Lawrence Hua
LHUA
9/19/2024

Table of contents

Goals for the New Dashcam Feature

Organizational Goals

1. **Market Differentiation through Child Detection**
    - **Measure**: Increase in sales after feature launch.
    - **Data**: Sales figures, customer acquisition rates, feedback surveys.
    - **Operationalization**: Track and compare sales figures before and after the introduction of the child detection feature. Conduct customer surveys to determine if this feature influenced purchasing decisions.
2. **Compliance with Data Privacy Regulations**
    - **Measure**: Number of privacy violations or complaints.
    - **Data**: Incident logs, user feedback, legal audit results.
    - **Operationalization**: Monitor privacy-related incidents and conduct regular audits to ensure compliance with privacy laws (e.g., GDPR), reviewing customer complaints related to privacy issues.
3. **Reduction of Development and Operational Costs**
    - **Measure**: Total cost of development and ongoing maintenance.
    - **Data**: Financial records, resource allocation logs.
    - **Operationalization**: Compare initial project cost estimates with actual development and maintenance costs post-launch, and track ongoing costs to ensure they stay within budget constraints.

System Goals

1. **Minimizing Latency in Reporting**
    - **Measure**: Time from child detection to authorities receiving the alert.
    - **Data**: System logs, timestamps of detection and alert transmission.
    - **Operationalization**: Record timestamps for each step in the reporting process and average the time to ensure latency goals are met.
2. **Ensuring Secure Data Transmission**
    - **Measure**: Frequency of successful data transfers without breaches.
    - **Data**: Security logs, breach reports, system monitoring data.
    - **Operationalization**: Track the success rate of data transmissions between dashcam and external devices, conducting regular system audits to maintain encryption and security protocols.
3. **Optimizing Power Usage for Battery-Operated Dashcams**
    - **Measure**: Battery life while using the child detection feature.
    - **Data**: Battery consumption logs, performance test results.
    - **Operationalization**: Test the dashcam in different power modes and monitor battery consumption to ensure optimal usage, especially when relying on battery power.

User Goals

1. **Protecting User Privacy and Data Security**
    - **Measure**: User satisfaction regarding data privacy.
    - **Data**: Customer surveys, privacy incident logs.
    - **Operationalization**: Survey users to assess their confidence in the system's data privacy measures and track incidents where privacy concerns arise.
2. **Providing a User-Friendly Setup and Interface**
    - **Measure**: Ease of setup and user experience.
    - **Data**: Post-purchase surveys, customer support interactions.
    - **Operationalization**: Survey users to evaluate the ease of setup and use of the child detection feature, and review customer support logs to identify recurring usability issues.

3. **Minimizing User Data Charges**
    - **Measure**: Average data usage per user.
    - **Data**: Data usage logs, customer feedback on mobile data costs.
    - **Operationalization**: Monitor real-world data usage and optimize transmission settings to minimize unnecessary uploads, while gathering feedback on user data cost concerns.

Model Goals

1. **Maximizing Accuracy in Child Detection**
    - **Measure**: Precision and recall of the model in detecting children.
    - **Data**: Test results from labeled datasets, real-world detection logs.
    - **Operationalization**: Evaluate the model across diverse conditions (e.g., lighting, weather) and compare performance to benchmark datasets, continuously monitoring real-world precision and recall rates.
2. **Reducing False Positives and False Negatives**
    - **Measure**: Rates of false positives and false negatives in real-world use.
    - **Data**: Test logs, real-world performance reports.
    - **Operationalization**: Regularly test the model using controlled datasets and real-world feedback to refine detection accuracy, minimizing false alerts and missed detections.
3. **Ensuring Model Compatibility with Various Dashcam Hardware**
    - **Measure**: Inference time and resource usage across hardware configurations.
    - **Data**: Benchmark results, performance logs on different dashcam models.
    - **Operationalization**: Test the model on multiple dashcam configurations, tracking processing time and resource use, and adjust model complexity to ensure smooth performance across all hardware.

Goal Relationships

1. **Model accuracy** directly influences **user satisfaction** and **system efficiency** by reducing false positives/negatives and speeding up detection and reporting. Accurate detection minimizes unnecessary alerts and helps authorities respond quickly.
2. **Power optimization** improves **system reliability** for battery-operated dashcams, ensuring extended battery life and preventing users from experiencing outages during critical detections. This also contributes to **user satisfaction** by reducing the need for frequent recharging.
3. **Data transmission efficiency** lowers **user costs** by reducing data usage while enhancing **system latency** through quicker and smaller data transfers, improving both user experience and operational efficiency.
4. **Privacy protection** is essential for maintaining **user trust** and supporting **organizational goals** like compliance with legal regulations. By ensuring strong privacy controls, the company can enhance its brand reputation and prevent potential legal issues.
5. **Minimizing false positives and false negatives** strengthens **system reliability** and **user trust**, reducing unnecessary interventions and ensuring critical detections are not missed, which ultimately improves the product's credibility and marketability.

Environment and Machine

Environmental Entities:

1. **Dashcam hardware**: The physical camera and its sensors that capture footage in vehicles.
2. **Power supply**: The vehicle's battery or a dedicated dashcam battery, which provides the system’s power.
3. **Network connection**: External networks such as Wi-Fi, Bluetooth, or mobile hotspots, required for data transmission.
4. **Lighting conditions**: The lighting in the vehicle's surroundings, which impacts video quality and, consequently, the accuracy of facial recognition.

Machine Components:

1. **AI Component (Facial Recognition)**: This system identifies faces in the footage and matches them against a database of missing children.
2. **Data Transmission System**: Responsible for sending detection data to authorities or central systems, ensuring security through encryption.
3. **Storage Protocols**: Handles local storage and backup in case of network failure, storing footage for a certain time before retrying transmission.

Requirement Decomposition

Requirement (REQ)

The key system requirement is to **minimize latency between detecting a missing child and reporting it to authorities**. This ensures timely action can be taken, meeting the system goal of fast, reliable communication.

Environmental Assumptions (ASM):

1. **Network Availability**: The vehicle is assumed to have access to stable network connections (Wi-Fi, Bluetooth, mobile hotspot) to transmit data.
2. **Power Supply Stability**: The dashcam must have access to continuous power through the car's battery or its own, ensuring uninterrupted operation.
3. **Good Lighting**: Adequate lighting conditions are needed for high-quality video capture and accurate facial recognition.
4. **Authority Availability**: Law enforcement or relevant authorities must be available to receive and act on alerts, and the necessary legal frameworks must be in place to enable this.

Machine Specifications (SPEC):

1. **AI Component (Facial Recognition)**:
    - The system must detect and identify a child from video footage within **5 seconds** of capture, with an accuracy rate of at least **95%**.
2. **Data Transmission**:
    - Upon detection, the system must transmit relevant data (e.g., image, location) to authorities within **1 second** of detection, provided network availability.
    - Data transmission must be encrypted to ensure compliance with privacy standards.
3. **Backup Protocol**:
    - In the event of a network outage, detection data must be stored locally for **up to 24 hours**, with automatic attempts to re-establish connection every **30 minutes**.

Risk Analysis: Fault Tree Analysis for Latency Violation

In this risk analysis, we focus on a critical system requirement: **minimizing latency in reporting missing child sightings**. The top event in this fault tree analysis is the violation of the latency requirement, leading to delayed reporting. We will break down the potential causes of this failure into intermediate and basic events and analyze the minimal cut sets to determine the root causes of the latency violation.

Top-Level Event: Latency Violation

The top-level event represents the failure to meet the system's latency requirement. If the system takes too long to detect, process, or transmit the identification of a missing child, it leads to a delay in reporting to authorities.

Intermediate Events Leading to the Top Event

1. **E1: Delay in Facial Recognition Detection**
    - The AI model takes longer than expected to identify a match, delaying reporting.
2. **E2: Delay in Data Transmission**
    - Network issues delay the transmission of detection data to authorities.
3. **E3: System Power Failure**
    - The dashcam experiences power failure, leading to interruptions in detection and reporting processes.

Basic Events Contributing to Intermediate Events

1. **B1: AI Processing Time Exceeds Limits** (Contributing to E1)
    - The AI model struggles with poor lighting or complex video conditions, causing delays in processing.
2. **B2: Poor Video Quality** (Contributing to E1)
    - Environmental factors like low lighting or obstructions lead to poor video quality, affecting detection.
3. **B3: High Network Latency** (Contributing to E2)
    - Network latency causes significant delays in transmitting the detection data.
4. **B4: Network Unavailability** (Contributing to E2)
    - The system encounters complete network unavailability, preventing data from being transmitted.
5. **B5: Power Supply Loss** (Contributing to E3)
    - The dashcam loses its power source, stopping detection and transmission.
6. **B6: Hardware Failure** (Contributing to E3)
    - Dashcam hardware malfunctions, stopping detection and reporting processes.

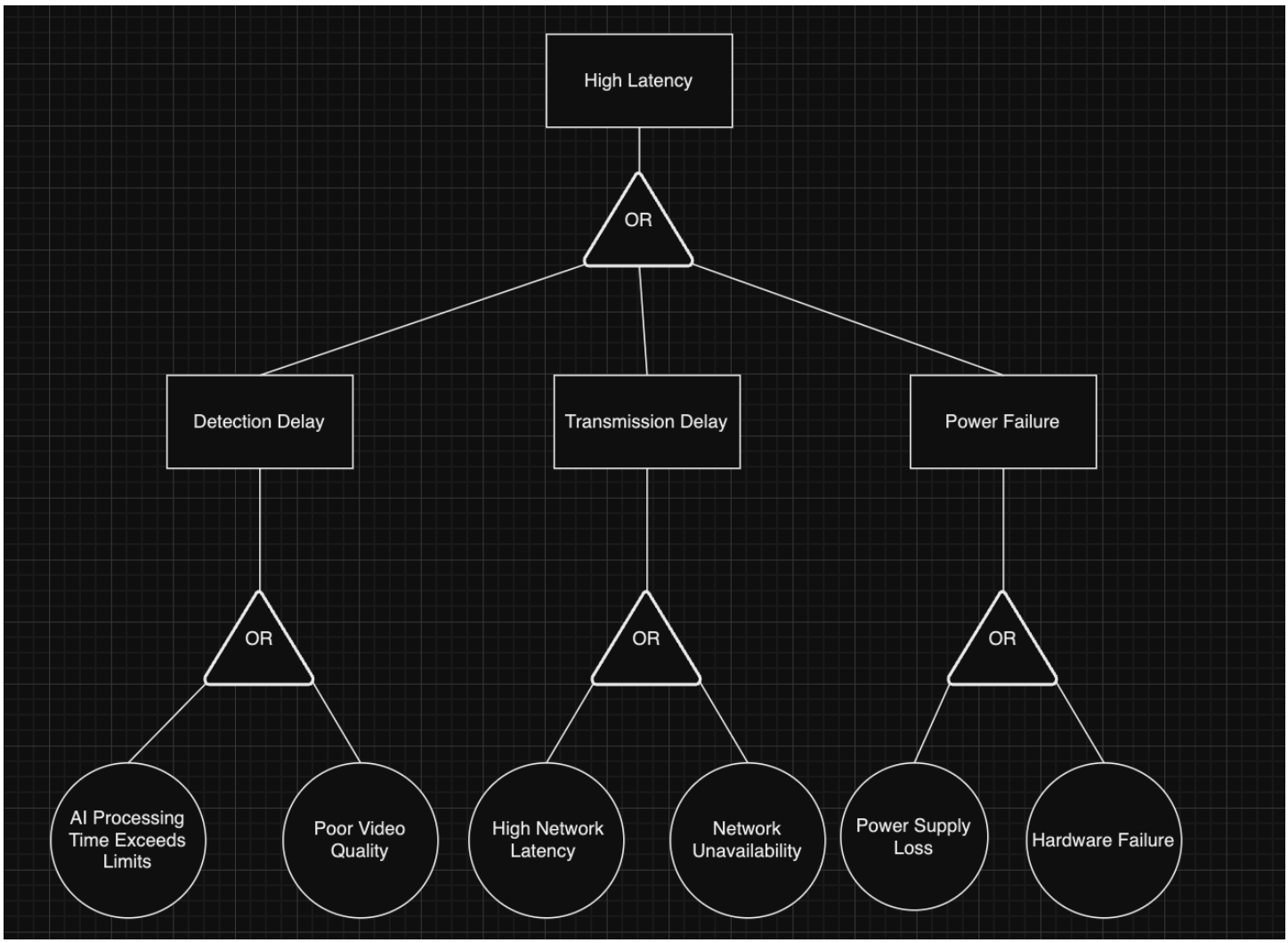
Minimal Cut Sets

Minimal cut sets represent the smallest combinations of basic events that can cause the top event. For this fault tree, the minimal cut sets are:

1. **{B1, B2}**: The AI model fails due to processing delays or poor video quality.
2. **{B3, B4}**: Network issues cause delays, either due to high latency or complete network unavailability.
3. **{B5, B6}**: The system fails due to power loss or hardware malfunction, preventing detection and reporting.

Each of these cut sets represents a critical failure that would lead to the violation of the latency requirement.

Initial Diagram:



Mitigations

To reduce the risk of the failure studied in the fault tree, we propose two system-level mitigation strategies. These mitigations address issues outside the machine learning component and focus on improving the robustness of the system's environment and infrastructure.

Mitigation 1: Redundant Network Connections

Description: Implement multiple network transmission options (Wi-Fi, Bluetooth, and mobile data) to create redundancy. If one network fails, the system automatically switches to another available network, ensuring that data transmission is maintained.

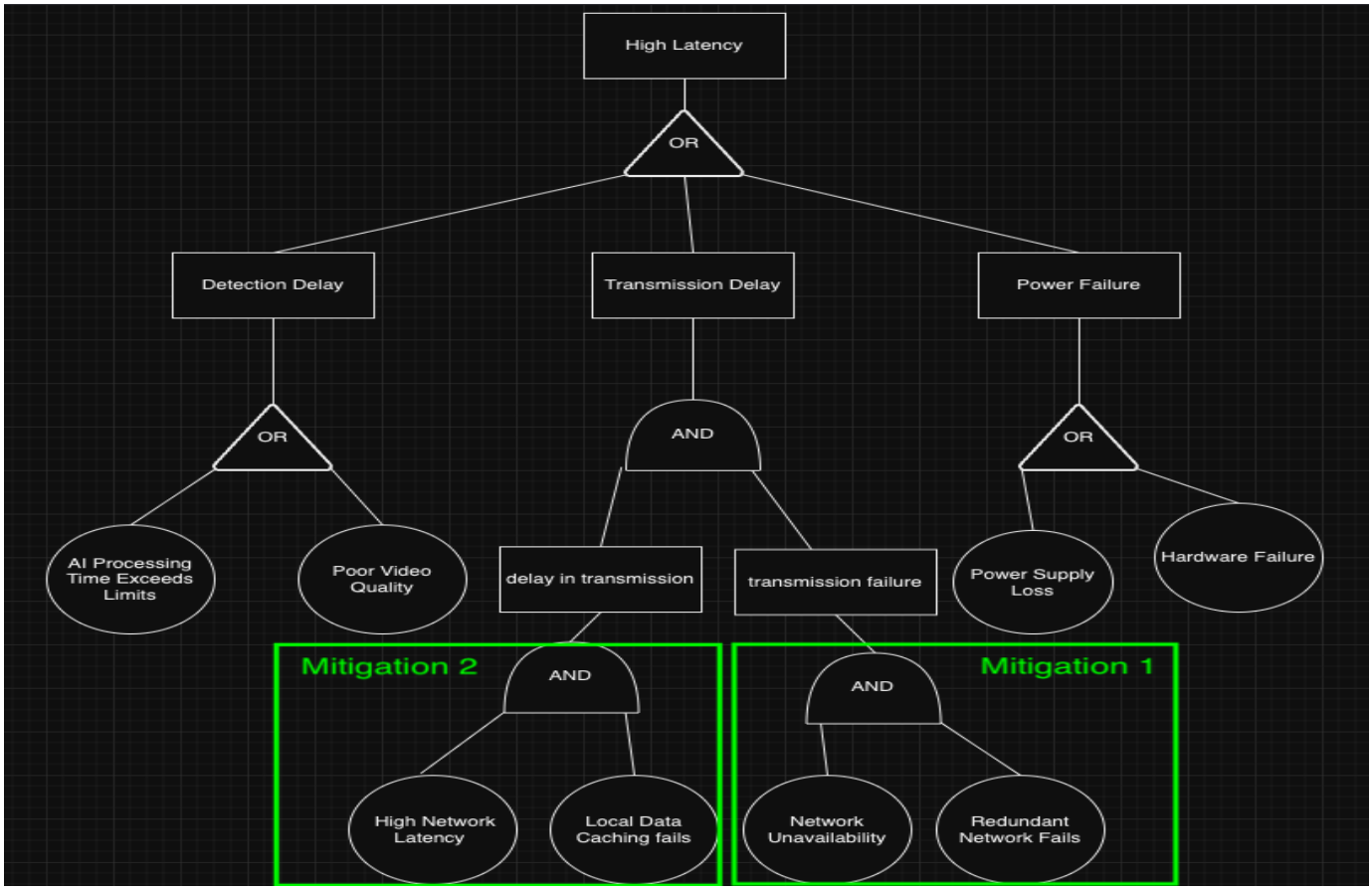
How it reduces the risk: This strategy directly mitigates the risk of **network unavailability** (B4) by providing fallback options. It ensures that if one network fails, the system will still be able to transmit detection data through another network.

Mitigation 2: Local Data Caching

Description: Implement a local storage mechanism that caches detection data if network connectivity is temporarily lost. The system stores the data for up to 24 hours and attempts to retransmit it every 30 minutes until a connection is re-established.

How it reduces the risk: This mitigation addresses both **network latency** (B3) and **network unavailability** (B4). If there is network latency or unavailability, the system will not lose data. Once connectivity is restored, the cached data will be transmitted, preventing a complete loss of detection reports.

Mitigation Diagram:



Conclusion

By implementing these mitigations, the system becomes more resilient to failures in network availability and latency. The use of **redundant network connections** ensures that detection data is not lost due to single points of failure in the network. Similarly, **local data caching** guarantees that data is preserved during temporary network outages, further reducing the risk of violating the latency requirement. These system-level mitigations significantly decrease the likelihood of failures leading to delayed reporting, improving the overall reliability of the system.