Self-Driving Car System

FULL NAME: YUPENG WEN

STUDENT ID: s224212855

TEACHERS: Hourieh Khalajzadeh

DATE OF COMPLETION: 16/09/2024

WORD COUNT: 2525

Scenario

AutoDrive, a globally recognized leader in the automotive industry, is at the forefront of innovation in autonomous driving technology. In response to the growing demands for safer, more efficient, and environmentally-friendly transportation solutions, the company is developing a cutting-edge fully autonomous driving system (ADS) aimed at transforming the future of personal and commercial transportation.

With road safety being a critical issue, AutoDrive seeks to address the fact that human error is responsible for the vast majority of traffic accidents globally. The ADS aims to significantly reduce these incidents by eliminating common human mistakes such as distracted driving, speeding, and improper decision-making in high-pressure situations. Furthermore, AutoDrive's system is designed to alleviate the increasing congestion in urban areas, which not only causes significant delays but also contributes to environmental pollution due to excessive fuel consumption.

By leveraging a combination of advanced sensors (LIDAR, cameras, and radar), artificial intelligence (AI), and machine learning, AutoDrive's ADS will enable vehicles to navigate complex road scenarios autonomously. This includes interactions with other vehicles, pedestrians, cyclists, and infrastructure in real-time. The system will operate efficiently in various driving environments such as congested city streets, open highways, suburban roads, and parking lots, offering drivers a seamless and convenient experience.

Problem and Vision Statement

Problem Statement

AutoDrive, a leading car manufacturer, is facing growing pressure to address critical issues related to road safety, traffic congestion, and environmental impact.

According to the research of Zhang, Y. et al. (2019), human error accounting for the vast majority of traffic accidents, the demand for safer and more efficient transportation systems is at an all-time high. In urban areas, congestion leads to significant delays, increased fuel consumption, and higher levels of pollution, while individuals with mobility challenges struggle to find reliable transportation options. Although autonomous driving technology holds the potential to address these challenges, existing solutions often lack the sophistication needed to handle complex road conditions, such as unpredictable traffic patterns and adverse weather. This situation highlights the need for a fully autonomous driving system that can provide safe, efficient, and environmentally-friendly transportation across diverse environments, ensuring accessibility and convenience for all users.

Vision statement

For urban commuters, delivery services, and individuals with mobility challenges who seek a safer, more efficient, and convenient transportation solution, AutoDrive's fully autonomous driving system offers real-time navigation and control in diverse driving environments, from city streets to highways. Unlike other autonomous systems, AutoDrive leverages advanced AI, LIDAR, and radar technology to ensure optimal safety, adaptability, and environmental sustainability, providing users with a seamless and reliable driving experience.

Challenges of Standard Requirement Analysis Techniques

Self-driving systems are complex, dynamic, and require advanced capabilities that go beyond traditional software development. Standard requirement analysis techniques, such as interviews, use cases, and data flow diagrams, often focus on well-defined, static systems where the functional and non-functional requirements are relatively

clear and predictable. However, these techniques face several limitations when applied to self-driving systems:

Dynamic and Unpredictable Environments

Traditional techniques are often based on predefined scenarios and rules. Self-driving systems, however, must operate in unpredictable, real-world environments, which can change rapidly (e.g., traffic conditions, weather, human behavior). Standard requirement techniques do not capture the full range of dynamic behaviors required for safe and reliable operation. According to the study of Wilkins et.al in 2007, An autonomous vehicle should consider the overall environment and dynamically adjust its control mechanism to balance performance and safety.

Handling Uncertainty and Ambiguity

Self-driving systems deal with uncertainties such as unexpected obstacles, erratic behavior from other drivers, and varying traffic laws. Standard requirement techniques struggle to accommodate such ambiguity and tend to focus on clear, well-defined functional requirements.

Complex Interactions and Dependencies

Self-driving systems involve a high degree of interaction between sensors, decision-making algorithms, and control mechanisms. Base on the study of HoBbach, Phillip Maxim in 2019, these systems must process vast amounts of data in real-time and make split-second decisions. Standard techniques do not easily capture the complexity and interdependencies of such systems.

Emergent and Evolving Behaviors

In self-driving systems, behaviors emerge from interactions between components (e.g., sensor data, AI algorithms). These behaviors are difficult to predict in advance,

making traditional methods insufficient for capturing all potential scenarios and responses.

Alternative Approaches to Supplement Requirement Specification

To address the shortcomings of standard requirement techniques, alternative approaches can be used to supplement the requirement specification of self-driving systems. These approaches are more suited to capturing complex, dynamic, and evolving system requirements:

Model-Based Systems Engineering (MBSE)

According to the book of A. Wayne Wymore 1993, MBSE uses formal models (e.g., SysML, UML) to describe the structure, behavior, and requirements of the system. This modeling technique helps capture complex interactions and dependencies between components, making it ideal for self-driving systems.

Advantages: Provides a clear and structured way to visualize the system. Supports traceability from high-level requirements to system design and implementation. Helps ensure that all aspects of the system are covered and validated (A. Wayne Wymore 1993).

Limitations: Requires specialized expertise in modeling languages and tools. Time-consuming and resource-intensive to build and maintain comprehensive models. May not capture emergent behaviors in real-world environments (Zeigler et.al 2018).

Scenario-Based Analysis

According to Kazman et al. (1996), scenarios and use cases were broadened to cover a wide range of real-world situations that a self-driving system might encounter,

including pedestrians crossing, adverse weather conditions, and sudden road changes.

Advantages: Provides detailed context for how the system behaves in specific, real-world situations. Helps identify edge cases and unusual conditions that may not be covered by traditional analysis.

Limitations: It can be challenging to define every possible scenario, and some edge cases may still be missed. This method can lead to an overwhelming number of scenarios, making it difficult to manage all cases effectively.

Prototyping and Simulation

Building prototypes or using simulation environments to model how the self-driving system will behave in various conditions (e.g., urban vs. rural driving, clear vs. adverse weather).

Advantages: Allows for iterative testing and refinement of system behavior. Simulations can expose system weaknesses in handlini)g unexpected events, helping to refine requirements.

Limitations: Creating detailed, realistic simulations is expensive and resource-intensive. Prototypes may not perfectly reflect real-world scenarios, limiting their effectiveness in gathering complete requirements.

Proposed Techniques

Self-driving systems like AutoDrive face several critical risks that could hinder their performance, safety, and public acceptance. Key risks include:

Safety Risks: Misinterpreting road conditions or obstacles, particularly in adverse weather or low-light environments, poses significant dangers.

Technological Failures: Sensor malfunctions (LIDAR, radar, cameras) and software bugs can lead to system misjudgements, impacting safety.

Cybersecurity Threats: Vulnerability to hacking or unauthorized system control can lead to vehicle misuse or data breaches.

Ethical Dilemmas: In scenarios of unavoidable accidents, the system may face complex moral decisions that challenge its programming.
Regulatory Compliance: Self-driving systems must adhere to different regional laws, and non-compliance could lead to legal and operational issues.
Environmental Challenges: Navigating difficult conditions, such as extreme weather or congested urban areas, remains a technical hurdle.

Risk Identification and Classification

To systematically identify and classify these risks, methods like Failure Mode and Effects Analysis (FMEA) and Fault Tree Analysis (FTA) are used. Risks are identified through data analysis, incident reporting, and system testing. For example:

- Safety risks are identified by analysing failures in road recognition, while technological risks are tracked by system diagnostics of hardware (e.g., sensors) and software performance (Liu et.al 2013).
- Cybersecurity risks are pinpointed via penetration testing to uncover system vulnerabilities.

Risks are then classified based on severity, likelihood, and detectability:
Severity: How critical the risk's impact could be (e.g., accidents caused by sensor failure would be highly severe).
Likelihood: How often these risks are expected to occur, based on historical performance.
Detectability: How easily these risks can be detected before causing issues.

Root Causes of Identified Risks

Safety Risks: Often arise from sensor errors, faulty AI algorithms, or slow data processing, caused by hardware degradation or software bugs.
Technological Failures: Can stem from poor system integration, outdated algorithms, or communication breakdowns between system components.
Cybersecurity Threats: Are typically caused by weak encryption protocols, inadequate access control, or software vulnerabilities.

Ethical Dilemmas: Result from incomplete AI models unable to make complex moral decisions in crash scenarios.

Regulatory Risks: Stem from a failure to update software to comply with ever-evolving traffic laws.

Eliminating and Reducing Risks

In order to mitigate these risks, the actions can be used:

Safety Risks: Use redundant sensors and real-time diagnostics to verify data from multiple sources and detect failures early.

Technological Failures: Implement advanced AI models and ensure fail-safe modes that shift to manual control during critical malfunctions.

Cybersecurity: Enhance security by employing end-to-end encryption, frequent software patches, and threat detection systems.

Ethical Issues: Build ethical decision-making frameworks within AI models to ensure proper actions in unavoidable accident scenarios.

Regulatory Compliance: Regularly update software to adhere to changing traffic laws and region-specific regulations.

Translating Additional Requirement specifications

Safety Risks

Additional requirement specifications:

1. The system must include redundant sensors (LIDAR, radar, cameras) that cross-check data in real-time to detect inconsistencies in road and obstacle recognition.
2. Real-time diagnostics must be implemented to monitor sensor performance and immediately identify failures.

Technological Failures

Additional requirement specifications:

1. Advanced AI models must be implemented to improve the system's decision-making capabilities.
2. The system should be able to detect hardware degradation and predict sensor failures based on diagnostic data.

Cybersecurity Threats

Additional requirement specifications:

1. The system must employ end-to-end encryption for all communication channels, including data exchanges between the vehicle, external networks, and cloud-based services.
2. Access control protocols must be robust, using multi-factor authentication to prevent unauthorized access.

Ethical Dilemmas

Additional requirement specifications:

1. AI models must incorporate an ethical decision-making framework to handle crash scenarios.
2. Ethical scenarios should be tested extensively, and any system decisions must be explainable and justifiable based on predefined ethical criteria.

Regulatory Compliance

Additional requirement specifications:

1. The software must include an automatic update feature that adjusts its algorithms and functions to comply with changing traffic laws and region-specific regulations.
2. Regular audits and compliance checks should be built into the development cycle to ensure adherence to these legal requirements.

Requirements Specification

Requirement 1

Requirement: The system must maintain the vehicle within its designated lane at all times, ensuring smooth lane transitions when necessary.

Rationale: Lane-keeping is crucial for the safe operation of autonomous vehicles. By maintaining the vehicle within its lane, the system minimizes the risk of accidents caused by veering into adjacent lanes or off the road. Ensuring lane discipline also contributes to the flow of traffic and overall road safety. A failure to reliably maintain lane position could result in traffic violations, collisions, or other dangerous situations.

Requirement 2

Requirement: The system must detect obstacles and take appropriate action (e.g., stop, slow down, or maneuver around) to avoid collisions.
Rationale: Detecting and responding to obstacles is essential for the safety of passengers and other road users. Without this capability, the autonomous vehicle could collide with objects, pedestrians, or other vehicles, leading to accidents. Accurate obstacle detection will allow the system to take preventive action, thereby avoiding incidents and maintaining a high level of trust from users and regulators.

Requirement 3

Requirement: The system must autonomously plan and follow optimal navigation routes using real-time traffic data.

Rationale: Efficient route planning reduces travel time and fuel consumption, contributing to both user convenience and environmental sustainability. By

leveraging real-time data, the system can avoid traffic congestion, accidents, and road closures, ensuring that the user reaches their destination in the shortest possible time. Failure to optimize routes could result in inefficient travel, user frustration, and increased environmental impact.

Requirement 4

Requirement: The system must identify and avoid pedestrians in or near the vehicle's path to prevent accidents.

Rationale: Pedestrian safety is a critical concern for autonomous vehicles. By detecting pedestrians and responding accordingly, the system helps reduce the risk of accidents involving pedestrians, which can result in injury or death. Ensuring this capability will also contribute to compliance with legal and ethical standards for road safety, especially in urban environments.

Requirement 5

Requirement: The system must autonomously park the vehicle in available parking spots, including parallel parking.

Rationale: Parking is a key aspect of driving, and automating this task enhances user convenience while ensuring efficient use of space in busy urban areas. By autonomously handling parking, the system will eliminate the potential for human error during parking maneuvers, such as collisions or misjudging space. This also improves accessibility for users with limited mobility.

Requirement 6

Requirement: The system must adapt its driving behavior in response to changing weather conditions, such as rain, snow, or fog.

Rationale: Adverse weather conditions can significantly affect driving safety. By adjusting the vehicle's speed, braking, and lane-keeping behavior, the system will

minimize risks associated with reduced visibility or slippery roads. Failure to do so could lead to dangerous situations, such as hydroplaning or collisions, which would undermine the system's reliability and user trust.

Requirement 7

Requirement: The system must prioritize the minimization of harm in situations where a collision is unavoidable, based on predefined ethical guidelines.

Rationale: Ethical decision-making in unavoidable accidents is one of the most challenging aspects of autonomous vehicle design. By integrating ethical frameworks, the system will be able to make decisions that minimize overall harm to passengers, pedestrians, and other road users. This feature is essential to ensuring public trust and acceptance of autonomous vehicles, as well as for regulatory compliance.

Requirement 8

Requirement: The system must protect user data by adhering to relevant data protection laws, such as GDPR.

Rationale: Autonomous vehicles collect significant amounts of data, including user preferences, routes, and personal information. Ensuring the privacy and security of this data is essential for compliance with global regulations and for maintaining user trust. Data breaches or misuse could result in legal consequences and loss of customer confidence in the system.

Requirement 9

Requirement: The system must detect and respond to vehicle malfunctions or external accidents by bringing the vehicle to a safe stop.

Rationale: Detecting emergencies is critical for maintaining safety in autonomous vehicles. Whether due to internal system failures or external accidents, the system must be able to recognize danger and respond appropriately. Bringing the vehicle to

a safe stop will prevent further damage or harm and ensure passenger safety. Failure to do so could lead to catastrophic results, both for the vehicle's occupants and other road users.

Requirement 10

Requirement: The system must comply with local, national, and international regulations governing the operation of autonomous vehicles.

Rationale: Legal compliance is mandatory for the deployment of autonomous vehicles. Without adhering to traffic laws and regulations, the system cannot be legally deployed on public roads. This includes compliance with speed limits, signalling, and right-of-way rules. Regulatory violations could result in penalties, legal challenges, and delays in adoption.

Requirement 11

Requirement: The system must communicate with other autonomous vehicles to share real-time information about traffic, hazards, and road conditions.

Rationale: Vehicle-to-vehicle communication enhances safety and efficiency by allowing autonomous cars to share critical information about their surroundings. This collaboration can prevent accidents, reduce traffic congestion, and optimize route planning. A failure to implement this feature could result in missed opportunities for efficiency and increased risk of collisions or traffic delays.

Reference List

Hoßbach, P.M., 2019. Automatic derivation of dependency chains within systems for automated driving via ontology based scenario representations (Master's thesis, Technische Universität Darmstadt).

Kazman, R., Abowd, G., Bass, L. and Clements, P., 1996. Scenario-based analysis of software architecture. *IEEE software*, *13*(6), pp.47-55.

Liu, H.C., Liu, L. and Liu, N., 2013. Risk evaluation approaches in failure mode and effects analysis: A literature review. Expert systems with applications, 40(2), pp.828-838.
Wilkins, D.E., Myers, K.L., Lowrance, J.D. and Wesley, L.P., 1995. Planning and reacting in uncertain and dynamic environments. Journal of Experimental & Theoretical Artificial Intelligence, 7(1), pp.121-152. https://doi.org/10.1080/09528139508953802
Zeigler, B.P., Mittal, S. and Traore, M.K., 2018. MBSE with/out Simulation: State of the Art and Way Forward. *Systems*, *6*(4), p.40.
Wymore, A.W., 2018. Model-based systems engineering. CRC press.