TECHNICAL WHITE PAPER

RESILIENT PNT FOR AUTONOMOUS MOBILITY

Precision Positioning, Navigation and Timing for Cooperative Collision Avoidance

A system architecture and validation framework for time-aligned state estimation, uncertainty-aware autonomy, trusted Agent-to-Agent exchange, resilient operation when GNSS is degraded, and earlier detection of collision risk across road, air, maritime, rail and industrial mobility.

T.L. TEDFORD ENTERPRISES, INC.

TL Space Technologies and Research

Version 1.0 | 9 September 2026 | International Technical Evaluation

US PATENT 12,142,143 B1

EXECUTIVE BRIEF

The decision in one page

Autonomy becomes safer when every participant can exchange a trustworthy, time-aligned and uncertainty-bounded picture of motion.

THE MOST IMPORTANT REQUIREMENT

A collision-avoidance system must know not only **where** an object is, but **when** that state was true, how fast it is changing, how uncertain the estimate is, and whether the source can still be trusted. High accuracy without integrity, freshness and continuity can create false confidence.

Proposed TLTE contribution

TLTE proposes a resilient PNT and cooperative-safety layer centered on transceiver/repeater **Agents**. Each participating vehicle or infrastructure point can acquire local measurements, maintain a disciplined clock, estimate position and motion with explicit uncertainty, exchange authenticated safety beacons, relay unexpired data through alternate paths, and support predictive conflict analysis at the edge. The approach is intended to complement - not replace - onboard perception, certified navigation sources, operator procedures or vehicle-specific safety controls.

Expected benefits, subject to measured verification

- Earlier awareness of vehicles, aircraft, vessels, robots and vulnerable road users beyond direct line of sight.
- More coherent fusion because measurements and intent are aligned to a common time reference.
- Graceful degradation through GNSS, inertial, map, infrastructure and cooperative relative-position sources.
- Faster local response by keeping safety decisions at the edge while using the wider network for context and coordination.
- Explicit confidence and integrity states so automation can reduce authority or enter a safe condition before an unbounded navigation error becomes a hazard.
- A common data and transport layer that can bridge road, air, maritime, rail, industrial and defense applications through domain-specific gateways.

EVIDENCE POSITION

This paper describes a proposed architecture, engineering rationale and test plan. It does not claim a government award, endorsement, certification, security clearance, combat-proven performance or independently validated whole-system capability. TLTE-reported prior prototype work and proposed performance targets require current, instrumented verification.

DOCUMENT MAP

Scope, contents and evidence status

A technical evaluation document designed for government, OEM, research, infrastructure and allied-partner discussion.

WHAT THIS PAPER COVERS

PNT fundamentals; accuracy, integrity and timing; autonomous-vehicle collision geometry; proposed TLTE Agent architecture; end-to-end message flow; GNSS-degraded operation; cybersecurity; fail-safe behavior; cross-domain uses; metrics; verification; a 30-day initial demonstration; deployment and governance.

WHAT THIS PAPER DOES NOT CLAIM

It is not a safety certification, operational authorization, production specification, contract commitment, patent claim construction or guarantee of zero collisions, continuous connectivity, immunity to jamming/spoofing, packet-loss elimination or EMP survivability. Those outcomes require requirements, test evidence and authority-specific approval.

Contents

04	What safety-critical PNT must provide
05	Why timing becomes distance
06	Proposed reference architecture
07	End-to-end operational process
08	Measurement and timing layer
09	State estimation and integrity
10	Agent mesh and packet handling
11	Predictive collision avoidance
12	Degraded and denied operation
13	Cybersecurity and safety boundaries
14	Autonomous platform applications
15	Performance measures and budgets
16	Verification campaign
17	30-day initial prototype demonstration
18	Deployment roadmap and responsibilities
19	International alignment and conclusion
20	References
21	Joint sign-off

Terminology: PNT means Positioning, Navigation and Timing. GNSS is the generic term for satellite-navigation constellations; GPS is the United States constellation. An **Agent** is TLTE's term for a proposed transceiver/repeater participant at a vehicle, infrastructure point or other authorized endpoint.

01 FOUNDATIONS

What safety-critical PNT must provide

PNT is a chain of evidence about state, time and trust - not a single receiver output.

Positioning	Where is the vehicle or object, in which coordinate frame, and with what orientation?	Supports lane, corridor, altitude, berth, track or work-zone occupancy.
Navigation	Where is it going, what path is permitted, and how should it move from current to desired state?	Links position to route, intent, constraints and maneuver planning.
Timing	When was each measurement true, how closely are clocks aligned, and how old is the received state?	Allows consistent fusion, ordering, ranging, replay rejection and motion prediction.

Six properties that must travel together

Accuracy	Difference between the estimated state and truth.
Integrity	Ability to warn before an error that exceeds the mission alert limit becomes hazardous.
Availability	Fraction of time the required service is ready for use.
Continuity	Likelihood that the service remains usable through the required operation interval.
Freshness	Age of the trusted state when it reaches the decision function.
Authenticity	Evidence that data came from an authorized source and was not altered or replayed.

ACCURACY IS NECESSARY, BUT NOT SUFFICIENT

An estimate may be precise yet wrong, authenticated yet stale, available yet untrustworthy, or accurate at the sensor while too old at the controller. The safety function must consume the state vector together with uncertainty, source health, clock status and age.

Minimum common state

A usable cooperative state should include a reference-frame identifier; three-dimensional position; orientation; velocity; acceleration or turn-rate where available; covariance or confidence bounds; synchronized timestamp; clock uncertainty; sensor/source-health flags; sequence number; message age limit; intended maneuver or path horizon; and authentication metadata.

02 TIMING

Why timing becomes distance

A position is only meaningful when its time is known. At speed, milliseconds convert directly into traveled distance.

The table shows distance traveled during elapsed time only. It is **not** total stopping distance and does not include sensing, actuator response, tire/road conditions, turn dynamics or safety margin.

Urban road vehicle	15.6 m/s (35 mph)	0.31 m	1.56 m	3.90 m
Motorway vehicle	29.1 m/s (65 mph)	0.58 m	2.91 m	7.28 m
Fast road / rail example	33.3 m/s (120 km/h)	0.67 m	3.33 m	8.32 m
Maritime craft	30.9 m/s (60 kn)	0.62 m	3.09 m	7.72 m
Aircraft example	128.6 m/s (250 kn)	2.57 m	12.86 m	32.15 m

The age-of-state budget

MEASURE END TO END

Trusted state age = sensor time-tag error + fusion processing + transmit queue + channel access + relay/routing + receive processing + scheduling delay. Each term should be measured at median, 95th, 99.9th percentile and worst credible operating condition.

Why a common clock changes the result

- It permits measurements from different sensors and vehicles to be propagated to the same epoch before comparison.
- It enables time-of-arrival, time-difference-of-arrival and two-way-ranging methods when hardware and calibration support them.
- It makes stale data visible and supports expiration, ordering, duplicate rejection and anti-replay controls.
- It improves event reconstruction because logs from multiple Agents can be aligned after an incident.
- It allows a controller to expand collision envelopes in proportion to clock uncertainty and data age.

TLTE's reported sub-20 ms beacon concept should be treated as an **update-interval design target**, not as proof of sub-20 ms end-to-end decision latency. Transport, processing, queuing and actuation must be measured separately under load.

03 ARCHITECTURE

Proposed reference architecture

A layered design preserves local safety while using cooperative exchange to extend awareness and resilience.

CORE SAFETY PRINCIPLE Every decision carries a timestamp, uncertainty, integrity state and expiration.

1 SENSE

- GNSS and augmentation
- IMU and odometry
- Radar, lidar, vision
- Map and infrastructure
- Peer ranging

2 ESTIMATE

- Common time base
- Pose and velocity
- Clock state
- Covariance
- Source health

3 EXCHANGE

- Authenticated beacons
- Age and sequence
- Priority and expiry
- Multi-path Agent mesh
- Interoperability gateway

4 ACT

- Conflict envelopes
- Time to closest approach
- Risk and integrity gates
- Alert or coordinated plan
- Safe fallback

Design principles

Local first	The vehicle retains onboard perception and safe fallback. A remote service is not a single point of failure.
Source diverse	GNSS is one input among inertial, odometry, radar/lidar/vision, maps, infrastructure and relative ranging.
Time explicit	Every measurement, estimate and message carries time, time quality and expiration.
Integrity gated	Automation authority depends on bounded uncertainty and health, not merely the presence of a coordinate.
Transport agnostic	The Agent layer is designed to map across authorized radio, wired and backhaul links through adapters.
Fail predictably	Loss of a source, path or clock moves the system through defined degraded states and safe behaviors.

ROLE OF THE TLTE AGENT

The proposed Agent is a cooperative endpoint and repeater. It can time-tag, validate, prioritize, authenticate, relay and expire safety data. It does not make an untrusted measurement true, and it cannot by itself guarantee radio coverage, spectrum access, global reach or collision-free operation.

04 PROCESS

End-to-end operational process

The safety chain is a continuous loop. Each stage produces evidence needed by the next.

01	Acquire	Collect GNSS/augmentation, inertial, odometry, perception, map, infrastructure and peer-ranging observations.
02	Time-tag	Stamp data as close to measurement as practical; record time source, offset estimate and clock uncertainty.
03	Screen	Check plausibility, calibration, signal quality, kinematic limits, cross-source disagreement and cybersecurity indicators.
04	Estimate	Fuse accepted observations into pose, velocity, acceleration, clock state and covariance in an identified frame.
05	Assess integrity	Compare uncertainty and health against the operational alert limits; assign trusted, degraded or unsafe state.
06	Package	Create a compact safety beacon with state, confidence, intent, timestamp, sequence, priority, expiry and authentication.
07	Exchange	Transmit locally; relay only authorized, fresh, nonduplicate traffic across alternate Agent paths as policy permits.
08	Align and fuse	Propagate peer states to a common epoch; reconcile coordinate frames and combine with onboard perception.
09	Predict	Calculate closest approach, time-to-conflict, reachable envelopes and maneuver compatibility over a bounded horizon.
10	Respond and record	Inform, warn, coordinate or actuate only within approved authority; preserve logs and learn from test evidence.

CONTROL RULE

No stage should silently substitute missing certainty. If time, frame, confidence or authenticity is unavailable, downstream functions must see that fact and reduce reliance accordingly.

05 MEASUREMENT

Measurement and timing layer

Diverse sources fail differently. The objective is independence of failure modes, not simply a higher sensor count.

Multi-constellation GNSS	Wide-area absolute position and time	Weak received signals; multipath, blockage, jamming and spoofing; monitor constellation and frequency independence.
Inertial sensors	High-rate relative motion independent of external radio	Error accumulates with time; calibrate bias, temperature and mounting.
Wheel / drivetrain odometry	Useful ground-vehicle speed and displacement	Slip, tire changes and nonholonomic assumptions can mislead.
Radar, lidar and cameras	Relative objects, landmarks and local geometry	Weather, occlusion, lighting, interference and model errors; maintain independent health checks.
Maps and route constraints	Context and physically plausible corridors	Staleness and localization ambiguity; version and validate map provenance.
Infrastructure anchors	Known-position corrections or ranging references	Coverage and survey integrity; protect timing, calibration and physical access.
Peer / cooperative ranging	Relative geometry and shared observations	Correlated errors and malicious peers; authenticate, bound trust and avoid circular certainty.

Clock discipline and holdover

A disciplined clock estimates both time offset and frequency drift. When a primary time source becomes unavailable, the system enters holdover and predicts time from its oscillator model. The usable holdover interval depends on oscillator quality, calibration, temperature, aging and the application's maximum time error. The clock should publish its growing uncertainty so consumers can widen safety margins or reduce authority.

TIME TRANSFER OPTIONS

Authenticated GNSS time; precision time distribution; network or packet time where its uncertainty is acceptable; two-way transfer that estimates path asymmetry; local atomic or high-stability references; and peer comparison as a cross-check, not automatic truth.

CALIBRATION ITEMS

Antenna and cable delay; RF and modem delay; sensor exposure time; operating-system scheduling; timestamp location; serialization; relay residence time; coordinate-frame lever arms; oscillator temperature response; and path asymmetry.

06 INTEGRITY

State estimation and integrity

The system must know when not to trust its own answer.

State estimator

A practical implementation may use an extended or unscented Kalman filter, factor graph, particle method or another validated estimator. The algorithm choice matters less than disciplined modeling of frames, time, sensor bias, correlations, outliers and uncertainty. The state may include three-dimensional pose, velocity, acceleration, attitude, sensor biases and clock offset/drift.

Integrity monitor

- Define alert limits from the operational design domain: lane boundary, separation corridor, altitude band, track authority, berth clearance or worker exclusion zone.
- Calculate protection levels or conservative confidence bounds and compare them with alert limits before enabling safety decisions.
- Use residual tests, innovation monitoring, solution-separation, redundant-source comparison and kinematic plausibility to detect faults.
- Model common-mode failures. Two receivers using the same antenna, constellation, correction stream or map are not fully independent.
- Track time to alert: a detector that eventually finds an error may still be unsafe if the warning arrives after the maneuver deadline.
- Expose uncertainty to the collision engine. Do not collapse confidence into a hidden yes/no flag.

AUTHENTICATED DOES NOT MEAN CORRECT

Cryptographic authentication can establish origin and message integrity. It cannot prove that a sensor was calibrated, the transmitter's location was true, or its estimate was free of spoofing. PNT integrity requires independent physical and statistical checks in addition to cybersecurity.

Collaborative localization

Cooperative relative measurements can improve estimation and fault detection when geometry and error correlations are understood. U.S. DOT research has demonstrated improved estimation and lower integrity risk in a specific two-vehicle experimental setup [13]. That evidence supports further testing of collaboration; it does not validate TLTE's implementation or guarantee gains in every geometry, density or threat condition.

07 COOPERATIVE LAYER

Agent mesh and packet handling

Safety traffic must be fresh, prioritized, bounded and resistant to loops, floods and stale replay.

Identity and protocol	Protocol/version, authorized Agent or pseudonym, equipment class and capabilities.
Time	Measurement epoch, transmit time where required, clock source, clock uncertainty and age limit.
Kinematics	Coordinate frame, position, orientation, velocity, acceleration/turn rate and vehicle dimensions.
Confidence and health	Covariance/confidence bounds, protection/integrity status, source-health and degraded-mode flags.
Intent	Route segment, maneuver, trajectory samples or reachable set over a limited horizon, with confidence.
Transport control	Sequence, priority, expiry/time-to-live, hop limit, geographic relevance and duplicate identifier.
Security	Authentication tag/signature, certificate or key reference, authorization scope and anti-replay evidence.

Relay and routing rules

- Safety-critical local awareness receives priority over bulk telemetry, diagnostics and nonurgent backhaul.
- Expired state is discarded. Store-and-forward is appropriate only while a message remains useful for its declared purpose.
- Sequence numbers, origin identifiers and content hashes support duplicate suppression; hop limits and geographic scope bound propagation.
- Path selection can score latency, packet delivery, congestion, trust and diversity. Multiple routes improve resilience only when they do not share the same failure point.
- The network should report delay and loss to the consumer. It should not hide degraded transport behind a last-known coordinate.
- Gateways map to authorized V2X, aviation, maritime, rail or tactical formats while preserving time, frame, uncertainty and provenance.

PACKET-LOSS POSITION

A mesh can mitigate packet loss through diversity, forward-error correction, selective repetition and alternate routing. It cannot promise zero packet loss. The collision function must remain safe when individual or sustained message losses occur.

08 COLLISION AVOIDANCE

Predictive collision avoidance

The goal is to identify incompatible occupancy of time and space early enough for a safe response.

SHARED STATE AT A COMMON TIME

Vehicle A pose + velocity + uncertainty

Vehicle B pose + velocity + uncertainty



Relative position and closing speed

PREDICTIVE TEST

r = pB - pA

vrel = vB - vA

tCPA = clamp[-(r dot vrel)/(vrel dot vrel), 0, H]

dCPA = norm(r + vrel x tCPA)

The conflict envelope expands as data ages or uncertainty grows.

From point estimates to reachable envelopes

A point estimate is inadequate for safety. Each participant should be represented by a time-indexed envelope that accounts for vehicle dimensions, state covariance, clock error, data age, motion-model uncertainty, road/airspace/waterway constraints and feasible maneuvers. A conflict occurs when envelopes overlap within the decision horizon and the probability or conservative bound exceeds the application's threshold.

Risk ordering

Awareness	Potential interaction exists but separation is comfortably above thresholds.	Track and update; no maneuver.
Advisory	Predicted separation is narrowing or uncertainty is growing.	Increase update priority; inform operator or planner.
Warning	Conflict threshold may be crossed within reaction horizon.	Issue clear warning; coordinate compatible maneuver where authorized.
Intervention	Imminent hazard and control authority is approved with adequate integrity.	Brake, steer, stop, loiter, climb/descend or otherwise enter validated safe behavior.
Integrity stop	Required PNT confidence cannot be bounded.	Do not guess. Reduce authority and execute domain-specific minimum-risk condition.

SENSOR PLUS COOPERATION

Cooperative PNT can reveal intent and hidden participants; onboard perception can detect unconnected obstacles and verify peers. The strongest safety case fuses both. Neither channel should be treated as universally sufficient.

09 RESILIENCE

Degraded and denied operation

Resilience means controlled service reduction with visible uncertainty, not pretending that the primary source never failed.

GREEN	AMBER	RED
Trusted sources agree	One or more sources degraded	Integrity cannot be bounded
Normal cooperative operation	Increase uncertainty; constrain autonomy	Alert, stop, loiter or revert safely

GNSS blockage / loss	Signal loss, geometry degradation, receiver flags, cross-source residuals.	Continue with inertial, odometry, perception, map, anchors and cooperative relative state; grow uncertainty with time.
GNSS jamming	Broad signal degradation, AGC/noise changes, multi-frequency or nearby-Agent correlation.	Quarantine affected measurements, geolocate interference only where authorized, prioritize terrestrial/relative sources, reduce authority.
GNSS spoofing	Implausible time/position shift, source disagreement, multi-antenna/angle checks, clock and dynamics inconsistencies.	Reject or isolate suspect source, roll back to last trusted state, increase protection level, alert and log.
Timing-source loss	Offset/drift monitor, missed synchronization, peer disagreement.	Enter calibrated holdover, publish clock uncertainty, constrain ranging and time-critical functions as error grows.
Communications loss	Missed beacons, rising loss/latency, route failure.	Maintain local sensing and minimum-risk behavior; seek alternate path; never assume silence means an empty path.
Anchor or peer compromise	Identity failure, inconsistent survey, impossible kinematics, reputation/health alarms.	Remove from solution, revoke authorization where supported, retain forensic record, avoid trust propagation.
Power / electromagnetic event	Voltage/current, resets, RF front-end or clock anomalies.	Protected power, shielding, filtering, redundancy and recovery procedures; validate at component and system level.

EMP AND HARDENING

EMP robustness cannot be established by network logic alone. It requires defined threat levels, enclosure and cable design, surge/overvoltage protection, antenna and power-path treatment, component selection, environmental testing and independent qualification. This paper makes no tested EMP-survivability claim.

10 TRUST

Cybersecurity and safety boundaries

A connected safety layer must assume external networks and peer inputs can be delayed, malformed, compromised or deceptive.

Identity and authorization	Mutual authentication where applicable; role- and message-level authorization; revocation; pseudonym strategy for privacy-sensitive civil use.
Freshness and anti-replay	Trusted timestamps, sequences, expiry, bounded clock error, nonce/challenge where needed and replay-window monitoring.
Data integrity	Cryptographic integrity plus semantic checks for physical plausibility, frame consistency, sensor health and cross-source agreement.
Platform integrity	Secure boot, signed updates, hardware root of trust where appropriate, least privilege, memory protection and protected key storage.
Segmentation	Separate external radio and application processing from safety-critical vehicle-control networks through constrained gateways and allowlists.
Availability	Rate limits, congestion control, priority queues, diversity and graceful local operation during denial-of-service or network partition.
Audit and recovery	Tamper-evident time-aligned logs, key/certificate lifecycle, incident response, rollback protection and recovery to known-good state.
Supply chain	Configuration control, bill-of-materials visibility, vulnerability management, controlled tools and independent verification of critical components.

Safety boundary for external data

The Agent network should provide advisory state to a safety gateway. Direct actuation requires a separately approved interface, hazard analysis and deterministic bounds. NHTSA guidance treats external vehicle networks as untrusted and recommends segmentation and strong gateway controls for safety-critical functions [11]. The same principle applies across air, maritime, rail and industrial vehicles.

PRIVACY BY PURPOSE

Collision avoidance generally needs recent local state, not permanent identity or indefinite location history. Minimize collection, restrict geographic and temporal scope, rotate civil identifiers where lawful, enforce retention rules and separate operational safety records from unrelated tracking uses.

11 APPLICATIONS

Autonomous platform applications

The common architecture is reusable; alert limits, coordinate frames, communications and safe states remain domain specific.

Road vehicles	Intersection movement, forward collision, blind zone, lane change, platooning and vulnerable-road-user awareness.	Lane-relative pose, heading, low state age, map version and local perception. Brake, slow, hold lane or stop within validated conditions.
UAS and advanced air mobility	Three-dimensional deconfliction, corridor/vertiport awareness, swarm spacing and contingency landing support.	Altitude/reference-frame discipline, 3D protection levels, high dynamics and lost-link rules. Loiter, separate, return or land as approved.
Maritime autonomous vessels	Closest-point-of-approach, port/harbor maneuver, formation and sensor-sharing beyond visual obstruction.	Chart datum, vessel dimensions, currents, heading/rate of turn and variable link delay. Slow, hold, alter course or stop where feasible.
Rail	Train separation, work-zone and grade-crossing awareness, consist tracking and maintenance robotics.	Track-constrained location, direction, braking curve, movement authority and infrastructure timing. Enforce restrictive signal or stop.
Industrial, mining and logistics	Worker/vehicle separation, yard/warehouse routing, convoy and robotic fleet coordination.	Indoor/outdoor continuity, local anchors, map/geofence control and low-speed high-precision relative state. Controlled stop.
Defense and emergency mobility	Contested-environment convoy, unmanned teaming, responder routing and shared operational awareness.	Assured/alternative PNT, emission and security policy, mission-specific cryptography and degraded procedures. Mission-defined minimum-risk state.

What carries across domains

- Common time and coordinate-frame declaration; explicit uncertainty and integrity; data expiry and priority; source provenance and authorization; route diversity; local fail-safe operation; and instrumented verification.
- The Agent can act as an adapter around existing standards. It should not force one radio, one navigation source or one vehicle-control protocol onto every operator.
- NHTSA describes vehicle-to-vehicle messages containing heading, speed and location used to assess collision threats [12]. ETSI's position-and-time facility similarly emphasizes position, time, confidence and cooperative updates [9].

12 MEASUREMENT

Performance measures and budgets

A credible program converts every benefit statement into a metric, a condition and a pass/fail rule.

Position and velocity error	Horizontal, vertical, along-track and cross-track error versus independent truth; report distributions, not only averages.	Determines spatial separation confidence.
Time error and holdover	Offset from traceable reference, drift rate and time until operational limit after source removal.	Controls fusion, ranging, freshness and logs.
Protection level / integrity risk	Conservative error bound, alert limit, probability of hazardous misleading information and time to alert.	Prevents precise-looking unsafe output.
Age of trusted state	Measurement epoch to availability at the collision function, including relays and queues.	Converts directly to motion uncertainty.
Update continuity	Inter-update gap distribution and longest outage under density, interference and route failure.	Reveals burst loss hidden by average rate.
Packet delivery and duplication	Delivery by deadline, out-of-order/duplicate rate and geographic relevance under load.	Measures useful information, not raw throughput.
Conflict-detection quality	Probability of detection, false alarm, missed detection, alert lead time and maneuver compatibility by scenario.	Links PNT/network results to safety value.
Recovery	Time and state error after source restoration, rekey, route healing, reboot or power interruption.	Measures operational resilience.

Requirement format

CONDITION + METRIC + THRESHOLD + EVIDENCE

Example: 'Within the defined closed-course operational design domain, at N participating Agents and the specified channel load, 99.9 percent of authorized safety states shall reach the collision function before the application deadline, measured from hardware timestamp to application receipt against synchronized instrumentation.' The actual N, deadline and threshold must be negotiated and justified.

Do not use a single nominal accuracy or beacon rate as a proxy for safety. Publish results by environment, speed, geometry, Agent density, interference condition, software build, hardware configuration and percentile. Preserve raw time-tagged data so an independent party can reproduce the analysis.

13 VERIFICATION

Verification campaign

Testing progresses from deterministic laboratory evidence to closed-course and operationally representative trials.

Nominal PNT	Static and dynamic routes with independent surveyed / inertial truth.	Error distributions, protection levels, continuity, state-age budget.
Timing and holdover	Remove or step the primary time source across temperature and load.	Offset, drift, time-to-limit, alarm and recovery.
Multipath, blockage and urban canyon	Repeat geometries with buildings, canopy, tunnel or shielded zones.	Source transitions, bias rejection and uncertainty growth.
Authorized jam / spoof testing	RF simulator, shielded facility or approved range with controlled waveforms.	Detection probability, time to alert, false alarm, quarantine and fallback.
Mesh density and mobility	Scale Agent count, speed, channel load, partitions, relay loss and route churn.	Deadline delivery, gaps, duplicates, route recovery and compute load.
Collision scenarios	Intersection, rear-end, crossing, merge, head-on, converging 3D paths and hidden participant.	Alert lead time, detection / miss / false alarm and safe response.
Cyber adversarial	Replay, malformed packet, unauthorized origin, compromised peer, flooding and downgrade attempts.	Rejection, containment, auditability and safe degradation.
Environmental / hardware	Temperature, vibration, EMC, power transient and applicable qualification profiles.	Clock, RF and compute stability; recovery; no unsafe output.

Independent evidence chain

- Freeze requirements, hardware, firmware, software, maps, keys and test configuration before each formal run.
- Use an independent ground-truth system whose failure modes do not mirror the unit under test.
- Time-synchronize the unit, truth system and network capture; record calibration and uncertainty of the test equipment.
- Pre-register pass/fail criteria and scenario counts; report failures and exclusions, not only successful demonstrations.
- Repeat across representative environments and with blinded or third-party witness where program decisions depend on the result.
- Trace every claim in the final report to data, configuration, analysis script and responsible reviewer.

SAFETY GATE

A demonstration proves only the configuration and conditions tested. Expansion to public roads, controlled airspace, navigable waters, rail operations or safety-critical control requires the responsible authority's approval and domain-specific assurance.

14 DEMONSTRATION

30-day initial prototype demonstration

A focused test can establish whether the core PNT-to-Agent-to-conflict chain merits a larger program. It is not a certification or global-network demonstration.

DAY-ZERO PREREQUISITES

Access to candidate transceiver/chipset hardware; at least 3-6 instrumented Agents or emulators; two mobile platforms or hardware-in-the-loop equivalents; closed test area; independent position/time truth; defined interfaces; safety officer; spectrum authorization; and named engineering owners. Schedule begins when prerequisites are available.

1-5	Freeze use case, hazards, coordinate frames, timing architecture, message schema, target metrics and baseline GNSS-only performance.	Interface control document; safety plan; baseline data; test cards.
6-10	Integrate hardware timestamping, clock-status output, Agent beacon, authentication, sequence/expiry and packet capture.	Two-way authenticated exchange with measured timestamp and transport delays.
11-15	Add fused state and uncertainty; cross-check GNSS with inertial/odometry or simulator; implement trusted/degraded/unsafe states.	State estimate compared with truth; source-loss and clock-holdover record.
16-20	Add peer alignment, closest-approach / conflict envelope and advisory display; run nominal crossing and following scenarios.	Repeatable detection with documented lead time, misses and false alerts.
21-25	Inject packet loss, relay failure, congestion, stale/replay data and controlled GNSS degradation in authorized conditions.	Visible degradation; alternate routing where available; safe rejection and fallback.
26-30	Repeat formal runs; independent witness review; analyze results; document defects and next-phase requirements.	Demonstration, data package, findings report and go / revise / stop recommendation.

Minimum demonstration claims allowed after success

If the data support them, TLTE may state only that the tested prototype configuration exchanged time-tagged cooperative state, measured latency and loss, detected defined conflicts, and entered defined degraded states under the documented scenarios. Claims about production readiness, certification, global coverage, safety improvement at scale, hostile-environment immunity or EMP survivability remain outside this initial demonstration.

15 TRANSITION

Deployment roadmap and responsibilities

Scale should follow evidence: corridor or site first, then federated regions, then cross-domain service where governance and infrastructure support it.

0 Requirements	Operational design domain, hazards, alert limits, interfaces, threat model and data rights.	Stakeholders approve measurable requirements and test authority.
1 Laboratory	Clock, estimator, protocol, security, routing and hardware-in-the-loop fault injection.	Core functions meet lab thresholds with traceable data.
2 Closed course	Real mobility, geometry, density, degraded GNSS, network partitions and collision scenarios.	Independent safety and performance review supports pilot.
3 Limited pilot	Defined corridor, base, port, airfield, yard, mine or campus with trained operators and fallback.	Operational benefit and risk evidence justify expansion.
4 Product / certification	Hardened hardware, production controls, cyber accreditation, domain assurance and maintainability.	Authority and OEM/operator approvals for intended use.
5 Federation and scale	Interoperable regional meshes, roaming/trust policy, timing infrastructure and lifecycle operations.	Sustained service, governance, funding and measured resilience.

Proposed responsibility model

TLTE

System concept and requirements contribution; Agent data-flow architecture; IP and technical documentation; prototype coordination; performance hypotheses; and support for integration, test analysis and corrective design.

PRIME / OEM / OPERATOR

Safety authority; certified or approved sensors, radios and vehicle controls; platform integration; spectrum and cyber compliance; manufacturing; configuration management; operational procedures; training and sustainment.

INDEPENDENT TEST BODY

Ground truth, calibration, controlled fault injection, witnessed procedures, data custody, statistical analysis, requirements traceability and an evidence-based findings report.

GOVERNMENT / REGULATOR

Operational need, protected test access, applicable standards, authorization boundaries, security requirements, acquisition pathway and decision on further evaluation or deployment.

A global service would additionally require deployed Agent density, terrestrial and/or space transport, spectrum rights, infrastructure ownership, cross-border trust, timing traceability, cybersecurity operations, maintenance, privacy rules and sustainable funding. The mesh concept is an enabling architecture; global availability is a separate infrastructure program.

16 ALIGNMENT

International alignment and conclusion

Current public policy and standards point toward layered, complementary and resilient PNT - while leaving implementation claims to evidence.

United States	NIST frames PNT as a risk-management and cybersecurity dependency; U.S. DOT has emphasized complementary PNT demonstration and operationally representative evaluation [1-4].
United Kingdom	The UK framework calls for resilient GNSS receiver chips, holdover clocks, sovereign timing, terrestrial eLORAN and high-accuracy augmentation; the 2026 Space Strategy describes layering space, terrestrial and quantum technologies [5-7].
International aviation	ICAO's complementary PNT direction seeks cooperative integration of ground, space and airborne capabilities to withstand disruption and deceptive signals [8].
Cooperative road transport	ETSI position-and-time management treats timestamp, coordinates and confidence as shared facilities data; NHTSA recognizes both cooperative safety messages and the need for careful AV testing and cybersecurity [9-12].

Standards posture

The architecture should map to the standards selected by the acquiring authority and platform owner. References in this paper are examples of alignment, not claims of conformance. Detailed profiles must define message sets, coordinate frames, timing traceability, cryptography, spectrum, safety assurance, software/hardware lifecycle, privacy, environmental qualification and human-machine interaction for each jurisdiction and domain.

CONCLUSION

PNT is the foundation that lets autonomous systems agree on time and space. The proposed TLTE architecture adds a cooperative layer around that foundation: diverse sensing, disciplined timing, explicit integrity, authenticated Agent exchange, predictive envelopes and controlled fallback. Its value will be established not by the breadth of the concept, but by disciplined tests showing that trusted state arrives early enough, remains bounded under failure and improves decisions without creating a new unsafe dependency.

Recommended next decision

Authorize a joint requirements session and the 30-day closed-course feasibility demonstration described on page 17, with independent ground truth and pre-agreed metrics. Use the resulting evidence to select the next step: refine, expand to an operational pilot, integrate with an OEM/prime platform, or stop. This is the fastest responsible route from architectural promise to defensible proof.

CORPORATE IDENTIFIERS

T.L. Tedford Enterprises, Inc. is identified by UEI DALZWVA9W7T4 and CAGE 8MF75. These are government-contracting identifiers; they are not military-service credentials, security clearances, awards or endorsements. US Patent 12,142,143 B1 was issued 12 November 2024.

REFERENCES

Selected authoritative sources

Sources accessed and checked through 9 September 2026. Draft documents are identified as drafts.

[1] National Institute of Standards and Technology, NIST IR 8323 Rev. 2, Foundational PNT Profile, Initial Public Draft, 6 May 2026. csrc.nist.gov

[2] Cybersecurity and Infrastructure Security Agency, Resilient PNT Conformance Framework, Version 2.0, 2022. cisa.gov

[3] U.S. Department of Transportation, Complementary PNT Action Plan, September 2023. transportation.gov

[4] U.S. Department of Transportation, Complementary PNT Services Rapid Phase II, updated 27 November 2024. transportation.gov

[5] UK Department for Science, Innovation and Technology, Positioning, Navigation and Timing: Overview, updated 2 February 2026. gov.uk

[6] UK Government, UK Space Strategy, 2026, section 'Building Resilient Positioning, Navigation and Timing.' gov.uk

[7] UK Geospatial Commission, Finding the Way Forward: Location Data to Enable Connected and Automated Mobility, 2023. gov.uk

[8] International Civil Aviation Organization, GNSS Radio-Frequency Interference Roadmap - Long-Term Actions, complementary PNT direction. icao.int

[9] European Telecommunications Standards Institute, ETSI EN 302 890-2 V2.1.1: ITS Position and Time Management, 2020. etsi.org

[10] National Highway Traffic Safety Administration, Automated Vehicle Safety, current public guidance. nhtsa.gov

[11] National Highway Traffic Safety Administration, Cybersecurity Best Practices for the Safety of Modern Vehicles, updated 2022. nhtsa.gov

[12] National Highway Traffic Safety Administration, Improving Safety and Mobility Through Vehicle-to-Vehicle Communication Technology, fact sheet. nhtsa.gov

[13] U.S. DOT Repository and Open Science Access Portal, Multi-Vehicle/Infrastructure Jammer/Spoofer Detection and Localization, 2024. rosap.ntl.bts.gov

REFERENCE NOTE

External references support the general engineering and policy context. They do not endorse TLTE, validate the proposed Agent architecture or establish conformance. Any acquisition, safety or certification decision must use the controlling version of the applicable authority's requirements.

JOINT SIGN-OFF

Presented by T.L. Tedford Enterprises, Inc.

Both editions contain both signatories. Only the left-to-right presentation order changes according to the principal communicator.

PURPOSE OF SUBMISSION

This white paper is respectfully presented for strategic, technical, defense, innovation, transportation, industrial and humanitarian evaluation. TLTE welcomes a requirements-led discussion, an appropriately protected technical exchange and a measured prototype demonstration with qualified government, research, prime-contractor, OEM and infrastructure partners.

Respectfully presented for strategic, technical, defence, innovation, industrial and humanitarian consideration.

AUTHORIZED SIGNATURE / DATE

Terry L. Tedford

Founder / Chairman / Frequency Architect
T.L. Tedford Enterprises, Inc.
TL Space Technologies and Research
US Patent 12,142,143 B1
UEI: DALZWVA9W7T4
CAGE: 8MF75
res0416h1@verizon.net
+1 817-808-8052
Aurora, Texas, United States

AUTHORIZED SIGNATURE / DATE

Mike Motrici

Co-Founder / Executive Lead, Global Humanitarian Initiatives
International Diplomatic Relations
T.L. Tedford Enterprises, Inc.
United Kingdom / International Contact
Mmv0512@gmail.com
+44 7833 604339

SHARED COMMITMENT

Technology in service of resilience, safety and humanity.

Contact routing

United States technical, corporate and government-contracting contact: Terry L. Tedford. United Kingdom and international diplomatic/humanitarian contact: Mike Motrici. Either representative may transmit this document; both remain identified on every formal edition.

Document control

Title: **Resilient PNT for Autonomous Mobility**
Subtitle: Precision Positioning, Navigation and Timing for Cooperative Collision Avoidance
Version: 1.0 | Date: 9 September 2026 | Status: Technical white paper for discussion and evaluation
Owner: T.L. Tedford Enterprises, Inc. / TL Space Technologies and Research