Text highlighted in Green is new (introduced by the framework). Uncolored text was in the participant's original requirements.

1. TITLE: Safety Penalties for Traffic Signal Control

SYSTEM_REQUIREMENT: The RL system must incorporate penalties to discourage unsafe behaviors in traffic signal control.
IMPLEMENTATION_DETAILS:
* Penalty discourages excessive queue lengths to prevent congestion and rear-end collisions
* Penalty discourages frequent or abrupt signal changes to prevent erratic phase transitions
* A constraint assigns a probability that a previously applied action will be reapplied consecutively with a default probability of 25% in Atari-like environments.

RATIONALE: Penalties ensure the RL agent does not learn unsafe behaviors that could lead to congestion, confusion, or accidents.

2. TITLE: Weighted Reward Function for Safety

SYSTEM_REQUIREMENT: The system must use a weighted reward function to prioritize safety constraints appropriately.
IMPLEMENTATION_DETAILS:
* Weights are assigned to each safety-related variable based on criticality
* Red-light violations are assigned a higher penalty than signal switching frequency
* Adaptive penalty scaling is used in online learning to adjust weights dynamically based on real-time traffic conditions such as peak pedestrian crossing times.

RATIONALE: A weighted system ensures that safety-critical violations receive higher penalties, maintaining a balance between optimization and safety.

3. TITLE: Normalization and Clipping for Safe Reward Scaling

SYSTEM_REQUIREMENT: The system must normalize and clip rewards to prevent the agent from favoring unsafe high-reward actions.
IMPLEMENTATION_DETAILS:
* Each reward component is normalized to prevent bias
* Safety-related penalties are weighted to dominate reward scaling
* Reward and action clipping prevents extreme values that could bias policy towards unsafe actions.

RATIONALE: Ensuring that no single high-reward action leads to unsafe decisions maintains a stable and safe learning process.

4. TITLE: Real-time Safety Monitoring and Anomaly Detection

SYSTEM_REQUIREMENT: The system must implement real-time monitoring and anomaly detection mechanisms.
IMPLEMENTATION_DETAILS:
* A real-time monitoring system is in place for both maintainability and safety
* Anomaly Detection Systems utilize statistical models and AI-based detectors to identify deviations from normal traffic patterns and trigger corrective actions

* An explainable RL model enables a supervisory controller to monitor and override unsafe actions.
RATIONALE: Continuous monitoring helps detect and mitigate unsafe agent behaviors in real-world scenarios.

5. TITLE: Predefined Safety Constraints for Traffic Signal Control

SYSTEM_REQUIREMENT: The system must enforce predefined safety constraints during execution.
IMPLEMENTATION_DETAILS:
* Minimum and maximum signal duration constraints
* Queue length and spillback prevention measures
* Safe phase transitions using vehicle speed monitoring
* Long-horizon sensors monitor overspeeding cars from a distance.

RATIONALE: Predefined safety constraints help prevent unsafe traffic situations and ensure predictable behavior.

6. TITLE: Safe Mode and Fallback Mechanisms

SYSTEM_REQUIREMENT: The system must include fallback mechanisms for handling failures or unsafe behaviors.
IMPLEMENTATION_DETAILS:
* A predefined Safe Mode is activated when the RL agent fails
* Safe Mode is either human-designed or achieved using a prevalidated agent
* Emergency Stop Mechanism allows immediate suspension of RL control and reverts to a predefined safe state.

RATIONALE: Ensuring that there is a fallback mechanism prevents catastrophic failures in case the RL agent behaves unpredictably.

7. TITLE: Human-in-the-Loop for Supervision

SYSTEM_REQUIREMENT: The system must allow human intervention when necessary.
IMPLEMENTATION_DETAILS:
* Human operators can override the RL system at any time
* Emergency Stop Mechanism provides a hard override
* Traffic control panels allow operators to manually set signal phases
* Intervention is warranted in cases of embedded system failures, sensor malfunctions, pedestrian-triggered emergency stops, unexpected weather conditions, or RL policy drift.

RATIONALE: Human oversight is essential for ensuring safe operation, especially in unpredictable or emergency situations.

8. TITLE: Out-of-Distribution (OOD) Input Detection

SYSTEM_REQUIREMENT: The system must detect and respond to out-of-distribution inputs.
IMPLEMENTATION_DETAILS:
* Statistical models built from realistic simulations detect deviations from expected inputs.

RATIONALE: Detecting anomalies helps ensure the system does not behave unpredictably in unfamiliar situations.

9. TITLE: Anomaly Detection for Multi-Agent Failures
SYSTEM_REQUIREMENT: The system must detect failures in other agents to prevent cascading failures.
IMPLEMENTATION_DETAILS:
Anomaly Detection System is used to monitor multi-agent interactions.
RATIONALE: Detecting failures in other agents prevents compounding safety risks in multi-agent environments.

10. TITLE: Safety in Ongoing Adaptation and Exploration
SYSTEM_REQUIREMENT: The system must validate safety during ongoing adaptation and exploration.
IMPLEMENTATION_DETAILS:
* Human-in-the-loop supervision allows overrides when necessary
* A replica network ensures stable learning in Deep Q-Network-based systems
* RL frameworks use callbacks to save model checkpoints at regular intervals based on performance.
RATIONALE: Ensuring safety during adaptation prevents learning-induced failures and maintains system stability.

11. TITLE: Conservative Exploration for Safety
SYSTEM_REQUIREMENT: The system must use conservative exploration techniques to balance learning and safety.
IMPLEMENTATION_DETAILS:
* Conservative ε-Greedy Exploration limits exploration probability based on risk factors
* Safety checkpoints are used to test models in digital twin environments before deployment
* If a new adaptation worsens safety metrics the system reverts to a previously validated safe policy
* Explainable RL is used to provide justifications for RL decisions.
RATIONALE: Conservative exploration reduces the risk of unsafe actions while still allowing learning and adaptation.

12. TITLE: Uncertainty Estimation for Decision-Making
SYSTEM_REQUIREMENT: The system must quantify and respond to uncertainty in decision-making.
IMPLEMENTATION_DETAILS:
* Ensemble learning is used for confidence estimation
* A confidence-weighted learning rate dynamically adjusts learning based on detected uncertainty.
RATIONALE: Understanding and mitigating uncertainty ensures that the system does not take unsafe actions due to unreliable predictions.

13. TITLE: Safety Metrics for Evaluation

SYSTEM_REQUIREMENT: The system must track safety metrics and define acceptable thresholds.
IMPLEMENTATION_DETAILS:
* Constraint Violation Rate (CVR) is used as a key safety metric
* CVR is calculated as (number of violations / total decision steps) * 100
* CVR thresholds: <=1% is normal <=3% is high-uncertainty based on ISO 26262.
RATIONALE: Tracking safety metrics helps evaluate the effectiveness of safety mechanisms and ensures compliance with standards.

14. TITLE: Safety Metrics Logging and Review
SYSTEM_REQUIREMENT: The system must log and review safety metrics during deployment.
IMPLEMENTATION_DETAILS:
* Periodic performance logging is conducted hourly or daily
* Additional logging is triggered by critical or medium-risk events such as anomalous traffic patterns or safety violations
* In high-risk cases, logging frequency increases to 5-15 minute intervals.
RATIONALE: Continuous logging and review of safety metrics ensure early detection of unsafe trends.

15. TITLE: Performance Degradation Detection
SYSTEM_REQUIREMENT: The system must detect when performance degrades and requires policy updates.
IMPLEMENTATION_DETAILS:
* Primary indicator of safety degradation is an increase in Constraint Violation Rate (CVR)
* Detection of reward trend deviations such as continuous downward trends or rolling average drops beyond a threshold over time
* Safe fallback activation is triggered when degradation is detected.
RATIONALE: Detecting performance degradation ensures timely interventions to maintain safety.

16. TITLE: Training Data Privacy Compliance
SYSTEM_REQUIREMENT: Ensure that the training data does not include sensitive information such as proprietary operational data, PII, or safety-critical system logs.
IMPLEMENTATION_DETAILS:
* Training data is strictly limited to state space and action representations ensuring no inclusion of sensitive information.
RATIONALE: Protecting privacy during training is crucial to preventing the unintentional exposure of sensitive or personally identifiable information.

17. TITLE: Secure Data Transmission
SYSTEM_REQUIREMENT: Implement robust encryption methods to secure data transmission between devices.
IMPLEMENTATION_DETAILS:

Encryption algorithms like Grains and Trivium which are well-suited for embedded systems are used to protect transmitted data.
RATIONALE: Securing data transmission prevents unauthorized interception and ensures that any sensitive information handled remains protected.

18. TITLE: Privacy-Preserving Sensor Selection
SYSTEM_REQUIREMENT: Ensure that selected sensors provide necessary state information while avoiding the capture of identifiable data.
IMPLEMENTATION_DETAILS:
* LiDAR sensors are used instead of cameras to provide necessary state data without capturing personally identifiable information such as license plates or driver identities.
RATIONALE: Using privacy-preserving sensors reduces the risk of collecting unnecessary sensitive data, thereby improving compliance with privacy regulations.

19. TITLE: Localized Data Storage Security
SYSTEM_REQUIREMENT: Ensure that sensitive data is stored only in local infrastructure, reducing exposure to external threats.
IMPLEMENTATION_DETAILS:
* Data is stored using local infrastructure requiring physical security measures rather than software-based controls.
RATIONALE: Minimizing external access to stored data mitigates the risks of unauthorized retrieval and potential cyber threats.

20. TITLE: Preprocessing-Based Data Protection
SYSTEM_REQUIREMENT: Ensure that privacy protections are enforced at the preprocessing stage to prevent data leakage during model training and inference.
IMPLEMENTATION_DETAILS:
* Data leakage prevention depends on the sensor selection and the system responsible for preprocessing ensuring that sensitive data is not exposed downstream.
RATIONALE: Preventing sensitive data exposure during preprocessing helps mitigate risks related to privacy violations during training and inference.