Gemma 3 Autonomous Target Capture: Engineering Research Report (Paper-grade)

Version: 2026-02-07 / Scope: LLM-driven vehicle controller with exploration-memory map and safety guard
Primary dataset: `session_2026-02-07T05-24-11-542Z`

LLM as primary planner | RAG-like memory context | 8-ray sensor fusion | Safety guard + mode hysteresis | Telemetry-first analysis

Abstract

本研究は「LLMを主役とした自律走行」で青ターゲットへの到達・接触を実現するため、 センサ群、探索重みマップ、LLM戦略モード、そして安全ガードを統合した実装の検証を行った。最新セッション（331.1s, 6620 samples）では、**Memory No-Go 平均 20.39%** と 危険セル学習は機能した一方、**Captures/Min 0.181**、**Safety Risk 33.63%**、 **Avg AI Latency 4798.9ms** が主要ボトルネックとして観測された。 追加改修として、壁ヒット境界クランプ、近接危険時ガード強化、戦略スイッチのヒステリシス制御を導入した。

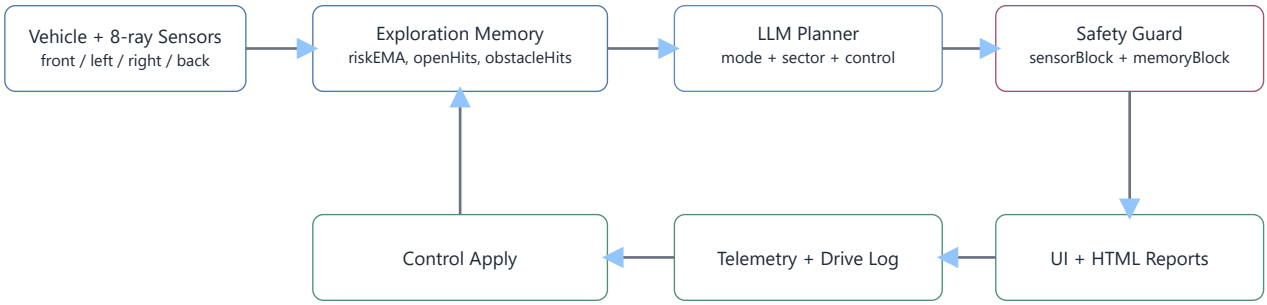
結果として、no-go セルを直接選択する失敗は 0% に抑制されたが、探索偏重と高遅延のため、 目標捕捉効率は依然として研究課題として残る。本稿は実装の再現手順、定量結果、妥当性脅威、 次フェーズ仮説を明示し、継続実験の基盤を提供する。

1. Research Questions

1. RQ1: ヒートマップ由来の記憶情報は、壁回避と探索効率に実効的か。
2. RQ2: LLM戦略モード切替は、局所危険下で安定して制御に反映されるか。
3. RQ3: 高遅延環境において、停止待機・安全ガードが性能劣化をどこまで抑えられるか。

2. System and Method

2.1 End-to-end Architecture



2.2 Memory Representation and Resolution

- Cell size: **2.0m** (`createExplorationMemory`)
- Context radius: **2 cells** (5x5 around vehicle, 24 candidates)
- LLM input is Top-K compressed, not full raster: frontier(3), risky(2), topCandidates(3), topSafeCandidates(3), sectorSafety(4), currentCell.

Scoring Function (implemented)

```
score = 0.95*novelty + 0.40*openBias - 0.95*risk - 0.09*distance
score -= boundsPenalty + unknownPenalty
if barrierBlocked: score -= 0.90
if obstacleDominant: score -= 0.95
if obstacleHits>=1 and risk>=0.62: score -= 0.55
```

Recent Safety Extensions

```
- boundary clamp: hit point outside bounds -> clamp to border cell and record obstacle hit
- front_tight_clamp: reduce forward throttle and bias steering when front arc is tight
- mode hysteresis: cooldown + dwell + vote for mode switching
```

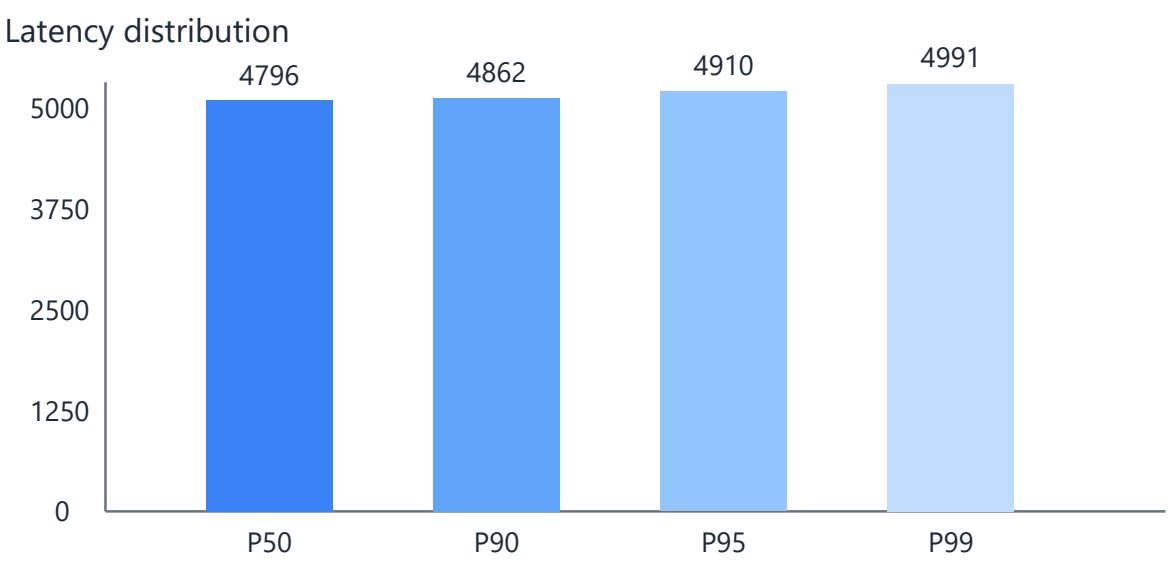
3. Experimental Data and Protocol

Asset	File	Size	Role
Telemetry (time series)	`session_2026-02-07T05-24-11-542Z_telemetry_2026-02-07T05-27-52-304Z_manual.json`	13,016,650 bytes	state, controls, strategy tags, memory diagnostics
Drive log (decision level)	`session_2026-02-07T05-24-11-542Z_drive_gemma_drive_log_2026-02-07T05-26-59-776Z_auto_stop.json`	1,734,188 bytes	LLM prompt/raw, parse method, safety guard, selected controls
Generated report	`session_2026-02-07T05-24-11-542Z_report_driver_limit_report_2026-02-07T05-29-08-186Z.html`	-	KPI summary and analyst narrative

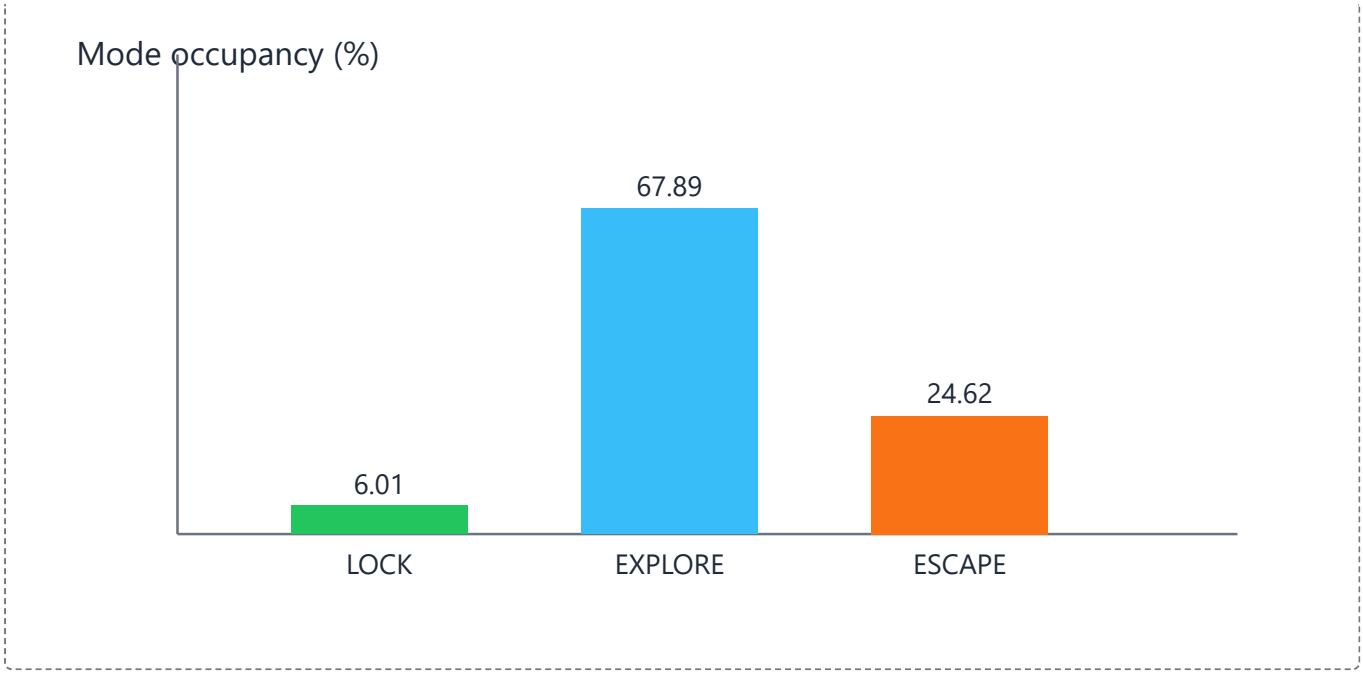
4. Results (Primary Session)

0.181 Captures / Min	**0.408** Intentionality	**33.63%** Safety Risk (<2.5m)
0.48% Stuck Ratio	**4798.9ms** Avg AI Latency	**43.07%** Strategy Switch Rate
67.89% Mode Share: EXPLORE	**24.62%** Mode Share: ESCAPE	**6.01%** Mode Share: LOCK
20.39% Memory No-Go (avg)	**0.00%** Selected No-Go	**1.305** Selected Weight (avg)

4.1 Latency Quantiles (ms)



4.2 Strategy Mode Mix



4.3 Derived Diagnostics

Metric	Value	Interpretation
MinObstacleDist p10 / p25 / p50	2.16 / 2.34 / 3.83 m	下位四分位が2.5m未満で、危険近接が継続的に発生。
MemoryLoopRate avg / p90 / max	0.612 / 1.000 / 1.000	再訪偏重。探索の新規性不足が示唆される。
Unique visited 2m cells	54	セッション長に対し空間カバレッジが限定的。
Edge proximity ratio	19.15%	外周近傍の滞在が高く、壁際行動の影響が残る。
Drive-log parse method	loose_recovery 61 / strict 2	LLM出力のJSON整形依存が非常に高い。
Decision interval (drive log)	avg 5.22s (p50 5.19s)	推論周期が長く、局所回避には不利。

5. Multi-run Trend (Recent 8 Reports)

Source files: latest report + `driver_limit_report_*.html` recent 7 files.

Report	Captures/Min	Safety Risk	Avg AI Latency	Switch Rate	Memory No-Go(avg)	Explore Share
session_..._05-29-08-186Z	0.18	33.6%	4728ms	43.7%	20.7%	68.9%
driver_limit_report_1770437159825	0.00	30.5%	5203ms	50.1%	9.4%	71.8%
driver_limit_report_1770436570876	0.00	30.7%	5189ms	43.2%	11.6%	73.7%
driver_limit_report_1770435646232	0.00	39.5%	4462ms	49.6%	N/A	74.6%
driver_limit_report_1770435326654	0.16	33.2%	4598ms	49.0%	N/A	70.1%
driver_limit_report_1770434634016	0.00	32.0%	4539ms	55.1%	N/A	71.9%
driver_limit_report_1770434072447	0.26	28.2%	4507ms	47.2%	N/A	75.9%
driver_limit_report_1770433510676	0.00	34.1%	4506ms	44.6%	N/A	74.2%

Observation: 最新改修で Safety Risk は最悪値から改善したが、依然 33%台。Explore share は一貫して高く、 Capture efficiency の支配因子として残る。

6. Intervention Summary and Technical Rationale

Intervention	Rationale	Location
Direction flip cooldown	短周期の前後反転を抑え、微振動行動を低減	`src/App.jsx:18, 850`
Inference-time vehicle hold	思考中の惰性移動を遮断し、判断時刻と実行時刻の状態差を縮小	`src/App.jsx (AI loop, applyControls 0)`
Boundary-hit clamp	外周壁ヒットが境界外判定で欠落する問題を修正	`src/services/explorationMemory.js:59, 314`
Aggressive obstacle no-go criteria	単発壁ヒットでも危険セル化し、回避学習を早期反映	`src/services/explorationMemory.js:129, 170, 201`
Safety guard hardening	前方狭隘時の前進をさらに制限し、escape steeringへ誘導	`src/services/ollamaService.js:161-242`
Mode hysteresis	SWITCH乱発抑制。cooldown+dwell+vote で戦略安定化	`src/services/ollamaService.js:5, 543, 802`
Panel visibility and priority HUD	運転監視の認知負荷低減。研究観測性を向上	`src/App.jsx:113, 1081, 1185`

7. Threats to Validity

- **Single-condition bias:** 同一環境・同一地形への依存。一般化は未検証。
- **Latency confound:** 高遅延が戦略品質と制御品質を同時に悪化させ、要因分離が難しい。
- **Parser dependence:** drive-log上、`loose_recovery` 比率が高く、純粋LLM出力の信頼性評価にバイアス。
- **Non-stationary policy:** 実装を頻繁改修中で、厳密なA/B統制が弱い。

8. Conclusion

本時点で、探索メモリは機能しており no-go 選択失敗を抑えている。しかし、目標捕捉性能は未だ低く、 実運用観点では **高遅延** と **探索偏重** が支配的制約である。 したがって次段は、(i) 推論周期短縮、(ii) LOCK優先の戦略重み再設計、(iii) 近接危険時の反射制御強化、 を最優先で進めるべきである。

8.1 Latest Update (2026-02-07 20:39 JST)

This addendum reflects the latest run logs generated after the original paper-grade report was written. Source files: `thelatestlogdata/session_2026-02-07T11-36-42-103Z_drive_gemma_drive_log_2026-02-07T11-39-00-115Z_auto_stop.json` and `thelatestlogdata/OLD/session_2026-02-07T11-19-41-795Z_drive_gemma_drive_log_2026-02-07T11-25-46-766Z_auto_stop.json`.

Metric	Previous Run (12b phase)	Latest Run (4b phase)	Delta / Note
Decisions	27	52	More control cycles executed
Avg AI Latency	12453.4 ms	5628.9 ms	Improved (about 55% faster)
P95 AI Latency	14733 ms	8816 ms	Improved tail latency
Distance (start -> end)	25.00 m -> 24.13 m	25.00 m -> 17.09 m	Approach improved
Minimum Distance to Target	18.61 m	1.65 m	Near-capture behavior observed
Target-hit Decisions	0	7	Target signal acquisition improved
Collision Max	2	12	Safety regressed
Same-Wall Repeat	1	10	Looping near obstacles increased
Reason-blocked Decisions	13	27	More actions were blocked
Reason Validation Pass Rate (last)	0.536	0.534	Almost unchanged
Missing Model Reason Steps	8	22	Main blocker in 4b run

Current Interpretation

- Switching to 4b clearly improves inference speed and target approach behavior.
- Safety degrades at the same time (collisions and same-wall repeats increase).
- The strict reason validator still blocks many steps because model-side reason output is often missing.
- The immediate priority is not AB automation yet; first stabilize reason handling so 4b can execute safe actions consistently.

Immediate Next Actions

1. Relax only `REASON_NOT_FROM_MODEL` under safe-distance constraints and keep sign/risk checks strict.
2. Keep 4b as default while logging reason-source ratios and blocked-step causes each run.

3. After safety recovers, start AB automation with fixed condition matrix (AB-1 to AB-4).

Appendix A. Reproducibility

A.1 Data extraction commands

```
node -e "/* telemetry + drive-log aggregate metrics */"
node -e "/* parse latest report stat boxes for trend table */"
```

A.2 Main code references

`src/App.jsx:18,26,113,463,507,700,850,1081,1185,1534`
`src/services/explorationMemory.js:59,129,170,201,314,323`
`src/services/ollamaService.js:5,161,184,242,543,579,802,909`

This document supersedes: `docs/llm_autodrive_research_report_2026-02-07.html`