CIM 2.1.1B **Design Flaws of Self-Driving Vehicles**

Introduction:

A critical review is an important process for the sustainability of a product. In this activity, you analyze Self Driving Vehicles find flaws, and suggest improvements.

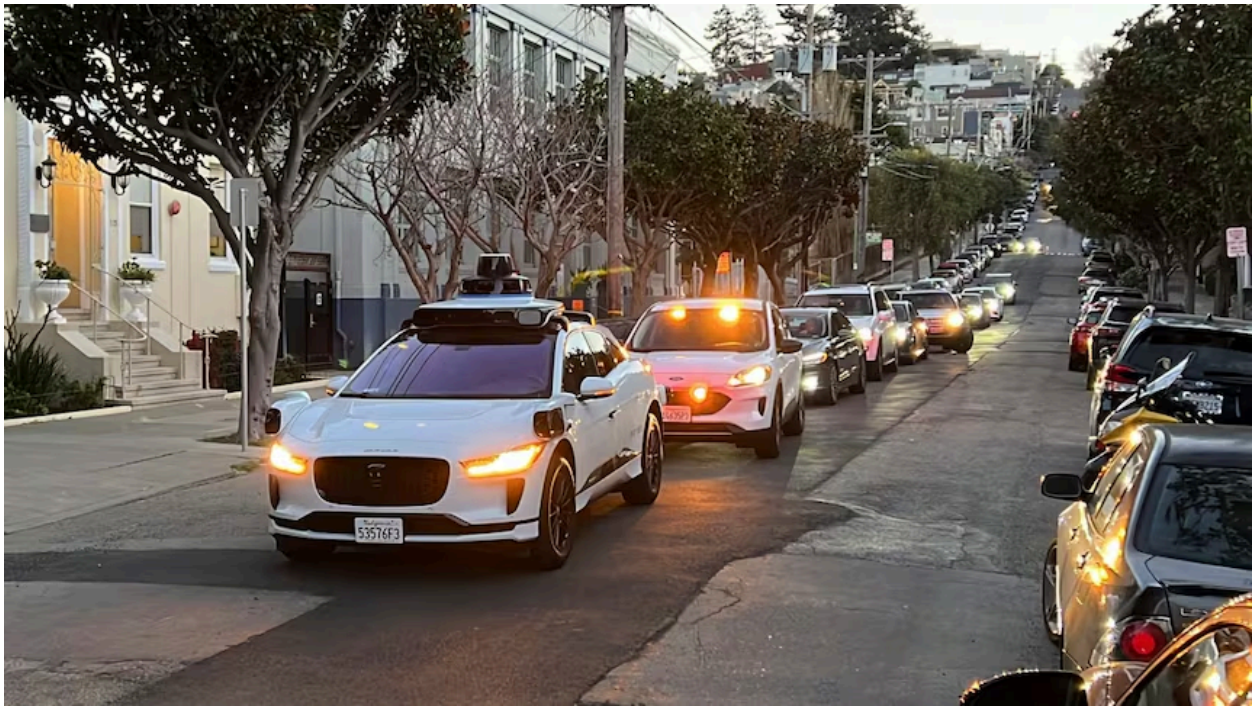
1. Review the Failure Mode and Effects Analysis video.
   https://www.nhtsa.gov/technology-innovation/automated-vehicles-safety

   https://electrek.co/2023/03/24/tesla-hacked-winning-hackers-model-3/#:~:text=Tesla%20was%20successfully%20hacked%20at,working%20closely%20with%20whitehat%20hackers.

   https://www.cbc.ca/radio/asithappens/san-francisco-robotaxi-traffic-jam-1.6938440#:~:text=10%2Dcar%20back%2Dup%20of,issues%20during%20popular%20music%20festival&text=says%20city%20official-,The%20day%20after%20California%20approved%20an%20expansion%20of%20driverless%20taxis,A%20music%20festival.
2. What would you recommend for the process of designing a Self Driving Vehicle? It is highly recommended to conduct more research to answer the questions.
   a. Begin with hazard analysis (FMEA) to identify failures like connectivity loss and cyberattacks.
   b. Translate safety guidance into concrete requirements and test plans.
   c. Define and limit the Operational Design Domain (ODD), expanding only with proven resilience.
   d. Build layered safety with graceful degradation and clear handover policies.
   e. Apply strong cybersecurity principles such as isolation, secure boot, and reduced attack surface.
   f. Validate through simulation, closed-course testing, and transparent public reporting.
3. Review the research attached to this assignment and indicate how you would improve it.
   a. San Francisco Robotaxi Jam: Vehicles stalled when cellular networks overloaded during a festival. Improvement: ensure offline autonomy and event-based deployment limits.
   b. Tesla Hack (Pwn2Own): Researchers chained Bluetooth and gateway vulnerabilities to take control. Improvement: Harden gateways, remove risky wireless paths, and enforce secure boot.
   c. NHTSA Guidance: Emphasizes safety, cybersecurity, and transparency. Improvement: align development with guidance and publish performance data.

Prepare a report of your findings including the following items.

a. Image of the bad design



b. Full description of the chosen product
   Urban robotaxi fleets (e.g., Cruise, Waymo).

c. Intended use of the product
   Safe, efficient driverless passenger transport.

d. Any design flaws with the product
   - Over-reliance on cellular connectivity
   - Poor emergency-response interaction
   - Cybersecurity vulnerabilities

e. Issues with flaws, related to economy, safety, functionality, and ethics
   a. Economy: Gridlock costs and reputational harm
   b. Safety: Delays emergency services and risks secondary crashes
   c. Functionality: Service fails under predictable conditions
   d. Ethics: Deployments without reliance erode public trust

f. Recommendation to redesign the product to correct the flaws described
   a. Connectivity-independent fallback autonomy.
   b. Event-aware geofencing and fleet dispersion.
   c. Built-in emergency responder integration.
   d. Harden gateways, remove insecure wireless pathways.
   e. Graceful degradation to clear lanes instead of blocking.
   f. Transparent safety data publication.

Conclusions:

Name and describe a product you typically use that has a defect related to economy, safety, functionality, and/or ethics.

Voice assistants (e.g., smart speakers) often misinterpret commands, leading to unintended effects or failures in tasks, showing how human-factors flaws reduce trust.

The Engineering Code of Ethics includes the four principles listed below. In what way, if any, do the four principles apply to the design flaws you listed above?

a. Use knowledge and skill for the enhancement of human welfare.
    - Designing SDVs that halt en masse due to bandwidth violates the obligation to enhance welfare; proposed offline fallbacks directly address this.

b. Be honest and impartial and serve with fidelity the public, their employers, and clients.
    - Transparent reporting of incidents/exploits and clear ODD limits honors public trust and customer safety (e.g., disclosure of Pwn2Own-class vulnerabilities).

c. Strive to increase the competence and prestige of the engineering profession.
    - Adopting rigorous security engineering and responder-centric testing elevates professional standards.

d. Support the professional and technical societies of their disciplines
    - Active participation in standards and safety-data initiatives (per NHTSA guidance and AV TEST) aligns with professional bodies' missions.