Connector Justification for Competition Form

Response for "Which Confluent connectors are you using?"

Current Implementation: Custom C++ Security Gateway Applications

Due to automotive industry regulatory requirements, our implementation uses custom C++ security gateway applications rather than direct Confluent CDC connectors. This approach is necessary because:

ISO 26262 Functional Safety Compliance:

- Vehicle ECU databases cannot have direct external network connections
- Safety-critical systems require air-gapped network isolation
- All data transmission must pass through certified security gateways

Cybersecurity Regulations (UN-ECE R155):

- Automotive systems must implement secure boundaries between vehicle networks and external connectivity
- Direct database connectors violate established automotive cybersecurity frameworks
- Data validation and encryption must occur at dedicated gateway layers

Production Architecture Integration: In production deployment, our security gateway applications would integrate with:

- **PostgreSQL CDC Source V2 Connector** for fleet management databases
- **Database Sink Connectors** for analytics and reporting systems
- **Schema Registry** for enterprise data governance across vehicle data streams

Technical Justification: Our C++ applications represent the secure telematics gateway layer that automotive systems actually implement in production. Direct CDC connectors would be used downstream for fleet management and analytics databases, while vehicle ECU data requires the secure gateway pattern we've demonstrated.

Enterprise Integration Pattern:

> Vehicle ECU Database → Security Gateway (C++ App) → Kafka → CDC Connectors → Analytics Databases

This architecture demonstrates understanding of real-world automotive deployment constraints while leveraging Confluent's enterprise connector ecosystem where appropriate in the data pipeline.