Using STAMP for the Modeling and Control Of Autonomous Vehicle Fleets at Intersections During Infrastructure Failures and Other Edge Cases

Updates to ISO 26262, ASPICE, SOTIF, ISO 21434

Contact us
Omnex Inc
info@omnex.com
US: +1-734-761-4940
EU: +49-1789888121

Juan Pimentel & Gregory Guska
March 26, 2026

OMNEX
www.omnex.com

Agenda

Introduction

- On December 22, 2025, a power blackout and wireless communication disruption in San Francisco caused a fleet of Waymo robotaxis to stand still, blocking traffic at multiple intersections
- This is not an isolated incident — AV fleets are increasingly vulnerable to infrastructure service failures
- The problem: how do we model, monitor, and control AV fleets at city intersections when the underlying infrastructure fails?
- Focus areas: traffic congestion, availability, and performance — not just safety

Problem Definition & Assumptions

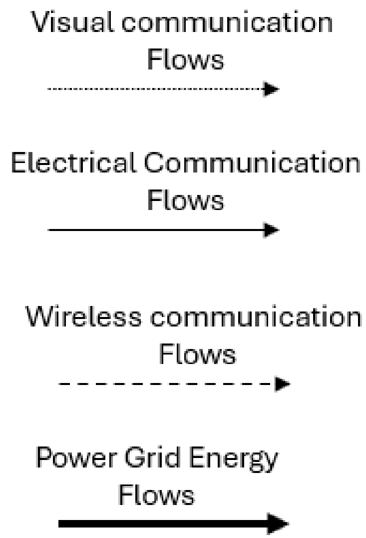
- AV fleets operate without human safety drivers or remote drivers; remote operators provide supervisory support only
- Fleet vehicles rely on wireless communications for remote operator interaction
- Traffic lights at intersections depend on the power grid
- AVs obey traffic laws but cannot control non-fleet vehicles or pedestrians
- Key challenge: infrastructure failures (power outages, wireless disruptions) combined with unpredictable human behavior create severe intersection congestion
- Research goal: develop models, policies, rules, and protocols to mitigate congestion under these conditions

Stakeholders & Actors

- A rich, multidisciplinary set of actors is involved:
  - **Vehicle layer**: Autonomous vehicles (AV), ego vehicle (EV), fleet vehicles (FV), other vehicles (OV)
  - **Operations layer**: Fleet operator (FO), remote operators (RO)
  - **Infrastructure layer**: Power grid (EG), wireless communications, traffic lights (TL)
  - **Environment layer**: Pedestrians, city intersection, emergency responders
  - **Governance layer**: City government, transport regulators, general public
- V2X communications (V2FO, V2RO, V2V, V2I, V2P) connect these layers

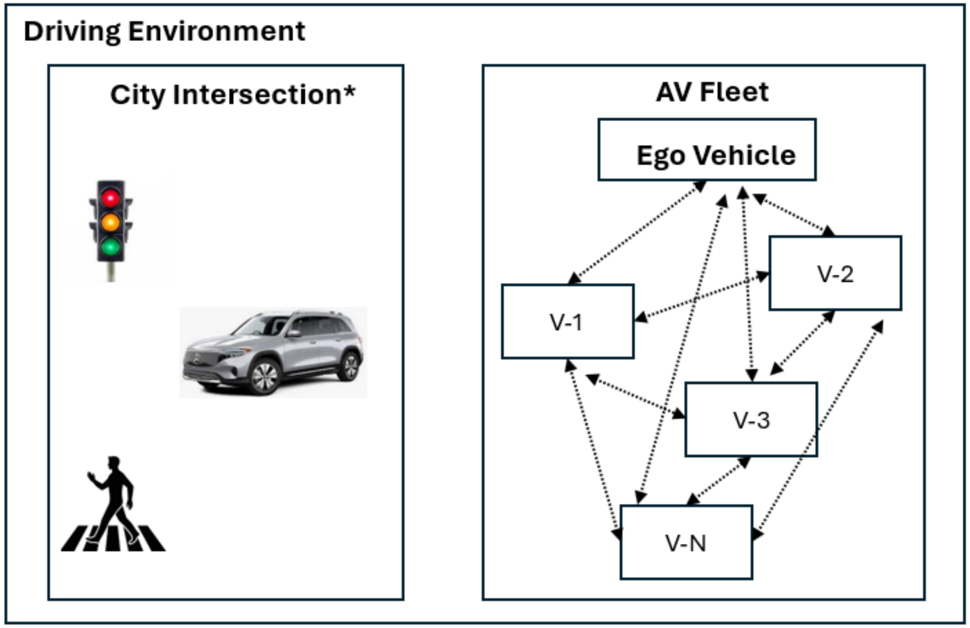
STAMP Framework Extensions

- Standard STAMP was designed primarily for safety analysis; this work extends it in two important ways:
- **Extension 1 — Performance & Availability**: STPA is adapted to address traffic congestion, fleet efficiency, and service availability, introducing *Inadequate Control Actions (ICAs)* alongside the standard Unsafe Control Actions (UCAs)
- **Extension 2 — Visual Monitoring as a Formal Feedback Channel**: Standard STAMP feedback is implicitly sensor/electronic-based; this work formally models visual monitoring — both direct (AV onboard cameras) and remote (operators viewing camera feeds) — as a distinct and explicit feedback channel
- The control structure distinguishes four communication flow types: visual, wireless, electrical, and power grid



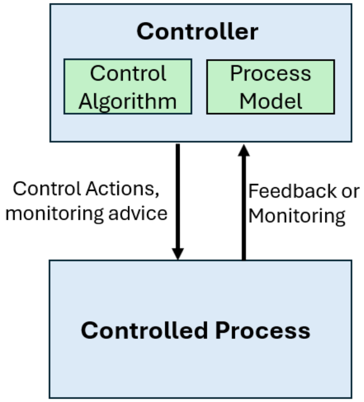
Control & Monitoring Model

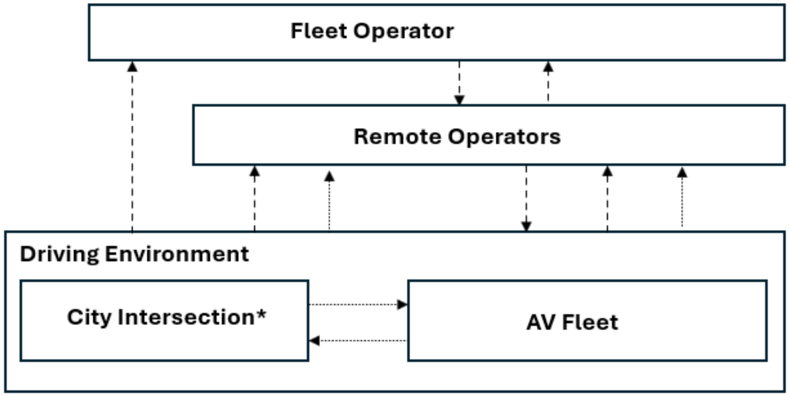
- The driving environment is decomposed into two parts:
  - ***City Intersection**** — traffic lights, non-fleet vehicles, pedestrians; these elements can only be *monitored*, not controlled
  - ***AV Fleet*** — ego vehicle plus N fleet vehicles; these are the controllable elements



Control & Monitoring Model

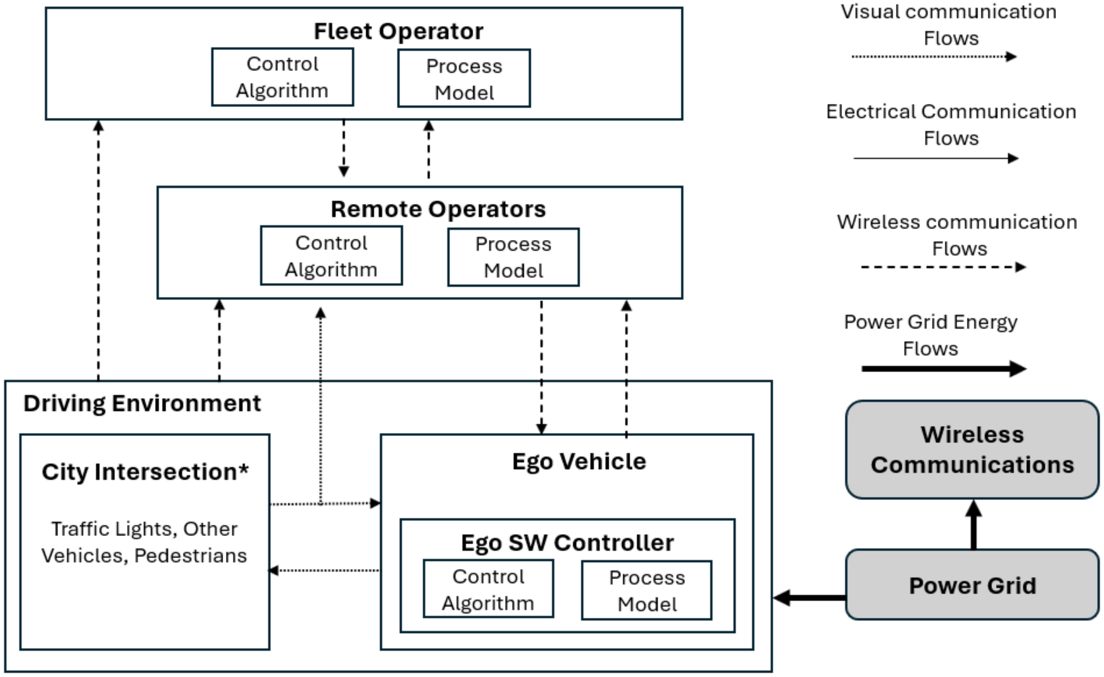
- Underlying basic STAMP control structure is used
  - In a supervisory and hierarchical fashion
- Supervisory control flow: **Fleet Operator → Remote Operators → AV Fleet**
- Control is performed exclusively via wireless communication
- Monitoring is performed wirelessly, visually, or a combination of both
- Remote operators can achieve visual awareness of the intersection through AV onboard camera feeds transmitted wirelessly





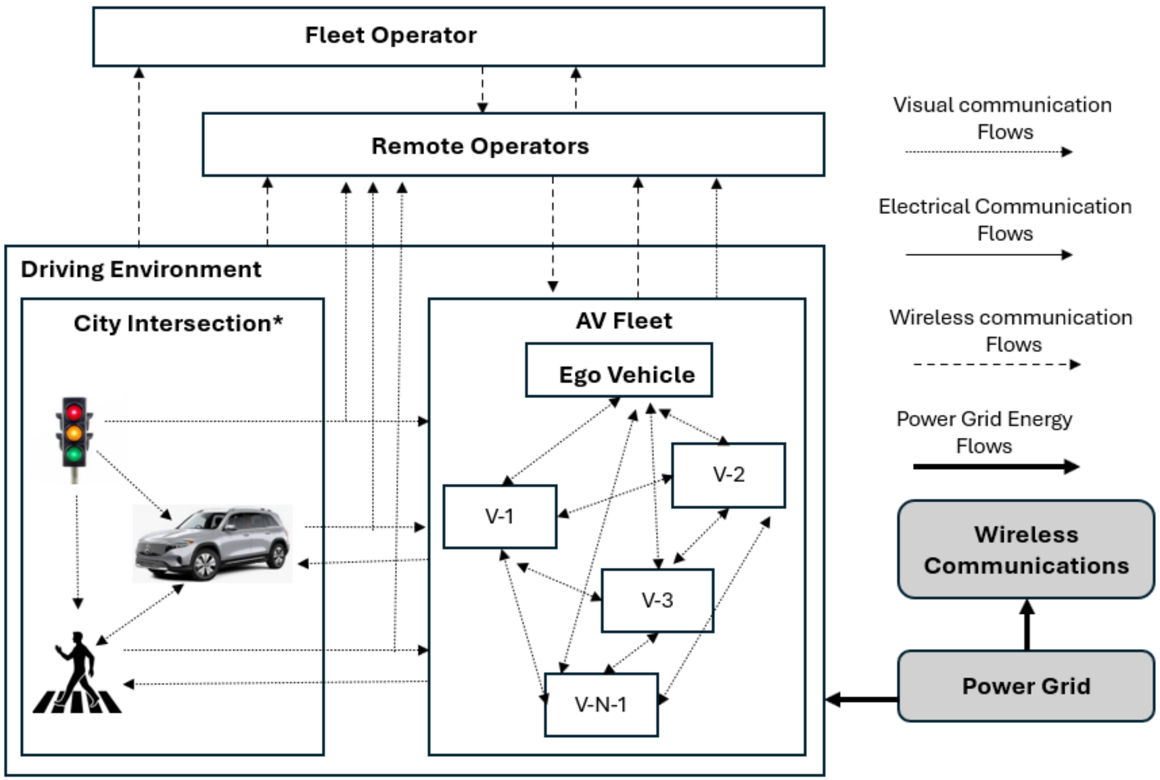
STPA Control Structures

- Two control structure cases are modeled:
  - **Case 1 — Ego Vehicle**: A single AV controlled by one remote operator, who is in turn directed by the fleet operator; the ego vehicle SW controller interacts with the city intersection* and depends on wireless communications and the power grid



STPA Control Structures

- **Case 2 – AV Fleet**: A distributed system of N vehicles and M remote operators; vehicles communicate with each other and with operators through a wireless network; fleet-level concerted control is possible



STPA Results: UCAs, ICAs & Loss Scenarios

- **Losses**: Intersection congestion (L-1), blocking emergency responders (L-2), crashes (L-3), hitting pedestrians (L-4)
- **System Constraints**: Reliability and latency of power grid, wireless communications, remote operator visual monitoring, and ego vehicle perception must all be acceptable
- **Unsafe Control Actions (UCAs)**:
  - UCA-1: Timid driving behavior of the ego controller
  - UCA-2: Remote operator issues incorrect monitoring advice (e.g., reports green light when it is red)

STPA Results: UCAs, ICAs & Loss Scenarios

- **Inadequate Control Actions (ICAs)**:
    - ICA-1/2/3: Remote operator issues incorrect advice regarding status, nature, or location of vehicles at the intersection
- **Key Loss Scenarios** (selected): Power grid outage (S-6), wireless communication outage (S-7), high communication latency (S-8), remote operator overload (S-1), reckless non-fleet drivers (S-10), immobilized vehicles (S-12)

Control Action Requirements & Distributed Protocols

- Control actions must satisfy the following requirements:
  - **Proactiveness** — anticipate failure conditions before they escalate
  - **Robustness** — handle surges in communication load and operator unavailability
  - **Resiliency** — have fallback rules when expected responses do not arrive
  - **Cautiousness** — avoid actions that could worsen congestion or create safety hazards
  - **Distributed** — congestion reduction is a concerted effort across all fleet vehicles, not just a single ego vehicle
- Distributed control protocols are envisioned as a key mechanism, with the fleet collectively negotiating intersection behavior under degraded conditions

Summary & Conclusions

- STAMP is applied to a novel, real-world problem: AV fleet management at intersections under infrastructure failures
- Two meaningful extensions to the STAMP framework are introduced: adaptation for performance/availability and formal visual monitoring modeling
- The *City Intersection** abstraction cleanly separates controllable from uncontrollable elements

Thank You!

Questions?

info@omnex.com
734.761.4940

QUALITY