TARO v11 Offline Learning Implementation Guide (Research Track)

Date: 2026-02-07
Architecture Basis: `ResearchData/taro_v11.md`

1. Scope

This guide translates v11 architecture into an executable research-to-engineering plan for TARO's offline learning module.

2. Delivery Tracks

Track A: Core engineering - deterministic data and model pipelines - compile-time safety gates - reproducible artifact lineage

Track B: Research evaluation - ablations - sparsity/noise robustness tests - paper-ready experiment reporting

Track C: Product hardening - rollout policy - monitoring, fallback, and regression control

3. Pathway Stones (Milestone Graph)

Each stone has Entry, Work, Exit.

Stone 00: Contract Freeze

- Entry: v10.1 runtime contracts documented.
- Work: freeze non-negotiables for runtime determinism and FIFO.
- Exit: signed v11 constraint checklist.

Stone 01: Data Inventory

- Entry: raw telemetry and base graph assets available.
- Work: profile all source schemas and missingness.
- Exit: `dataset_manifest` v1 with coverage report.

Stone 02: Time Alignment

- Entry: source timestamps identified.
- Work: normalize all time into model engine ticks and timezone policy.
- Exit: alignment validation report with zero ambiguous fields.

Stone 03: Sequence Builder

- Entry: aligned data.
- Work: construct edge/transition sequences by time order.
- Exit: reproducible sequence dataset snapshot.

Stone 04: Baseline Reproduction

- Entry: sequence dataset.
- Work: rerun v10.1 compile and benchmark as control baseline.
- Exit: locked baseline metrics table.

Stone 05: Encoder MVP

- Entry: baseline locked.
- Work: implement edge/context temporal encoder (RNN/LSTM first).
- Exit: stable training convergence on dev split.

Stone 06: Candidate Generator MVP

- Entry: encoder outputs usable.
- Work: generate profile candidates (no structure mutation yet).
- Exit: candidate coverage and score distribution report.

Stone 07: Deterministic Selector

- Entry: scored candidates.
- Work: deterministic top-K + confidence threshold selector.
- Exit: same ranking across repeated runs with identical seed.

Stone 08: FIFO Gate

- Entry: selected profile updates.
- Work: enforce strict FIFO validity and rejection taxonomy.
- Exit: zero FIFO-unsafe proposals in accepted set.

Stone 09: Compile Integration

- Entry: accepted updates.
- Work: inject refined profiles into `.taro` build path.
- Exit: model loads successfully with unchanged runtime contracts.

Stone 10: Routing Metrics Loop

- Entry: first learned model compiled.
- Work: evaluate ETA MAE/MAPE and route regret on held-out set.
- Exit: measurable gain over baseline or rollback decision.

Stone 11: Calibration Layer

- Entry: raw candidate confidence available.
- Work: calibrate confidence and optimize accept/reject frontier.
- Exit: improved calibration and stable fallback behavior.

Stone 12: Robustness Stress Suite

- Entry: calibrated profile learning.
- Work: run sparsity and noise stress tests.
- Exit: robustness curve report (performance vs degradation level).

Stone 13: Structural Proposal Sandbox

- Entry: profile learning stable.
- Work: enable constrained connector-edge proposals in sandbox only.
- Exit: topology-integrity-safe proposal subset.

Stone 14: Structure Safety Gates

- Entry: sandbox structure proposals.
- Work: add legality, direction, geometry, and turn-feasibility checks.
- Exit: only safe structure proposals survive.

Stone 15: Parity Gate Expansion

- Entry: refined model variants ready.
- Work: enforce A* vs Dijkstra parity over pinned random query sets.
- Exit: zero parity failures for release candidates.

Stone 16: Runtime Non-Regression

- Entry: candidate release model.
- Work: compare runtime memory/latency against baseline.
- Exit: within approved SLO deltas.

Stone 17: Auditability Pack

- Entry: stable compile outputs.
- Work: persist candidate decisions, rejection reasons, and lineage hashes.
- Exit: full audit pack for each model build.

Stone 18: Shadow Rollout

- Entry: all offline gates green.
- Work: deploy in shadow mode with no serving impact.
- Exit: shadow metrics consistent with offline validation.

Stone 19: Controlled Rollout

- Entry: shadow success.
- Work: partial geography/time-window rollout under fallback controls.
- Exit: no critical regressions in production telemetry.

Stone 20: Paper Dataset Freeze

- Entry: multiple stable runs completed.
- Work: freeze splits, seeds, configs, and metrics for publication.
- Exit: reproducibility bundle ready.

Stone 21: Ablation Completion

- Entry: dataset freeze.
- Work: execute ablation matrix (candidate policy, K, confidence, structure mode).
- Exit: final ablation tables and plots.

Stone 22: Draft Claims Validation

- Entry: full results available.
- Work: validate each paper claim against data with uncertainty bounds.
- Exit: claim-to-evidence matrix.

Stone 23: Final v11 Gate

- Entry: product and research checks complete.
- Work: release readiness review.
- Exit: v11 profile-learning release candidate signed.

4. Experiment Protocol Standard

For every experiment: - pin data snapshot ID - pin seed list - pin config hash - store metric outputs and confidence intervals - store rejected-candidate reason histogram

No result is accepted without reproducibility metadata.

5. Failure Handling Policy

Hard stop conditions: - non-zero accepted FIFO violations - non-deterministic export artifacts under same seed/input - A*/Dijkstra parity mismatch for release candidate

Soft warning conditions: - modest metric gains with high complexity overhead - unstable calibration near threshold boundary

6. Research Paper Asset Checklist

Must-have artifacts: 1. method diagram tailored to TARO pipeline 2. formal objective and constraints 3. benchmark and ablation tables 4. robustness plots under missing/noisy data 5. runtime non-regression summary 6. reproducibility appendix (seeds, hashes, configs)

7. Recommended Execution Order

1. Stones 00-10 (profile-only path)
2. Stones 11-12 (calibration + robustness)
3. Stones 13-16 (optional structure + parity/system hardening)
4. Stones 17-23 (audit, rollout, and publication closure)

This ordering maximizes learning impact while minimizing architecture risk.