimisation	MUST HAVE

[NFR-SEC-001] Transport security		MUST HAVE
Priority: MUST HAVE Group: Security and trust		
Requirement	All network endpoints (MQTT and HTTP) MUST use TLS with certificate verification; plaintext connections MUST be refused.	
Acceptance criteria	Inspection of broker and ingress configuration; a plaintext connection attempt fails	

[NFR-SEC-002] Key custody		MUST HAVE
Priority: MUST HAVE Group: Security and trust		
Requirement	Private keys MUST remain with their owning service or vehicle; no key material is shared between vehicles or copied into the convoy layer. Issuer keys remain with the OCM W-Stack; the CD never holds an issuer key. The release-token signing key MUST be distinct in type and purpose from access-token keys.	
Acceptance criteria	Inspection confirms key ownership per component	

[NFR-SEC-003] Identity separation		MUST HAVE
Priority: MUST HAVE Group: Security and trust		
Requirement	Administrative, vehicle and service identities MUST be separate; no identity is used in more than one role. A vehicle identity calling console or lab-control endpoints MUST be rejected.	
Acceptance criteria	M1: a vehicle identity cannot call console or lab-control endpoints	

[NFR-SEC-004] Broker ACLs and request authorisation		MUST HAVE
Priority: MUST HAVE Group: Security and trust		
Requirement	Business endpoints that act on a vehicle MUST require the access token with identity and run binding. Broker ACLs MUST prevent vehicle accounts from publishing release or administration messages and from subscribing to foreign vehicle topics. Traffic-light phase messages require the infrastructure access token.	
Acceptance criteria	M1: vehicle A cannot act as B; a vehicle cannot publish on release topics	

[NFR-SEC-005] Secret-free logs and data minimisation		MUST HAVE
Priority: MUST HAVE Group: Security and trust		
Requirement	Logs and the event log MUST NOT contain private keys, credentials or usable tokens; tokens appear as fingerprints only. Only synthetic station identifiers are processed; no personal data is stored (FR-GW-015).	
Acceptance criteria	Inspection of the event schema and of a demo log	

6.2 Deployment (NFR-DEP)

ID	Name	Priority
NFR-DEP-001	Target environment	MUST HAVE
NFR-DEP-002	Helm deployment and failure domains	MUST HAVE
NFR-DEP-003	Health and mode visibility	MUST HAVE

[NFR-DEP-001] Target environment		MUST HAVE
Priority: MUST HAVE Group: Deployment		
Requirement	The CD MUST be deployed into and demonstrated in the provided FACIS Kubernetes environment; source code resides in the client-designated repository. Development builds and unit tests MAY run on contractor systems, including a local broker and test doubles of the OCM W-Stack adapters; test doubles MUST NOT be part of the deployed container images or Helm charts.	
Acceptance criteria	The release runs in the FACIS environment and is witnessed by the client	

[NFR-DEP-002] Helm deployment and failure domains		MUST HAVE
Priority: MUST HAVE Group: Deployment		
Requirement	Delivery MUST use Helm charts with separate deployments for the convoy layer (gateway, geofinder/STS, business broker), each vehicle, the traffic light, the world service and the operations UI. Fault injection MUST be able to stop exactly one of these groups while the others keep running.	
Acceptance criteria	T-12: the convoy layer is stopped while world and vehicles keep running	
	Install and uninstall run without manual steps	

[NFR-DEP-003] Health and mode visibility		MUST HAVE
Priority: MUST HAVE Group: Deployment		
Requirement	Every service MUST expose a health interface. The dashboard MUST show a demo-ready indicator (health, valid status, free reservations, standstill, end of the STS start-up hold), the active profile, the NATIVE/MOCK labels and the release tag.	
Acceptance criteria	Health, demo-ready indicator and release tag are witnessed	

6.3 Timing (NFR-TIM)

ID	Name	Priority
NFR-TIM-001	Stopping bounds (informative)	MUST HAVE
NFR-TIM-002	Call timeouts	MUST HAVE
NFR-TIM-004	Issuance halt	MUST HAVE
NFR-TIM-005	UI update	MUST HAVE
NFR-TIM-006	Time base	MUST HAVE

[NFR-TIM-001] Stopping bounds (informative)		MUST HAVE
Priority: MUST HAVE Group: Timing		
Requirement	The system MUST implement the stopping mechanisms behind the bounds of Table 6a so that every vehicle reaches standstill by local expiry or protective stop in each demonstrated fault case. Table 5a is informative: it explains the expected stopping time with the Table 5 defaults; measured times are shown in the event log, not qualified against the bounds.	
Acceptance criteria	M4/M5: every affected vehicle reaches standstill; times are visible in the event log	

[NFR-TIM-002] Call timeouts		MUST HAVE
Priority: MUST HAVE Group: Timing		
Requirement	Every call to the OCM W-Stack or PCM Cloud MUST have a timeout (call_deadline, default 5 s, Table 5); on timeout the result is SERVICE_UNAVAILABLE.	
Acceptance criteria	Unit test: a delayed response leads to SERVICE_UNAVAILABLE	

[NFR-TIM-004] Issuance halt		MUST HAVE
Priority: MUST HAVE Group: Timing		
Requirement	The emergency stop MUST halt all STS issuance within halt_budget (default 1 s, Table 5), with reachable and blocked downlinks alike.	
Acceptance criteria	M5: the confirmed emergency-stop command is recorded as FAULT_INJECTED (fault type EMERGENCY_STOP); no TOKEN_ISSUED is signed later than its onset plus halt_budget; the dashboard shows the halt as successful only after the STS has acknowledged it	

[NFR-TIM-005] UI update		MUST HAVE
Priority: MUST HAVE Group: Timing		
Requirement	Dashboard fields MUST update within the UI update interval (default 1 s, Table 6); when no update arrives the display MUST mark itself stale.	
Acceptance criteria	A paused event stream is shown as stale	

[NFR-TIM-006] Time base		MUST HAVE
Priority: MUST HAVE Group: Timing		
Requirement	All components MUST use the NTP-synchronised clock of the Kubernetes environment for timestamps. Local deadlines and protective-stop timers MUST run on a monotonic clock and MUST NOT be affected by wall-clock adjustments.	
Acceptance criteria	Inspection: deadline and protective-stop timers use the monotonic clock	

6.4 Event log and demonstration evidence (NFR-EVD)

ID	Name	Priority
NFR-EVD-001	Event log	MUST HAVE
NFR-EVD-004	No-message demonstration	MUST HAVE

[NFR-EVD-001] Event log		MUST HAVE
Priority: MUST HAVE Group: Event log and demonstration evidence		
Requirement	Each business event MUST carry event_type, timestamp, component, run_id, release_mode, the capability label (NATIVE/MOCK) where a verification or status result is involved, and the applicable session and station IDs. Failure events carry a Table 4 code. The events of Table 5a MUST be emitted and shown in the dashboard.	
Acceptance criteria	The event log of the demonstration contains the Table 4a events with the listed fields	

[NFR-EVD-004] No-message demonstration		MUST HAVE
Priority: MUST HAVE Group: Event log and demonstration evidence		
Requirement	In M4 the business downlink of the affected vehicle MUST be blocked during the withdrawal window, and the event log MUST show that no business message and no TOKEN_CLEAR reached that vehicle until standstill.	
Acceptance criteria	M4: blocked downlink, local expiry stop and server-side invalidation are visible in the event log	

6.5 Configuration and repository (NFR-CFG)

ID	Name	Priority
NFR-CFG-001	Versioned configuration	MUST HAVE
NFR-CFG-003	Repository, build and CI	MUST HAVE
NFR-CFG-004	Unit tests	MUST HAVE

[NFR-CFG-001] Versioned configuration		MUST HAVE
Priority: MUST HAVE Group: Configuration and repository		
Requirement	All timing, model and scenario settings MUST be versioned in the repository together with the profile schema (FR-CFG-001). Secrets and generated run IDs MUST NOT be configuration inputs.	
Acceptance criteria	The profile used in the witnessed demonstration is identified by its repository tag	

[NFR-CFG-003] Repository, build and CI		MUST HAVE
Priority: MUST HAVE Group: Configuration and repository		
Requirement	The complete CD implementation (ORCE flows, custom nodes, UI, Helm charts, fixtures, tests) MUST be delivered in the client-designated repository with pinned dependencies and reproducible build instructions. CI (GitHub Actions) MUST run lint, unit tests and the standard XFSC licence/dependency scan. Every change to the main branch MUST enter through a pull request that a named person has approved after review; direct pushes to the main branch MUST be disabled. Code and tests produced with AI assistance follow the same rule.	
Acceptance criteria	The client rebuilds and deploys the tagged release from the repository	
	Inspection: branch protection of the main branch requires an approving review, and every merged pull request of the tagged release shows a named approver	

[NFR-CFG-004] Unit tests		MUST HAVE
Priority: MUST HAVE Group: Configuration and repository		
Requirement	Unit tests MUST cover token validation in the order of Table 2a and the drive state machine (T-04, T-05), the token deadline, the discovery reference vectors of Table 5g, the motion proof including T-10, the STS session logic, the status age rule, the profile consistency checks and the traffic-light checks; they run in CI. Each test that implements a step of Table 3a, a row of Table 5b or 5c, a vector of Table 5g or an edge check of Section 10.3 MUST name that step, row, vector or check and assert the result stated there.	
Acceptance criteria	The CI report of the tagged release shows these tests passing	
	Inspection: every step of Table 2a, every vector D-01 ... D-12, every combined vector of T-05 and T-10 maps to at least one named test that asserts the stated result	

6.6 Delivery and documentation (NFR-DEL)

ID	Name	Priority
NFR-DEL-001	Handover documentation	MUST HAVE
NFR-DEL-002	Integration Note and mandatory tool stack	MUST HAVE
NFR-DEL-003	Licences	MUST HAVE
NFR-DEL-005	Demonstration script	MUST HAVE

[NFR-DEL-001] Handover documentation		MUST HAVE
Priority: MUST HAVE Group: Delivery and documentation		
Requirement	The handover MUST contain an English README, installation, start, stop and reset instructions, the interface description, credential provisioning instructions via OCM W-Stack/PCM Cloud, the documented mocks (if any) and a demo runbook covering M1–M5.	
Acceptance criteria	A client operator follows the runbook and runs a nominal demonstration	

[NFR-DEL-002] Integration Note and mandatory tool stack		MUST HAVE
Priority: MUST HAVE Group: Delivery and documentation		
Requirement	The contractor MUST deliver an Integration Note (1–2 pages) recording the FACIS credential profile, the OCM W-Stack, PCM Cloud, ORCE and FACIS UI Builder versions used, the MQTT broker product and version, the FACIS trust list used for verification, the holder arrangement (FR-GW-014), whether the OCM W-Stack distinguishes verification sub-reasons (FR-GW-004) and any client-approved mock (FR-GW-003). The CD MUST be built on ORCE (flows and custom nodes), OCM W-Stack, PCM Cloud and the FACIS UI Builder package.	
Acceptance criteria	Client review of the Integration Note	
	All components run as ORCE instances; credentials via OCM W-Stack/PCM Cloud; UI via FACIS UI Builder	

[NFR-DEL-003] Licences		MUST HAVE
Priority: MUST HAVE Group: Delivery and documentation		
Requirement	All code MUST be licensed under Apache-2.0; only FOSS dependencies compatible with Apache-2.0 MAY be used, and licence notices MUST be delivered with the source.	
Acceptance criteria	Inspection of the delivery and the CI licence scan	

[NFR-DEL-005] Demonstration script		MUST HAVE
Priority: MUST HAVE Group: Delivery and documentation		
Requirement	The demonstration script of Section 10.2 consists of M1–M5 and R, each executed once in the FACIS environment and witnessed by the client; M3 is executed once per release mode (motion-proof/console and coordinated/traffic-light). No other combination is required. The further acceptance evidence is stated in Section 11.2.	
Acceptance criteria	The demonstration protocol records each scenario with date, result and witness	

6.7 Start-delay indicators (NFR-KPI)

ID	Name	Priority
NFR-KPI-001	Start-delay indicators	OPTION

[NFR-KPI-001] Start-delay indicators		OPTION
Priority: OPTION (O-2) Group: Start-delay indicators		
Requirement	With option O-2, for each M3 run the event log MUST record, per rank, the GO issuance time $t_{GO}(r)$, the motion-onset time $t_{move}(r)$ and the start lag $t_{GO}(r) - t_{GO}(r-1)$. No acceptance threshold applies; values are indicators for the comparison of the release modes (FR-OPS-010).	
Acceptance criteria	Values are visible after M3(a) and M3(b)	

7. Data and interface definitions

This section carries the definitions the requirements refer to. Table 5a is informative.

Table 1 Agent-to-drive messages (FR-VEH-014); BRAKE_STARTED and DEGRADATION_STARTED are log events

Message	Direction	Semantics
TOKEN_SET	Agent → drive	Raw release JWT; validated on every receipt (FR-VEH-006); an identical current token extends nothing.
TOKEN_CLEAR	Agent → drive	Regular/emergency/reset clear; begins or preserves braking; clears a fault at standstill, never the session lock (FR-VEH-010).
SM_ACK / SM_NACK(reason)	Drive → agent	Accepted token fingerprint or typed rejection with the reason of the first failing check of Table 3a (Table 5).
SM_STATE	Drive → agent	IDLE/ARMED/ROLLING/FAULT; ROLLING continues while braking; IDLE, ARMED and FAULT only at standstill (FR-VEH-007).

Table 2 Drive state machine (FR-VEH-006 ... 013); rejection reasons follow Table 2a

State	Event → behaviour / next state
IDLE (standstill)	Valid TOKEN_SET(ARMED) of a new admissible session → ARMED · TOKEN_SET(GO) → SM_NACK(SESSION_STATE_INVALID) · invalid token → SM_NACK(reason) · token of a locked session → SM_NACK(SESSION_CLOSED) · TOKEN_CLEAR → stays
ARMED (standstill)	TOKEN_SET(GO), same session, higher token_seq, valid distance $\geq d_{min}$ → ROLLING · invalid or over-age sample → SM_NACK(SENSOR_FAULT) · distance $< d_{min}$ → SM_NACK(SAFETY_STOP) · identical redelivery → SM_ACK, extends nothing · renewal TOKEN_SET(ARMED), same session, higher token_seq → stays ARMED, new deadline · lower token_seq → SM_NACK(TOKEN_STALE) · TOKEN_CLEAR → IDLE, session locked · deadline reached → FAULT(TOKEN_EXPIRED), session locked, DEGRADATION_STARTED
ROLLING ($\leq v_{max}$; continues while braking)	Renewal TOKEN_SET(GO), same session, higher token_seq → stays, new deadline · lower token_seq → SM_NACK(TOKEN_STALE) · deadline reached → braking within delta_local, DEGRADATION_STARTED → FAULT(TOKEN_EXPIRED) at standstill · TOKEN_CLEAR → braking → IDLE · free distance $< d_{min}$ → braking → FAULT(SAFETY_STOP) · missing/invalid/over-age sample → braking → FAULT(SENSOR_FAULT) · TOKEN_SET of the locked session → SM_NACK(SESSION_CLOSED) · role/phase/rank change → SM_NACK(SESSION_STATE_INVALID)
FAULT(reason) (latched, standstill)	TOKEN_SET of the locked session → SM_NACK(SESSION_CLOSED) · TOKEN_SET of a new session → SM_NACK(FAULT_LATCHED) · TOKEN_CLEAR → IDLE (fault cleared, session lock kept; never starts motion)

Table 2a Token acceptance order (FR-VEH-006). The first failing check gives the single SM_NACK reason.

Step	Check (fails when ...)	SM_NACK reason
1	Schema, typ cd-release+jwt, algorithm ES256, exact claim set or policy_version is wrong; an access token presented as a release token fails here	TOKEN_SCHEMA_INVALID
2	Signature is invalid or the	SIGNATURE_INVALID

Step	Check (fails when ...)	SM_NACK reason
	key is not the STS release-token key (issuer/kid)	
3	station_id differs from the vehicle's stationId	STATION_MISMATCH
4	run_id differs from the current run, or no current run_id is set	RUN_MISMATCH
5	Token belongs to a locked session, also while braking or in FAULT	SESSION_CLOSED
6	Token of a new session while FAULT is latched	FAULT_LATCHED
7	now $\geq$ exp, or nbf > now + nbf_tolerance	TOKEN_EXPIRED; NBF_FUTURE
8	Token of the current session with a lower token_seq than the current token, or with the same token_seq and different content (an identical current token is answered SM_ACK and extends nothing); token_seq is never compared across sessions	TOKEN_STALE; TOKEN_SCHEMA_INVALID
9	GO from IDLE, GO-to-ARMED regression, change of role, predecessor or rank, or a token of another session that is not locked while the drive logic is ARMED or ROLLING (including braking)	SESSION_STATE_INVALID
10	For ARMED-to-ROLLING: missing, invalid or over-age	SENSOR_FAULT; SAFETY_STOP

Step	Check (fails when ...)	SM_NACK reason
	distance sample; then valid distance below d_min	

Table 3 Interfaces

Interface	Direction	Semantics
HAL	Vehicle ↔ world service (independent transport)	setTargetSpeed, stop, getDistance, getMotionState with units, validity and timestamps (FR-VEH-015).
Position source	World service → agent	Timestamped x/y/speed with noise; the agent publishes authenticated reports at the profile interval (FR-GEO-005).
Uplink switch	Lab control → vehicle	Per-vehicle switch that suppresses the vehicle's outgoing business traffic (uplink-off fault, Table 6d).
Run control	Lab control → drive logic and agent of each vehicle (authenticated)	run_id at the initial start and at reset step 4 (Table 6e); until it is received the drive logic rejects every token (FR-VEH-004, Table 3a step 4).
Credential	Agent → PCM Cloud → gateway	Credentials issued by the OCM W-Stack into the vehicle's PCM Cloud holder; presented to the gateway (FR-GW-001, FR-VEH-001).
Verification	Gateway → OCM W-Stack	Presentation verification; result labelled NATIVE, with a separate MOCK label for a client-approved supplementing check (FR-GW-003).
Status	Gateway → OCM W-Stack status list	Polling, invalidation and recovery (FR-GW-005, FR-GW-006).
Traffic-light phase	Traffic light → business broker → STS, dashboard	Authenticated phase messages with infrastructure access token (FR-TL-001, NFR-SEC-004).
Console / lab control	Operator → ORCE operations instance	Start, invalidation/recovery, faults of Table 6d, agent stop and status-list block for integration tests, emergency stop, reset (FR-OPS-002 ... 004, FR-SIM-004).

Table 4 Codes

Code / group	Emitter	Meaning
VP_INVALID	Gateway	Negative verification result; sub-reason CREDENTIAL_REVOKED from the status list; CHAIN_INVALID or BINDING_INVALID where the OCM W-Stack distinguishes them (FR-GW-004).
ACCESS_TOKEN_INVALID / IDENTITY_MISMATCH	Request receivers	Authorisation failure or wrong bound identity; also unauthenticated phase messages (FR-GW-002, FR-TL-001).
SERVICE_UNAVAILABLE	Gateway / STS	OCM W-Stack or PCM Cloud unreachable, invalid answer or timeout (FR-GW-004, NFR-TIM-002).
SESSION_CONFLICT / STATE_TIMEOUT / LEAD_UNAVAILABLE	STS	Reservation conflict, named state timeout, lead failure (FR-STs-001, -004, -008).
SESSION_STATE_INVALID	STS / drive	Operation or phase incompatible with the current state.

Code / group	Emitter	Meaning
POSITION_INVALID	Geofinder	Invalid, stale or foreign position report (FR-GEO-001, FR-GEO-005).
TOKEN_SCHEMA_INVALID / SIGNATURE_INVALID / TOKEN_EXPIRED / NBF_FUTURE / STATION_MISMATCH / RUN_MISMATCH / TOKEN_STALE	Drive	Release-token validation failure (FR-VEH-006, Table 3a).
SESSION_CLOSED / FAULT_LATCHED	Drive	Locked session; latched fault (FR-VEH-010, FR-VEH-013, Table 3a).
SENSOR_FAULT / SAFETY_STOP	Drive	Invalid sensing; valid obstacle distance below d_min (FR-VEH-011, FR-VEH-012).
CONFIG_INVALID / RESET_INCOMPLETE	Lab control / starting component	Invalid profile or failed consistency check; failed reset (FR-CFG-001, FR-CFG-002, FR-OPS-004).

Table 4a Business events (NFR-EVD-001). Every event carries event_type, timestamp, component, run_id and release_mode.

Event	Emitter	Additional fields
TOKEN_ISSUED	STS	Operation type (initial ARMED / GO promotion / renewal), sequence, phase, nbf/exp, fingerprint; for a LEAD GO with trigger traffic-light the phase_event_id and T0.
TOKEN_ACCEPTED	Drive	Fingerprint, deadline, state.
RENEWAL_REFUSED	STS	Request ID, code, t_disable where applicable.
PHASE_CHANGED	STS	Previous/new phase; motion report IDs (motion-proof) or rank and offset (coordinated).
BRAKE_STARTED	Drive	Cause and brake time.
DEGRADATION_STARTED	Drive	Mode (standstill), t_exp, session_id, station_id.
STANDSTILL	World / drive	Observed speed, timestamp, drive state.
SESSION_ENDED	STS	DONE/ABORTED and reason.
FAULT_INJECTED	Lab control	Fault type (a Table 6d fault or EMERGENCY_STOP), onset, affected component.
STATUS_CHANGED	Gateway	Credential, operation, NATIVE/MOCK label, request start of the observation.
RESET_COMPLETED	Lab control	New run_id.

Table 5 Parameters (fixed demonstration defaults; may be adjusted during integration within the checks of FR-CFG-002)

Parameter	Default	Used by
TTL / renewal fraction	10 s / 0.5	FR-STs-009, FR-VEH-002
nbf_tolerance	1 s	FR-STs-009, FR-VEH-006
Access-token lifetime	10 min	FR-GW-002
Status poll interval / maximum status age	1 s / 30 s	FR-GW-006, FR-GW-007
delta_local / sensor_max_age	0.10 s / 0.20 s	FR-VEH-009, FR-VEH-011, FR-VEH-012
halt_budget / call_deadline	1 s / 5 s	FR-OPS-003, NFR-TIM-002, NFR-TIM-004
World tick / drive tick / position sample / report interval	0.05 s / 0.05 s / 0.10 s / 1 s	FR-VEH-002, FR-SIM-001

Parameter	Default	Used by
position_stale	3 s	FR-GEO-001, FR-GEO-002, FR-STS-010, Table 6g D-09
v_max / a_accel / a_brake	0.3 m/s / 1 m/s ² / 1 m/s ²	FR-SIM-001
d_min / distance margin	1.0 m / 0.01 m	FR-VEH-007, FR-VEH-011
Vehicle / dummy length	0.20 m / 0.20 m	FR-SIM-001
sigma_pos / lane threshold	0.10 m per axis / 0.30 m	FR-GEO-002, FR-SIM-002
Gap threshold / stable cycles / geofinder cycle	2.20 m / 3 / 1 s	FR-GEO-004
Cut tolerance / discovery distance resolution	0.10 m / 1 mm	FR-GEO-003
Discovery standstill / duration	0.05 m/s / 3 s	FR-GEO-002
v_move / motion reports	0.10 m/s / 2	FR-STS-006
State timeouts proposed/confirmed/issued/armed/rolling	3/3/3/10/60 s	FR-STS-004, FR-TL-003
standstill_epsilon	0.001 m/s	FR-STS-007
Track points / direction	(0,0),(3,0),(3,3),(0,3),(0,0); listed order (12 m perimeter)	FR-SIM-001, FR-GEO-003
Reference lead target	2.0 m	FR-STS-007
UI update interval	1 s	NFR-TIM-005
release_mode	motion-proof (default) or coordinated	FR-STS-006, FR-TL-003
Trigger source	console or traffic-light	FR-TL-002
Coordinated GO offset per rank	1.0 s (to be confirmed by the client within check (4) of FR-CFG-002)	FR-TL-003
Participants / STS / traffic light	3 participants and one reference dummy / one STS / one light (fixed scope)	FR-OPS-007, FR-TL-001

Table 5a Expected stopping times (informative; NFR-TIM-001)

Case	Expected stop	Remark
Local expiry	braking starts $\leq t_{exp} + \delta_{local}$; standstill $\leq t_{exp} + B_{stop}$	$B_{stop} = \delta_{local} + v_{max}/a_{brake} = 0.4$ s with Table 6 defaults.
Uplink off while ROLLING	standstill $\leq t_{fault} + TTL + B_{stop}$ (+ processing time of a renewal sent before t_{fault})	No renewal request arrives after t_{fault} .
Uplink off while ARMED / awaiting GO	standstill $\leq t_{fault} + position_stale + TTL + B_{stop}$	No GO is signed without a fresh position (FR-STS-010).
STS or convoy-layer stop	standstill $\leq t_{fault} + TTL + B_{stop}$	No signature after the stop; world and vehicles continue.
Credential invalidation	standstill $\leq t_{fault} + propagation + TTL + B_{stop}$	Propagation of the OCM W-Stack status list is shown, not qualified.
Emergency stop	standstill $\leq t_{fault} + halt_budget + TTL + B_{stop}$	Also with blocked downlink (FR-OPS-003).

Case	Expected stop	Remark
Sensor invalid while ROLLING	detection $\leq$ last valid sample + sensor_max_age + delta_local; then braking	Protective stop (FR-VEH-012).

Table 5b Status decision rule (FR-GW-011)

Status	Condition	Admission / new session / ARMED / GO	Renewal
Valid	Authentic status list, at least one successful observation, age < maximum status age (measured from the request start of the last successful observation, FR-GW-007), credential not suspended or revoked	Allowed	Allowed
Blocked	No successful observation, unauthentic status list, age $\geq$ maximum status age, or credential suspended/revoked	Blocked	Blocked

Table 5c Session protocol (FR-STS-004)

State	Entry / behaviour	Transition	Timeout
PROPOSED	Atomically reserve participants; send proposal with participants, rank, predecessor, wave_predecessor and release mode (FR-STS-001, FR-STS-015).	All confirm $\rightarrow$ CONFIRMED; reject/timeout $\rightarrow$ ABORTED.	proposed
CONFIRMED	Check roles, identities and valid status.	All initial ARMED tokens issued $\rightarrow$ TOKENS_ISSUED; failed check $\rightarrow$ ABORTED.	confirmed
TOKENS_ISSUED	Await drive acknowledgements; renewal of ARMED tokens with valid status.	All ARMED $\rightarrow$ ARMED; reject/timeout $\rightarrow$ ABORTED.	issued
ARMED	Roles binding (FR-STS-005); LEAD GO on console start or not before T0 of a valid phase message (FR-TL-002).	LEAD motion $\rightarrow$ ROLLING; failure/timeout/red before LEAD GO $\rightarrow$ ABORTED.	armed
ROLLING	Follower GO by motion proof (FR-STS-006) or at T0 + r $\times$ offset (FR-TL-003); at target halt issuance and send STOP (FR-STS-007).	Target and all standing $\rightarrow$ DONE; lead loss/timeout $\rightarrow$ ABORTED (FR-STS-008); in release mode coordinated, a follower GO not signed within the ARMED timeout after T0 $\rightarrow$ ABORTED with STATE_TIMEOUT naming ROLLING (FR-TL-003).	rolling
DONE	All standing; no more issuance.	Terminal.	–
ABORTED	No more issuance; vehicles may still be stopping.	Terminal; reservations persist until the last token has expired plus B_stop (FR-STS-002).	–

Table 5d Demonstrated faults (FR-SIM-004)

Fault	Stopped or blocked	Remains active
Uplink off	Outgoing business traffic of the chosen vehicle (uplink switch)	Agent, drive, world, other vehicles
STS stop	STS (ORCE instance scaled to zero until the following reset)	Gateway, vehicles, world, dashboard
Convoy-layer stop	Gateway, geofinder/STS and business broker	Vehicles, world, dashboard (local view) (T-12)
Sensor invalid	Distance validity of the chosen vehicle	Drive, world
Downlink block (M4)	All business traffic to the affected vehicle, including STOP	Outgoing reports of that vehicle, world

Table 5e Reset (FR-OPS-004)

Step	Action
1	Block new sessions and token issuance.
2	Wait for standstill of every vehicle (by STOP or expiry).
3	Restore this run's credential changes via the OCM W-Stack status list (lift suspension or re-issue); TOKEN_CLEAR local faults; end every injected fault of Table 6d and restart every component it stopped; restore the scenario placement.
4	Distribute a new run_id over the run-control interface (Table 4); lift the block of step 1 and any emergency-stop halt (FR-OPS-003); report demo-ready only after health, valid status, free reservations, standstill and the end of the STS start-up hold (FR-STS-002). Any failure → RESET_INCOMPLETE.

Table 5f Reference placement for M2/M3 (FR-GEO-003, FR-GEO-004, FR-STS-005; vector D-01 of Table 6g)

Object	Front arc length	Role	Clearance
CD-V1	4.90 m	LEAD / NONE	1.70 m to CD-V2 (free distance 1.50 m = $d_{min} + 0.50$ m)
CD-V2	3.20 m	FOLLOW / CD-V1	1.00 m to the dummy; 2.70 m to CD-V3 (gap threshold 2.20 m + 0.50 m)
Dummy	2.20 m	Passive obstacle	1.70 m to CD-V3 (free distance 1.50 m; 0.50 m of travel before the protective stop at d_{min})
CD-V3	0.50 m	FOLLOW_GAP / GAP; wave_predecessor CD-V2	Formation span 4.40 m, below half the 12 m perimeter

Table 5g defines the discovery reference vectors. Inputs are noise-free position reports at the report interval of 1 s, fed into an empty geofinder state from $t = -3$ s on, unless a vector states an earlier start; geofinder cycle n runs at $t = n - 1$ s and evaluates the reports received up to that time. Unless stated otherwise, CD-V1 ... V3 are admitted, unreserved, on the lane centre line and report speed 0 m/s in every report, so that they meet the discovery standstill duration from cycle 1; the dummy sends no reports. Positions are front arc lengths s along the Table 5 track in driving direction (perimeter 12 m); arcs are measured front to front in driving direction. Outcomes give the formation reported under the stable-cycle rule of FR-GEO-004 and, where stated, the cycle at whose end it is reported.

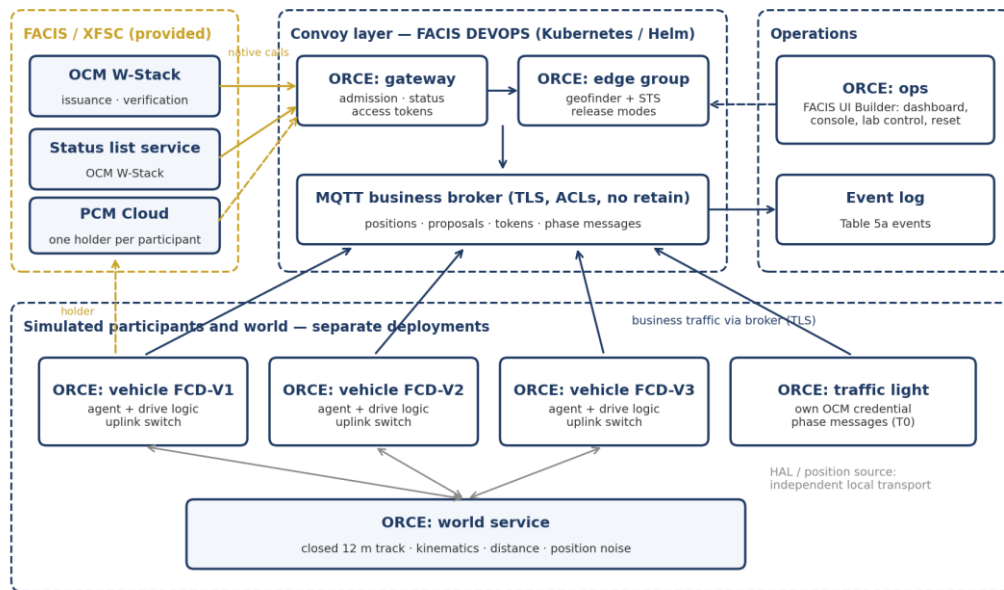
Table 5g Discovery reference vectors (FR-GEO-001 ... 004, FR-CFG-003; unit tests in CI)

ID	Input	Expected outcome
D-01	Reference placement: V1 4.90 m, V2 3.20 m, V3 0.50 m	V1 LEAD/NONE, V2 FOLLOW/V1, V3 FOLLOW_GAP/GAP; wave_predecessor of V3 is V2; reported at the end of cycle 3
D-02	Origin-shifted: every position of D-01 plus 8.00 m modulo 12 m (V1 0.90 m, V2 11.20 m, V3 8.50 m)	As D-01
D-03	As D-01 with V3 at 1.00 m (arc V3 to V2 equals the gap threshold of 2.20 m)	V1 LEAD/NONE, V2 FOLLOW/V1, V3 FOLLOW/V2 (no gap)
D-04	As D-01 with V3 at 0.90 m (arc V3 to V2 is 2.30 m)	As D-01
D-05	As D-01 with V2 reported 0.35 m to the outside of the track at $x = 3.35$ m, $y = 0.20$ m (nearest track point $s = 3.20$ m; lateral distance 0.35 m, above the lane threshold of 0.30 m)	V2 not eligible; V1 LEAD/NONE, V3 FOLLOW_GAP/GAP; wave_predecessor of V3 is V1
D-06	As D-01 with V2 reporting a speed of 0.08 m/s	As D-05
D-07	As D-01 with V1 and V2 holding an active reservation	No formation (one participant)
D-08	As D-01; every report of V2 is delivered twice, and one older report of V2 arrives after a newer one	Duplicates and the older report are discarded; the D-01 formation is reported at the end of cycle 3, as in D-01
D-09	As D-01, but the input starts at $t = -8$ s; V3 reports (standing) only from $t = -8$ s to $t = -4$ s, so that its last accepted report is older than position_stale in every cycle	V3 not eligible; V1 LEAD/NONE, V2 FOLLOW/V1
D-10	Cycle 1 as D-05; from cycle 2 on as D-01	No formation is reported at the end of cycles 1, 2 and 3; the D-01 formation is reported at the end of cycle 4
D-11	V1 7.00 m, V2 3.50 m, V3 0.50 m (span 6.50 m)	No formation (span above half the perimeter)
D-12	V1 6.54 m, V3 0.50 m; V2 at 3.20 m holding an active reservation (arcs 6.04 m and 5.96 m, difference 0.08 m below the cut tolerance; span 5.96 m)	No formation (ambiguous cut); without the cut tolerance V3 would be LEAD/NONE and V1 FOLLOW_GAP/GAP

8. Architecture and implementation approach

8.1 Component overview

Figure 1 Component Overview



All CD components run as separate ORCE instances, each a separate Kubernetes deployment and failure domain: the federation gateway; the edge group with geofinder and STS; the dedicated MQTT business broker; the operations instance with dashboard, console and lab control built with the FACIS UI Builder package; one instance per vehicle containing agent and drive logic; the traffic light; and the world service. The gateway is the only component that calls the OCM W-Stack; vehicles reach the federation only through the gateway (FR-VEH-001). Logic that needs unit tests (token validation, deadline, discovery, STS session logic, profile checks) is implemented as plain JavaScript/TypeScript modules with injected clock and transport, wrapped by thin ORCE custom nodes, and tested in CI without ORCE, the cluster or the OCM W-Stack (NFR-CFG-004). Flows only connect these nodes.

8.2 Design decisions

Decision	Statement	Consequence
Mandatory XFSC/FACIS stack	NFR-DEL-002, FR-GW-013: ORCE, OCM W-Stack, PCM Cloud, FACIS UI Builder	One technology stack; native verification and status; UI conformant with FAP via the UI Builder.
One STS, no dispatcher	FR-STS-001, FR-STS-002	Fixed scope; STS stop demonstrated by expiry stopping.
Token-borne release, expiry as the independent fallback	FR-STS-009 ... 014, FR-VEH-006 ... 010	No message is needed to stop; M4 shows it with blocked downlink.
Two release modes, one switch	FR-STS-006, FR-TL-002, FR-TL-003	release_mode in the profile; coordinated mode with fixed offsets per rank.
Separate failure domains	FR-SIM-002, FR-SIM-003, NFR-DEP-002	Convoy layer can be stopped while vehicles and world keep running (T-12).
Demonstration instead of qualification	NFR-DEL-005, NFR-TIM-001	Acceptance by witnessed demonstration; Table 5a is explanatory.
Testable core modules	NFR-CFG-004, FR-GW-013	Logic in plain modules behind thin ORCE custom nodes; one adapter per OCM W-Stack function; expected test results taken from Tables 2a, 5b, 5c and 5g.

8.3 Dependencies and licences

The technology stack is fixed by NFR-DEL-002 (ORCE, OCM W-Stack, PCM Cloud, FACIS UI Builder package) and NFR-DEP-002 (Helm on the FACIS DEVOPS Kubernetes environment). All code is licensed under Apache-2.0; only Apache-2.0-compatible FOSS dependencies are used (NFR-DEL-003). The MQTT broker product is named in the Integration Note (NFR-DEL-002).

9. Repository and delivery

The client-designated repository holds the ORCE flows and custom nodes, the UI, Helm charts, the profile with schema, the fixtures and discovery reference vectors, the unit tests and the documentation (NFR-CFG-003). Delivered with the source: interface description with example messages (FR-IF-001), code and event list (FR-IF-002), README, runbook and credential provisioning instructions (NFR-DEL-001). The demonstrated release is identified by its repository tag (NFR-CFG-001).

10. Demonstration and verification

10.1 Environment and fixtures

All scenarios run once in the FACIS cloud environment with the profile of the tagged release (NFR-CFG-001): the Table 5 defaults or values adjusted within the checks of FR-CFG-002, with release_mode and trigger source set per M3 run. Fixtures: the reference placement of Table 5f, its origin-shifted variant (Table 5g, D-02) and one obstacle-free fixture for M4 and M5 (FR-CFG-003). Station identifiers CD-V1 ... CD-V3 are synthetic. M3 runs once per release mode (NFR-DEL-005).

Integration tests run once in the FACIS cloud environment with the lab-control switches of FR-SIM-004 and are recorded in the demonstration protocol: the connection to the status list is blocked and released, and admission succeeds again without restart (FR-GW-012); the agent logic of a rolling vehicle is halted with the agent-stop switch, and the vehicle stops by local expiry without any old token restarting motion (FR-VEH-004).

10.2 Demonstration scenarios

Scenario	Content	Exit	Main requirements
M1 Admission and status	Credentials of CD-V1 ... V3 and the traffic light issued via the OCM W-Stack into PCM Cloud (condition precedent); positive admission; rejection of an invalid presentation, a revoked credential and a forged identity (vehicle A for B); rejection of a vehicle identity calling a console or lab-control endpoint and of a vehicle publishing on a release topic; revocation, re-issuance via the OCM W-Stack and recovery via the status list without automatic start.	E1	FR-GW-001 ... 015, FR-VEH-001, FR-TL-001, NFR-SEC-003, NFR-SEC-004
M2 Formation	Reference placement and origin-shifted variant; order, gap segmentation and roles shown on the dashboard.	E2	FR-GEO-001 ... 005, FR-STS-001, FR-STS-005, FR-OPS-001
M3 Wave	(a) motion-proof / console; (b) coordinated / traffic-light T0 with offset per rank. In both: FOLLOW_GAP protective stop before the dummy, target STOP, DONE. With option O-2 the start-delay indicators are shown.	E2	FR-STS-004 ... 009, FR-STS-014, FR-VEH-007, FR-VEH-011, FR-TL-002, FR-TL-003, FR-OPS-007
M4 Withdrawal without message	Obstacle-free fixture; last participant rolling; its credential is revoked via the status list; its business downlink is blocked; it stops by local expiry; the others complete.	E3	FR-GW-005, FR-GW-008, FR-STS-013, FR-VEH-016, FR-VEH-017, NFR-EVD-004
M5 Faults and reset	Obstacle-free fixture; uplink off; STS stop; convoy-layer stop (T-12); sensor invalid; emergency stop with reachable and blocked downlink; each followed by a reset to demo-ready.	E4	FR-STS-002, FR-VEH-009, FR-VEH-012, FR-SIM-003, FR-SIM-004, FR-OPS-002 ... 004, NFR-TIM-004
R Deployment and handover	Helm deployment of the tagged release in FACIS cloud environment; client operator follows the runbook; demonstration protocol signed.	E5	NFR-DEP-001 ... 003, NFR-CFG-003, NFR-DEL-001 ... 005

10.3 Edge checks

Check	Case	Expected result	Form
T-04	TOKEN_CLEAR, then an old still-valid GO token	No motion; old session stays closed (SESSION_CLOSED)	Unit test
T-05	Each check of Table 2a failing alone. Combined failures: locked session and expired; locked session and invalid signature; FAULT latched, new session and wrong station; old ARMED token of the same session, still within its validity window, after GO; GO from IDLE with an invalid sensor sample; old run and expired after reset. Access token as release token.	SM_NACK with the reason of the first failing check of Table 2a (SESSION_CLOSED, SIGNATURE_INVALID, STATION_MISMATCH, TOKEN_STALE, SESSION_STATE_INVALID, RUN_MISMATCH, TOKEN_SCHEMA_INVALID for the listed combinations); no motion; valid state unchanged	Unit test
T-10	The wave_predecessor of the FOLLOW_GAP participant becomes unavailable (stale position or blocked status) before its motion proof	No GO for the dependent follower; it remains at standstill	Unit test
T-12	Convoy-layer stop with the world running	Vehicles stop by local expiry; vehicle services are not stopped	Demonstrated in M5

10.4 Unit tests in CI

Unit tests cover token validation in the order of Table 2a and the drive state machine (T-04, T-05), the token deadline, the discovery reference vectors of Table 5g, the motion proof including T-10, the STS session logic, the status age rule (FR-GW-007), the profile consistency checks (FR-CFG-002) and the traffic-light checks of FR-TL-002; they run in CI (NFR-CFG-004).

11. Delivery, acceptance and scope control

11.1 Change control

Scope changes require an explicit client decision and are recorded in the repository change log. An unmet condition precedent of Section 4 is decided in the same way; the decision states its effect on milestone dates and effort.

11.2 Client acceptance

Acceptance is recorded by the client on the demonstration protocol once E1–E5 are met, the CI report of the tagged release shows every unit test of Section 10.4 and every unit test named in the acceptance criteria of Sections 5 and 6 passing, the integration tests have passed, every acceptance criterion of Sections 5 and 6 that is verified by inspection (Section 5) is recorded in the protocol without open finding. Ordered options are accepted as stated in Section 2.3. Acceptance is not inferred from silence or from deployment alone.

12. Storyline traceability

Each requirement is assigned to the exit criteria whose scenarios its acceptance criteria name. Requirements verified only by unit test, integration test or inspection are listed separately.

Exit criterion	Scenarios	Requirements
E1	M1	FR-GW-001, FR-GW-002, FR-GW-003, FR-GW-004, FR-GW-005, FR-GW-009, FR-GW-014, FR-GW-015, FR-VEH-001, FR-TL-001, NFR-SEC-003, NFR-SEC-004
E2	M2, M3, T-05, T-10	FR-GEO-003, FR-GEO-004, FR-STS-004, FR-STS-005, FR-STS-006, FR-STS-007, FR-VEH-006, FR-VEH-011, FR-OPS-001, FR-OPS-007, FR-CFG-003, FR-TL-002, FR-TL-003
E3	M4	FR-GW-005, FR-GW-008, FR-GW-011, FR-STS-010, FR-STS-013, FR-VEH-009, FR-VEH-016, FR-VEH-017, FR-OPS-001, FR-CFG-003, NFR-TIM-001, NFR-EVD-004
E4	M5, T-04, T-12	FR-STS-002, FR-STS-010, FR-VEH-009, FR-VEH-010, FR-VEH-012, FR-VEH-015, FR-VEH-017, FR-SIM-003, FR-OPS-001, FR-OPS-003, FR-OPS-004, FR-CFG-003, NFR-DEP-002, NFR-TIM-001, NFR-TIM-004
E5	R	FR-GW-001, FR-IF-001, NFR-DEP-001, NFR-DEP-003, NFR-DEL-001, NFR-DEL-002, NFR-DEL-003, NFR-DEL-005
Unit tests, integration tests / inspection only	CI, integration tests (Section 10), inspection	FR-GW-006, FR-GW-007, FR-GW-010, FR-GW-012, FR-GW-013, FR-GEO-001, FR-GEO-002, FR-GEO-005, FR-STS-001, FR-STS-008, FR-STS-009, FR-STS-012, FR-STS-014, FR-STS-015, FR-VEH-002, FR-VEH-004, FR-VEH-007, FR-VEH-008, FR-VEH-013, FR-VEH-014, FR-SIM-001, FR-SIM-002, FR-SIM-004, FR-OPS-002, FR-OPS-006, FR-IF-002, FR-CFG-001, FR-CFG-002, NFR-SEC-001, NFR-SEC-002, NFR-SEC-005, NFR-TIM-002, NFR-TIM-005, NFR-TIM-006, NFR-EVD-001, NFR-CFG-001, NFR-CFG-003, NFR-CFG-004
Options (Section 2.3)	M3 with O-2; M1 and inspection with O-1	FR-OPS-010, NFR-KPI-001; O-1 extends FR-GW-014

13. Glossary

Term	Meaning
Access token	Token issued by the gateway after admission, bound to stationId, tenant and credential identifiers (FR-GW-002).
B_stop	$\Delta_{local} + v_{max}/a_{brake}$: local reaction plus maximum braking duration.
Conditions precedent	Services, credentials and access the client provides after project start, outside the effort frame (Section 4).
Δ_{local} / sensor_max_age	Maximum time from a local stop decision to the start of braking / maximum age of a distance sample that may be used (Table 5).
Demonstration protocol	Record of the witnessed demonstration per scenario with date, result and witness.
Discovery reference vector	Client-defined geofinder input with its expected outcome (Table 5g).
FACIS UI Builder package	FACIS package for building FAP-conformant user interfaces; used for dashboard and console.
Geofinder	Cloud component that discovers formations from authenticated position reports.
Integration Note	Records of the FACIS credential profile, the versions of OCM W-Stack, PCM Cloud, ORCE and FACIS UI Builder, the FACIS trust list, the holder arrangement, the verification sub-reasons provided and any client-approved mock (NFR-DEL-002).
Laboratory abort	The emergency stop of the CD (FR-OPS-003); not a physical emergency stop.
NATIVE / MOCK	Result produced by the OCM W-Stack / by an explicit, client-approved mock that supplements a native result for a recorded gap (FR-GW-003).
OCM W-Stack / PCM Cloud	XFSC organisational credential manager (issuance, verification, status list) / XFSC personal credential manager used as holder per vehicle.
OPTION	Priority of a requirement that belongs to an option of Section 2.3; delivered and accepted only if the option is ordered.
ORCE	Eclipse XFSC orchestration engine based on Node-Red; runtime of all CD components. Link: https://github.com/eclipse-xfsc/orchestration-engine
Release mode	motion-proof (default; GO after proven predecessor motion) or coordinated (GO at $T_0 + r \times \text{offset}$).
Start-up hold	Interval of $TTL + B_{stop}$ after an STS start during which no session is opened and no token is signed (FR-STS-002).
STS	Smart-traffic service: the single cloud component that reserves participants, runs the session protocol and issues release tokens.
$t_{disable}$ / t_{exp}	Instant from which the STS signs nothing more for a vehicle / local expiry instant of the vehicle's last accepted token (FR-VEH-016).
T_0	Green-onset time in an authenticated traffic-light phase message.
Test double	Replacement of an OCM W-Stack adapter used in CI and local development only; never deployed (FR-GW-013).
Trigger source	console or traffic-light T_0 (FR-TL-002).
TTL	Release-token lifetime, $exp - nbf$ (Table 5).
Wave predecessor	Previous authorised participant whose motion releases the follower in motion-proof mode.