NAME: ABDULLAH  
ID: 221837

QUIZ 2- Software Design Architecture

# Scenario:

An autonomous vehicle control system is designed to make real-time driving decisions, ensuring safety, fault tolerance, and low-latency responses. The system must process sensor data instantly, detect obstacles, and apply emergency braking if needed, while also ensuring cybersecurity against external attacks.

# Question:

Analyze how real-time processing, fault tolerance, and security interact in this system. Contrast the challenges of balancing these attributes and infer the consequences of prioritizing one over the others. List potential failures that could arise from improper trade-offs.

# Analysis of Real-Time Processing, Fault Tolerance, and Security in Autonomous Vehicle Control System:

## 1. Real-Time Processing:

Real-time processing is super important for autonomous vehicles because they need to make quick decisions. The system needs to process sensor data (like cameras, LIDAR, radar) in real-time so it can detect obstacles and make decisions fast, such as applying emergency brakes when necessary. It’s crucial for the system to respond quickly to avoid accidents.

One of the challenges is that real-time systems need to meet strict time limits, and if the system is too slow, it can’t detect obstacles in time or make the right decision, which is risky.

If we focus too much on real-time processing and ignore fault tolerance or security, the system might work fast but could crash because it doesn't handle errors or attacks properly. This could lead to serious accidents.

## 2. Fault Tolerance:

Fault tolerance is important because it helps the vehicle continue working if something goes wrong, like if a sensor stops working or if there's a failure in the system. The system should be able to switch to a backup to keep the vehicle safe.

The challenge here is that fault tolerance takes extra time, so it could slow down the system, which goes against the real-time needs. If the system checks for problems or switches to backups, it might take too long, and the vehicle could miss important actions like braking.

If we focus too much on fault tolerance and ignore real-time processing, the vehicle could end up making decisions too slowly, causing accidents.

## 3. Security:

Security is super important to protect the vehicle from cyberattacks, like someone hacking into the system or messing with sensor data. If a hacker takes control of the vehicle, it could be disastrous.

The problem is that security measures, like encryption or extra checks, can slow down the system because they add extra processing time. This could make it harder for the system to make quick decisions.

If we focus too much on security and ignore real-time processing, the vehicle could take too long to react, and in a dangerous situation, it might miss an opportunity to act quickly. On the other hand, if we ignore security to make the system faster, the vehicle could be hacked and the system could fail badly.

# Consequences of Prioritizing One Over the Others:

## 1. Prioritizing Real-Time Processing Over Fault Tolerance:

If we prioritize real-time processing and ignore fault tolerance, the vehicle might not detect problems like broken sensors or a failure in the system. This can lead to wrong decisions or even crashes. For example, if a sensor stops working, the system might not switch to a backup, causing a failure in the decision-making process.

## 2. Prioritizing Real-Time Processing Over Security:

If we focus too much on real-time processing and don’t consider security, hackers might attack the system and mess with its sensors or data. This could cause the vehicle to make wrong decisions, like failing to brake or misinterpreting road conditions.

## 3. Prioritizing Fault Tolerance Over Real-Time Processing:

If fault tolerance is given more importance and we ignore real-time processing, the system might be too slow in making decisions. For example, switching to backup systems could delay the decision-making process, and the vehicle might miss avoiding an obstacle.

## 4. Prioritizing Fault Tolerance Over Security:

If fault tolerance is prioritized too much and we neglect security, the vehicle might become vulnerable to cyberattacks. Hackers could take control of the system or manipulate sensor data, which could cause accidents or take control of the vehicle.

## 5. Prioritizing Security Over Real-Time Processing:

If security is prioritized too much and real-time processing is sacrificed, the vehicle might not react fast enough in dangerous situations, which could lead to accidents. Security measures like encryption might add delays that slow down the system.

## 6. Prioritizing Security Over Fault Tolerance:

If security is given too much focus and fault tolerance is neglected, the vehicle might fail to handle system failures. A fault might go undetected, and the vehicle could crash or malfunction.