SAFETY CRITICAL ADVANCED AUTOMOTIVE SYSTEMS (AEL ZG621)

Situational Learning

Name: Sidheswar Ghosh **BITS ID: 2023HT65255**

TABLE OF CONTENT:

Problem Statement: Brake By Wire (BBW)

The goal of this project is to implement a Brake by Wire (BBW) system in MATLAB Simulink to simulate its functionality and evaluate its performance. BBW is a modern braking system where mechanical linkages are replaced with Electronic Control Unit (ECU), providing precise braking force control and enhancing the overall safety and performance of vehicles. The implementation will model the entire BBW process, including sensor inputs, electronic control logic, actuators, and feedback loops, ensuring that the system meets safety standards such as ISO 26262 to ensure the BBW system meets the required Automotive Safety Integrity Levels(ASIL).

To evaluate the safety and reliability of a Brake By Wire (BBW) system will be using Hazard Analysis and Risk Assessment (HARA) Techniques, Failure Diagnostics through Fault Tree Analysis (FTA), and failure rate analysis through Failure in Time (FIT) analysis technique. The analysis will also involve calculating metrics like Single Point Fault Metric (SPFM) and Multi Point Fault Metric (MPFM).

Abstract

The Brake By Wire (BBW) system is an advanced technology that replaces conventional hydraulic braking systems. This is electronically controlled actuators, enabling precise, efficient, and responsive braking performance. The main aim of the functional safety and reliability evaluation of a BBW system as per ISO 26262 standards. The study involves performing Hazard Analysis and Risk Assessment (HARA) to identify potential hazards, evaluate their severity, occurrence, and controllability, and assign appropriate Automotive Safety Integrity Levels (ASIL). Furthermore, Fault Tree Analysis (FTA) is conducted to identify root causes of system failures, and hardware circuits are analyzed to compute failure rates using metrics such as Single Point Fault Metric (SPFM) and Multi Point Fault Metric (MPFM). The project also includes dependent failure analysis and applies tools like MATLAB Simulink for system modeling. The results aim to provide insights into designing a fault-tolerant BBW system that meets the required safety and performance standards.

Introduction

The Brake By Wire (BBW) system represents a significant shift from conventional hydraulic braking systems to an electronic braking system, where braking is controlled through electrical signals and actuators rather than mechanical or hydraulic linkages. While this technology offers significant advantages in terms of precision, modularity, and energy efficiency. Also introduces a set of potential hazards that shall be carefully addressed to ensure the safety and reliability of the system.

Hazard Severity

Severity class	Exposure class	Controllability class		
		C1	C2	C3
S1	E1	QM	QM	QM
	E2	QM	QM	QM
	E3	QM	QM	A
	E4	QM	A	B
S2	E1	QM	QM	QM
	E2	QM	QM	A
	E3	QM	A	B
	E4	A	B	C
S3	E1	QM	QM	A[a]
	E2	QM	A	B
	E3	A	B	C
	E4	B	C	D

Severity Classes

	Class			
	S0	S1	S2	S3
Description	No injuries	Light and moderate injuries	Severe and life-threatening injuries (survival probable)	Life-threatening injuries (survival uncertain), fatal injuries

Class of probability of exposure regarding operation situation

	Class				
	E0	E1	E2	E3	E4
Description	Incredible	Very low probability	Low probability	Medium probability	High probability

Description of AIS stage with Severity Class mapping

Severity Class	AIS stage	Description of the AIS stages according IOS26262, part3, B.2.2
S0	AIS 0	no injuries;
S1	AIS 1	light injuries such as skin-deep wounds, muscle pains, whiplash, etc.;
S2	AIS 2	moderate injuries such as deep flesh wounds, concussion with up to 15 minutes of unconsciousness, uncomplicated long bone fractures,
S2	AIS 3	severe but not life-threatening injuries such as skull fractures without brain injury, spinal dislocations below the fourth cervical vertebra without
S3	AIS 4	severe injuries (life-threatening, survival probable) such as concussion with or without skull fractures with up to 12 hours of unconsciousness,
S3	AIS 5	critical injuries (life-threatening, survival uncertain) such as spinal fractures below the fourth cervical vertebra with damage to the spinal cord, intestinal
S3	AIS 6	extremely critical or fatal injuries such as fractures of the cervical vertebrae above the third cervical vertebra with damage to the spinal cord, extremely

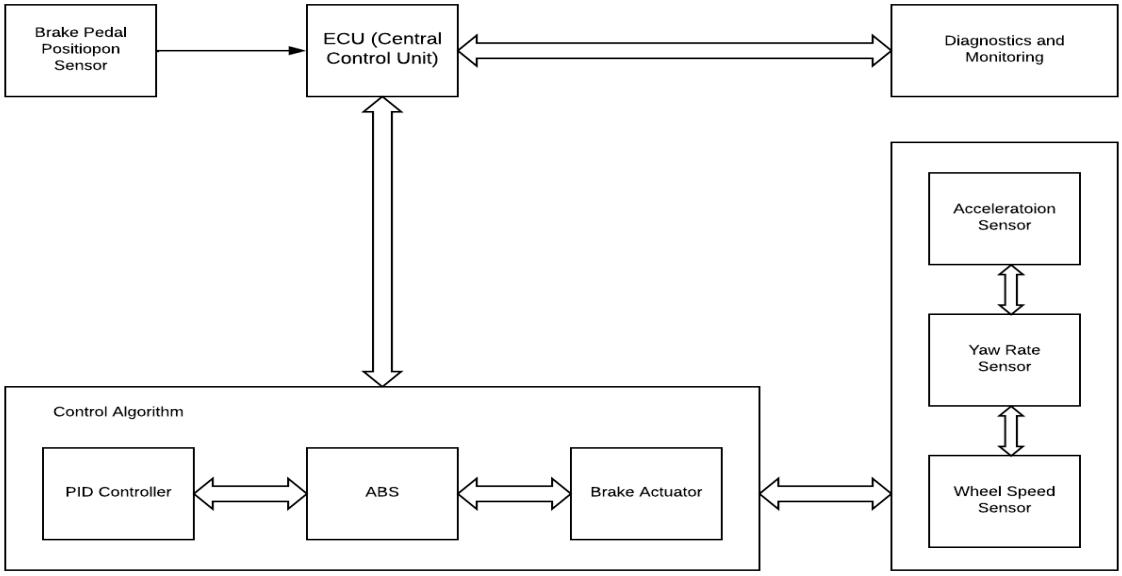
Classes of Controllability

	Class			
	C0	C1	C2	C3
Description	Controllable in general	Simply controllable	Normally controllable	Difficult to control or uncontrollable

Exposure

Exposure	Description	Remarks
E0	Incredibly low	Don't use this in general
E1	Very low probability	Probability <1%
E2	Low probability	0< Probability <1%
E3	Medium	1< Probability <10%
E4	High	>10%

Architecture



Brake-By-Wire (BBW) Architecture Explanation

The Brake-By-Wire (BBW) system replaces traditional hydraulic braking systems with an electronically controlled system. This architecture ensures better control, efficiency, and safety by leveraging sensors, actuators, and advanced control algorithms.

Key Components of BBW Architecture

1. **Brake Pedal Position Sensor**
   Function: Detects the driver's input on the brake pedal (force or position).
   Role in the System: Converts mechanical pedal motion into an electrical signal and sends it to the ECU.
   Purpose: Provides real-time information about the driver's braking intention.

2. **Electronic Control Unit (ECU)**
   Function: Central processing unit of the BBW system.
   Role in the System:
   - Processes input signals from the brake pedal sensor and feedback signals from other sensors (wheel speed, yaw rate).
   - Executes advanced control algorithms, such as PID and ABS logic.
   - Generates braking force commands for individual brake actuators.
   - Communicates with other systems via the CAN bus.

   Purpose: Ensures proper distribution of braking force while maintaining stability and control.

3. **Feedback Sensors**
   Provide critical information about vehicle dynamics to the ECU for precise braking control.
   a. **Wheel Speed Sensors:**
      - Measure the rotational speed of each wheel.
      - Detect wheel slippage or lockup conditions during braking.
      - Help the ABS module prevent wheel lockup by modulating brake force.
   b. **Yaw Rate Sensor:**
      - Measures the vehicle's rotational movement around its vertical axis.
      - Provides data for stability control, especially during cornering or emergency braking.
   c. **Acceleration Sensor:**
      - Measures longitudinal (forward/backward) and lateral (side-to-side) acceleration.
      - Helps optimize brake force distribution based on driving conditions.

4. **Control Algorithms**
   Advanced algorithms inside the ECU that compute braking commands.
   a. **PID Controller:**
      - Ensures smooth and accurate brake force application.
      - Adjusts braking response based on feedback from sensors to minimize overshoot, undershoot, or oscillation.
   b. **ABS (Anti-lock Braking System):**
      - Prevents wheels from locking during hard braking.
      - Modulates brake force to maintain traction and steerability.

5. **Brake Actuators**
   Function: Physically apply brake force to the wheels based on commands from the ECU.
   Types:
   - **Electro-Hydraulic Actuators:** Use hydraulic pressure controlled by an electric motor.
   - **Electromechanical Actuators:** Use electric motors to directly apply braking force without hydraulics.

   Role in the System:
   - Execute precise braking force for each wheel.
   - Respond quickly to dynamic changes in braking requirements.

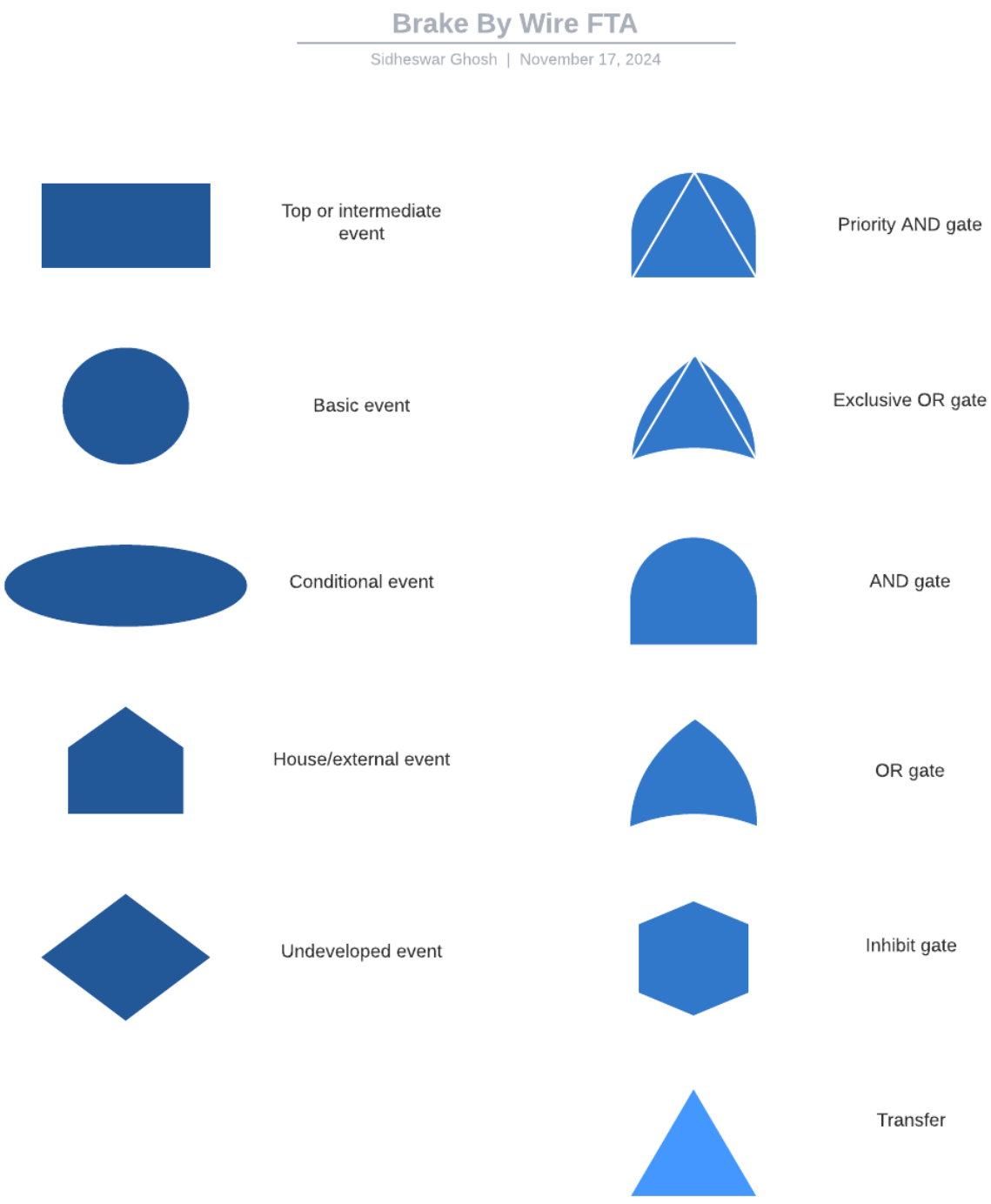
6. **Diagnostics and Monitoring Module**
   Function: Ensures the BBW system operates safely and reliably.
   Role in the System:
   - Continuously monitors the health of sensors, ECU, and actuators.
   - Detects faults or failures and triggers fail-safe mechanisms if necessary.
   - Logs errors and provides feedback to the driver or maintenance team.

7. **CAN Bus (Controller Area Network)**
   Function: Communication network for all BBW components.
   Role in the System:
   - Facilitates real-time data exchange between the ECU, sensors, and actuators.
   - Ensures synchronization of all subsystems in the braking process.

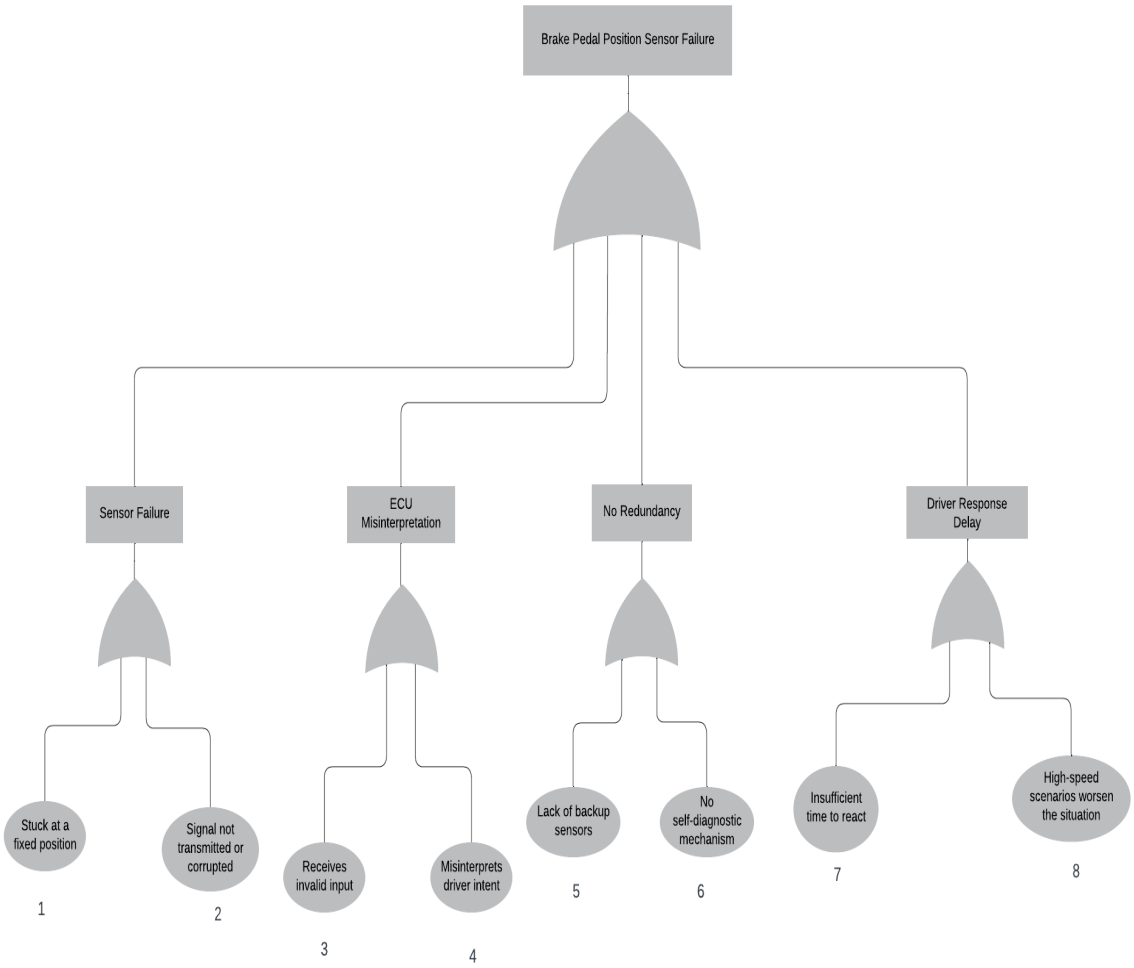
Hazard Analysis and Risk Assessment (HARA)

Item/ Function	Hazard ID	Hazard Description	Operating Mode	Guide word	Situation	Severity (S)	AIS Score	Justification	Exposure (E)	Justification	Probability	Controllability (C)	Justification	Reference	ASIL	Safety Goal	Safety Measure(s)
Item 1	HAZ_001	Brake Pedal Position Sensor	Idling	Stuck at	Misinterpret driver intent, causing unintended or no braking when transitioning from idling to driving	S2	2	Vehicle is stand still and gear is not engaged	E1	failure does not directly lead to collisions during idling but could cause issues when transitioning to driving mode		C2	The driver can easily control over the brake pedal in idling mode		QM	Ensure reliable and accurate brake pedal position sensing at all times	Implement Redundant sensor, self-diagnostics and notify the driver of sensor issues promptly.
Item 1	HAZ_002	Brake Pedal Position Sensor	Driving	Stuck at	The system interprets incorrect or no driver input due to the stuck sensor, causing unintended braking actions or no braking at all.	S3	4	This failure can lead to serious accidents, especially in emergency braking scenarios	E2	Failures in the pedal position sensor are possible during normal driving conditions		C3	Drivers may not react in time to apply manual braking if the sensor misinterprets their input		B	Ensure the sensor accurately reflects the driver's braking intent and mitigates failures	Implement Redundant sensor, self-diagnostics and notify the driver of sensor issues promptly.
Item 2	HAZ_003	Wheel Speed Sensors	Idling	Stuck at	In idling mode, the stuck speed sensor may not have immediate consequences but could lead to improper wheel speed data during transition to driving mode, impacting ABS or traction control	S2	2	Hazard has a low immediate impact during idling, It could affect vehicle stability during transition to motion	E2	Low-risk scenario where wheel speed sensor faults are less likely to cause hazardous effects		C1	Drivers can easily control the vehicle manually during idling, and the system has time to compensate before entering motion		QM	Ensure accurate and continuous wheel speed sensor data, even during idling, to prepare for driving transitions	Implement Redundant sensor, self-diagnostics and notify the driver of sensor issues promptly.
Item 2	HAZ_004	Wheel Speed Sensors	Driving	Stuck at	The hazard can lead to failures in systems like ABS and traction control, increasing the risk of skidding or losing stability during acceleration, braking, or cornering	S3	4	Loss of ABS or traction control functionality can result in a crash, especially during adverse conditions	E4	Potentially its very danger when ABS is deactivated specially in wet/slippery condition		C3	Drivers have limited ability to manually compensate for skidding or instability, particularly in emergencies or wet/slippery conditions		D	Ensure that wheel speed data is accurate, continuous, and reliable during driving	Implement Redundant sensor, Cross verification algorithm and notify the driver of sensor issues promptly.
Item 3	HAZ_005	Torque Sensors	Idling	Stuck at	The hazard can cause incorrect braking force interpretation, but since the vehicle is stationary, the risk of immediate harm is low	S0	0	Vehicle is stand still and gear is not engaged	E1	Faults in torque sensors during idling mode are uncommon due to limited operational stress		C0	Controllable in general		NA	None	None
Item 3	HAZ_006	Torque Sensors	Driving	Stuck at	Excessive torque may cause abrupt stops, leading to rear-end collisions, while insufficient torque may lead to longer stopping distances, particularly during emergencies	S3	4	Incorrect torque data can cause serious safety hazards, including collisions	E3	Failures in torque sensors can occur occasionally during normal or aggressive driving due to mechanical or electronic faults		C3	Drivers have limited ability to compensate for braking system malfunctions during dynamic driving conditions		C	Ensure accurate torque measurements during driving and mitigate the impact of sensor faults	Implement Redundant sensor, Real-time diagnostics and transition to fail-safe mode in case of failure
Item 4	HAZ_007	PID Governing	Idling	Gain too high	Excessive control outputs due to high gain may lead to unstable braking or unintended system behaviors	S1	1	Potential system instability may lead to minor safety risks during idling	E1	The hazard is unlikely to occur during idling due to limited system dynamics		C0	Easily controllable as vehicle is in idle condition		QM	Ensure stable and reliable PID parameters to prevent system instability	Implement real-time gain monitoring, self adaptive tuning algorithm and periodic plausibility check
Item 4	HAZ_008	PID Governing	Idling	Gain too low	Insufficient control due to low gain can delay braking responses, causing sluggish or inadequate system behavior	S0	0	Delays in system response pose minimal risks during idling, but may affect readiness for transitions	E1	The hazard is unlikely to occur during idling, given the limited system activity		C0	Drivers retain full control during idling and can intervene manually if needed		NA	None	None
Item 4	HAZ_009	PID Governing	Idling	Overshoot	Overshoot in braking control could cause the system to apply excessive braking force, creating instability or abrupt vehicle motion	S0	0	Gear is not engaged hence Under idling the car is stationery hence its in safe hands	E1	Overshoot is unlikely during idling due to limited dynamic conditions		C0	Drivers can easily manage braking during idling, making the hazard highly controllable		NA	None	None
Item 4	HAZ_010	PID Governing	Idling	Undershoot	Delayed braking force application due to undershoot could affect system readiness for transitions to active driving modes	S0	0	While delayed responses pose minimal risk during idling, they may reduce system readiness	E1	Undershoot is unlikely during idling due to limited dynamic requirements		C0	Easily controllable as vehicle is in idle condition		NA	None	None
Item 4	HAZ_011	PID Governing	Driving	Gain too high	High PID gain may lead to overcorrection of braking force, causing sudden braking or vehicle instability, particularly during high-speed driving or sharp maneuvers	S3	4	System instability or sudden braking can result in accidents, especially at higher speeds	E4	Overshoot in control gains is possible during dynamic driving, particularly in high-speed or adverse conditions.		C3	Drivers may struggle to control or mitigate abrupt braking or instability caused by high PID gain, especially during emergencies		D	Ensure PID control gains are stable and prevent excessive control outputs that could cause instability	Implement real-time gain monitoring, self adaptive tuning algorithm and periodic plausibility check
Item 4	HAZ_012	PID Governing	Driving	Gain too low	Insufficient braking force caused by low PID gain can lead to longer stopping distances, particularly during high-speed or emergency braking situations	S2	3	Delayed braking response can result in accidents, especially during emergencies or high-speed conditions	E3	Undershoot may occur during dynamic driving due to varying load or system disturbances.		C2	Drivers have limited ability to compensate for delayed braking force, especially in critical scenarios.		A	Ensure PID gain is sufficient to maintain responsive and effective braking force under all driving conditions	Implement real-time gain monitoring, self adaptive tuning algorithm and periodic plausibility check
Item 4	HAZ_013	PID Governing	Driving	Overshoot	Excessive braking caused by overshoot may lead to sudden deceleration, loss of control, or rear-end collisions, particularly in high-speed or emergency scenarios	S3	4	Abrupt or excessive control responses can result in serious accidents or vehicle instability	E4	Overshoot may occur during dynamic driving, especially under varying load or system conditions		C3	Drivers may struggle to control or compensate for aggressive braking, particularly at high speeds or in emergencies		D	Ensure PID control is stable and prevents excessive control outputs that could cause instability or accidents	Implement real-time gain monitoring, self adaptive tuning algorithm and periodic plausibility check
Item 4	HAZ_014	PID Governing	Driving	Undershoot	Insufficient braking force caused by low PID gain can result in longer stopping distances, posing risks in high-speed or emergency scenarios	S3	4	Inadequate braking response during dynamic driving conditions can result in collisions or loss of vehicle control	E3	Undershoot may occur during varying system demands, particularly in dynamic or high-speed conditions		C3	Drivers have limited ability to manually compensate for insufficient braking force in emergencies		C	Ensure PID control gain is sufficient to maintain responsive and effective braking force under all driving conditions	Implement real-time gain monitoring, self adaptive tuning algorithm and periodic plausibility check

Fault Tree Analysis (FTA)

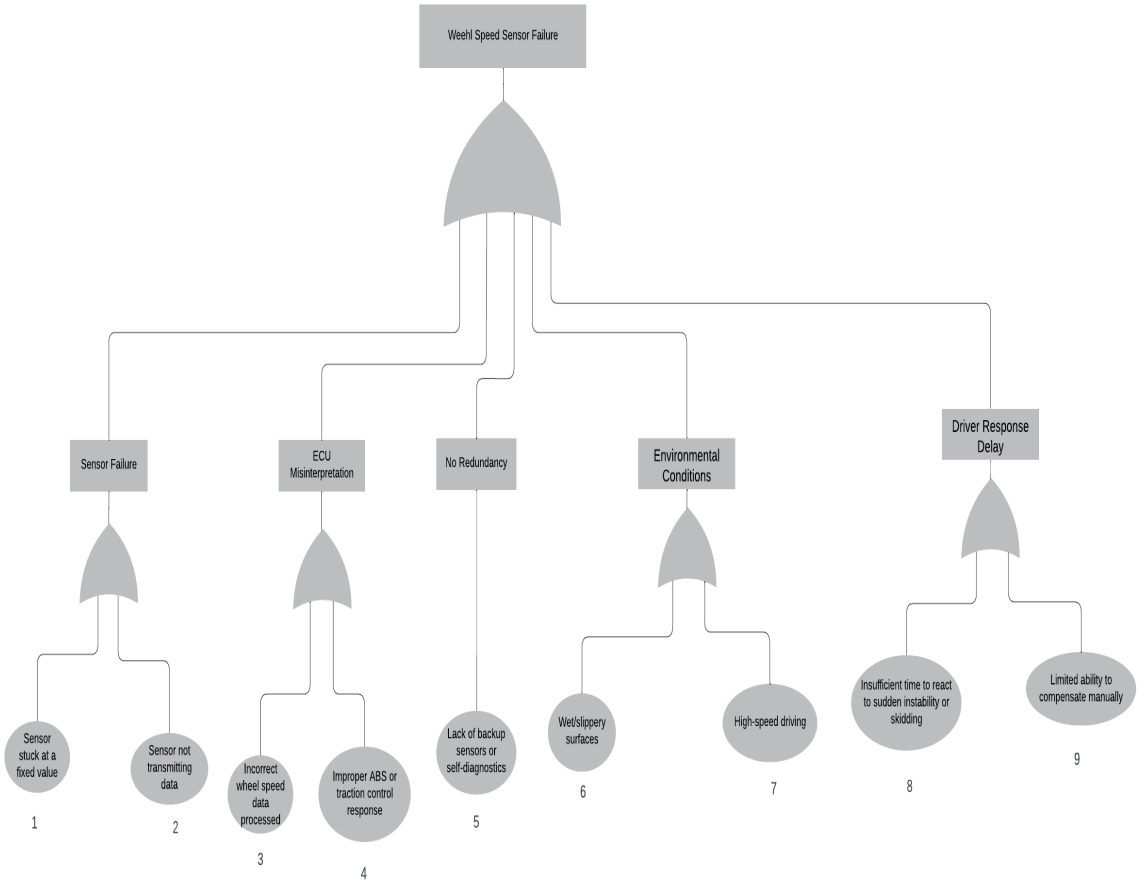


FTA: Brake Pedal Position Sensor Failure



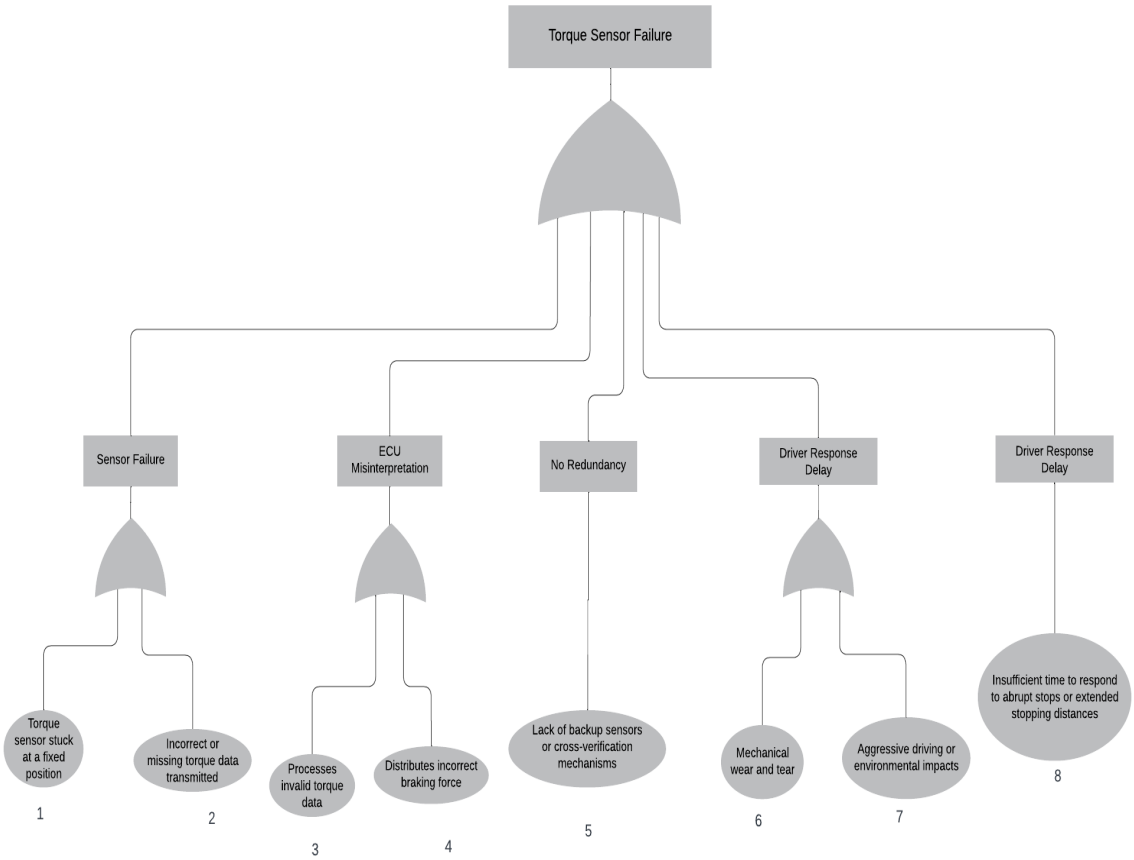
Reliabiligty Block Diagram: Brake Pedal Position Sensor Failure

FTA: Wheel Speed Sensor Failure

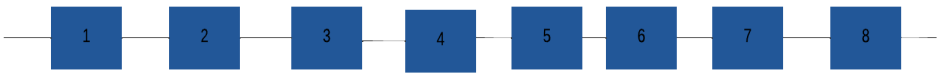


Reliabiligty Block Diagram: Wheel Speed Sensor Failure

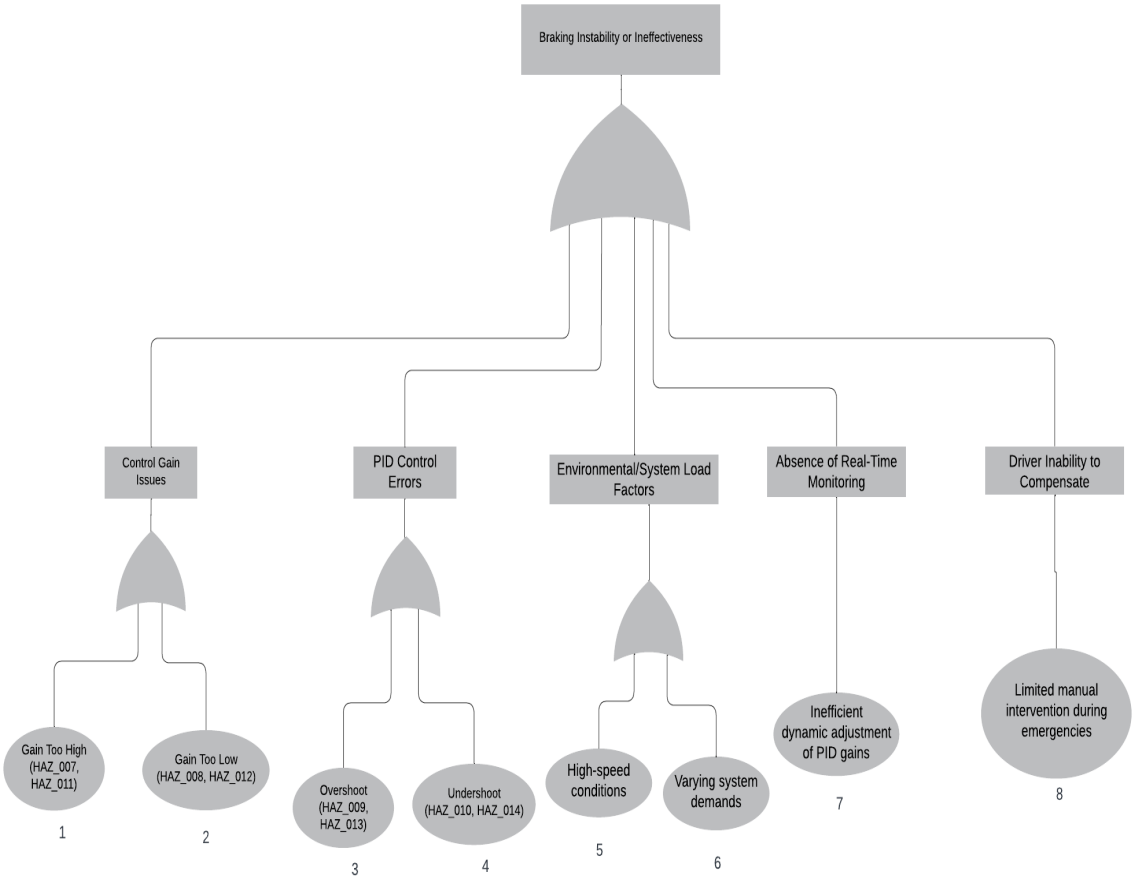
FTA: Torque Sensor Failure



Reliabiligty Block Diagram: Torque Sensor Failure



FTA: PID Malfunction (Braking Instability or Ineffectiveness)



Reliabiligty Block Diagram: PID Malfunction (Braking Instability or Ineffectiveness)

Dependent Failure Analysis (DFA)

The DFA evaluates the potential for multiple failures that are related or dependent on each other. In systems with redundancies, independent failures are usually assumed to be rare, but dependencies (e.g., common power supplies or communication paths) can lead to simultaneous failures.

In a **BBW system**, for example, dependent failures could arise if:

- **The power supply** to both the ECU and actuator is interrupted simultaneously, causing both components to fail together.
- **Communication failures** between the ECU and the brake actuators (if all signals travel through the same bus, a single point of failure on the communication bus could disable the entire braking system).

Dependent Failure Analysis Approach:

1. **Identify all dependent components**: For instance, multiple subsystems (e.g., sensors, actuators, controllers) depending on a single power supply or communication bus.
2. **Assess the likelihood of a dependent failure**: Evaluate how failures in one part of the system could affect other parts.
3. **Mitigation**: Introduce redundancies in critical areas (e.g., dual communication buses, multiple independent power sources).

Single Point Failure Metric (SPFM)

- **SPMF** measures the impact of a single point of failure in a system. In the context of a BBW system, an example of an SPM could be the **power supply**. If the power supply fails and there's no redundancy, the entire system fails.
- **Mitigation**: Implementing a secondary power source, such as a backup battery, reduces the likelihood of a single point of failure.

MPFM (Multiple Point of Failure Metric):

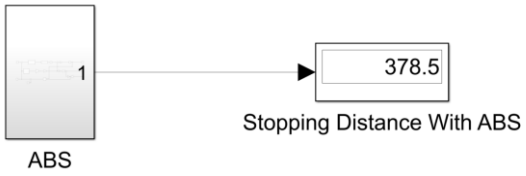
- **MPFM** evaluates the likelihood of multiple components failing simultaneously. This can be critical for systems with redundant components, where multiple failures must occur for the system to fail.
- In BBW, for example, if there are two brake actuators (one primary and one backup), both must fail for the braking system to completely fail.
- **Mitigation**: The failure probability can be reduced by adding more redundancy or by ensuring independent operation of redundant components.

Model and Code Link:

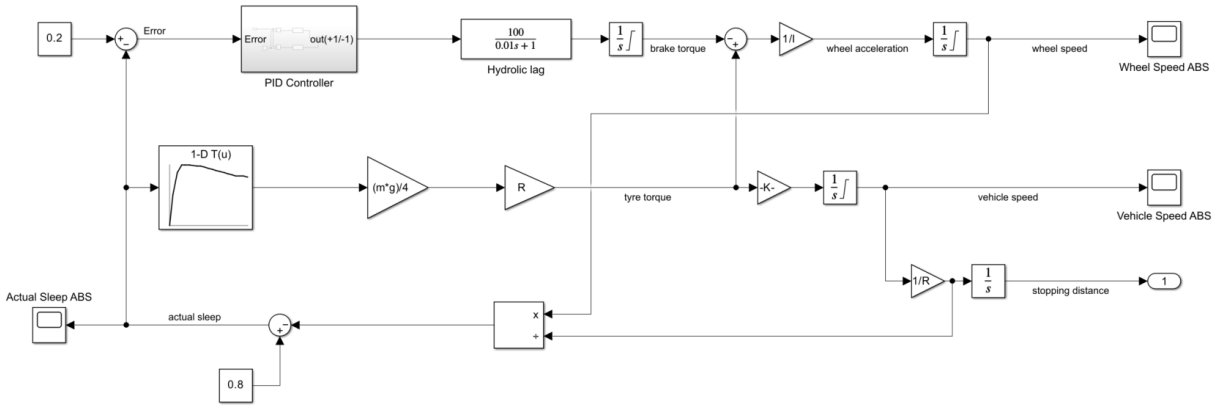
GitHub: https://github.com/sidheswar12/Brake_By_Wire

Model Screenshots

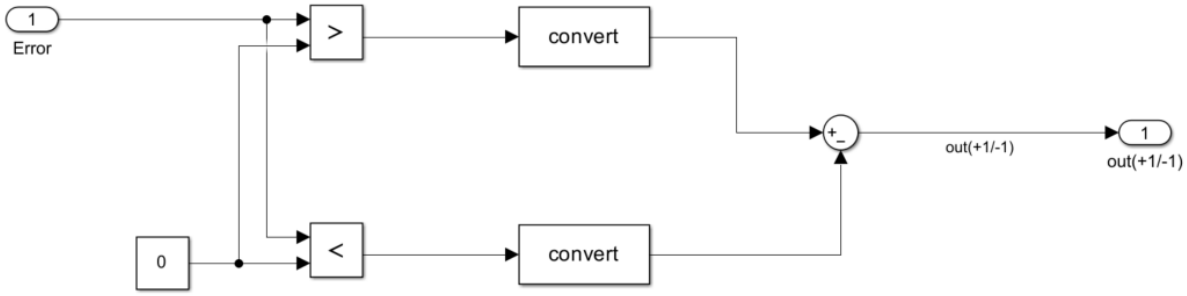
BBW Main Model displaying stopping distance with ABS



ABS block

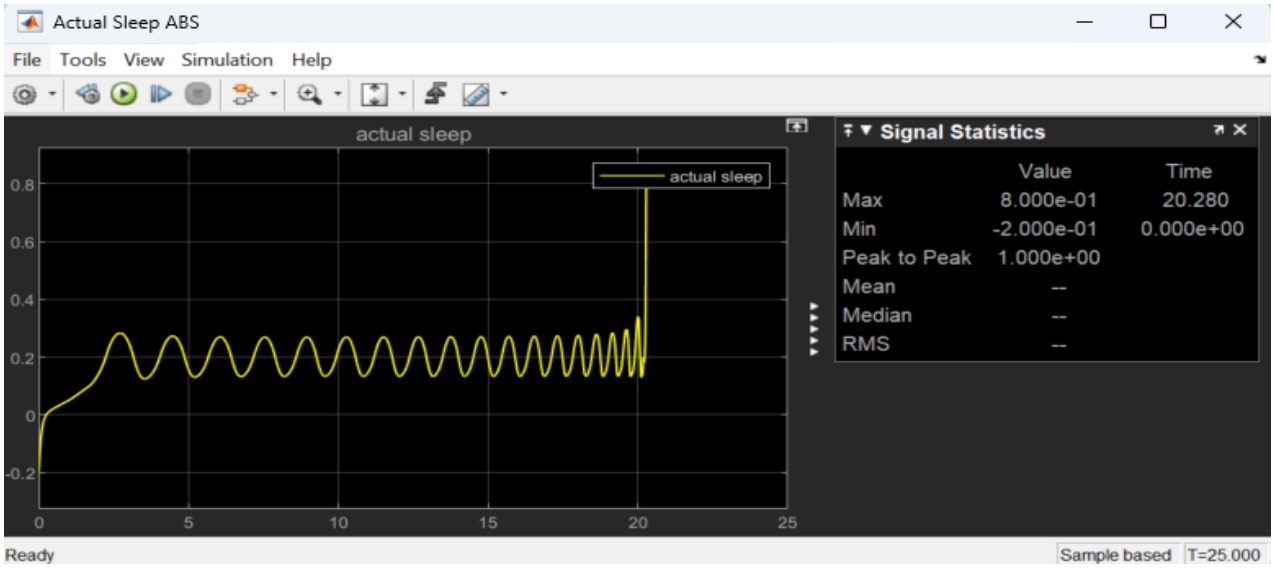


PID Controller

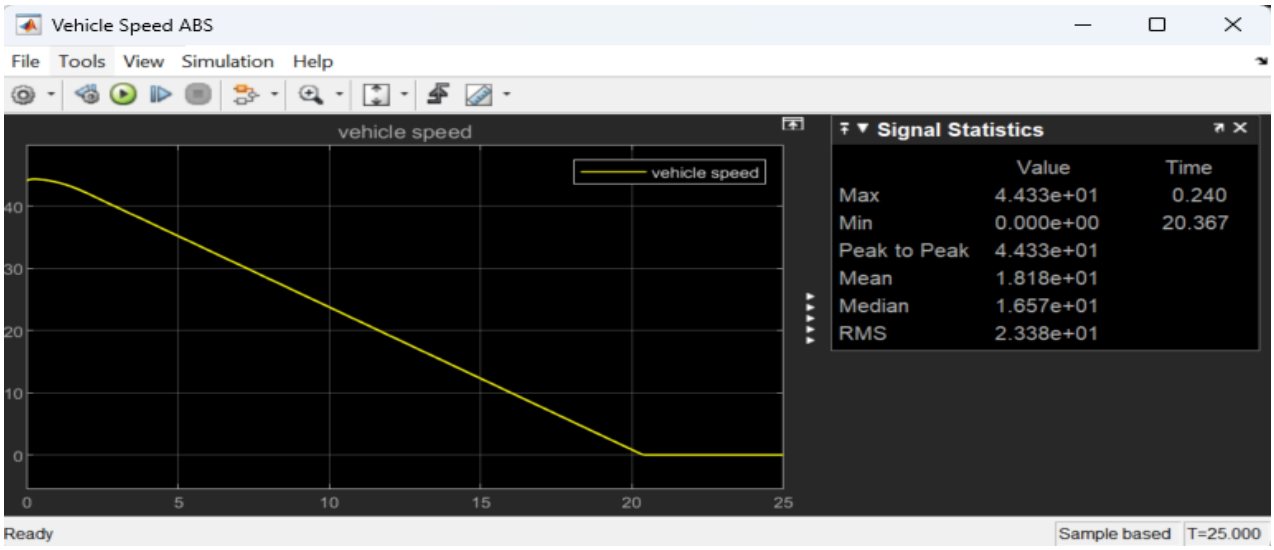


Simulation Result

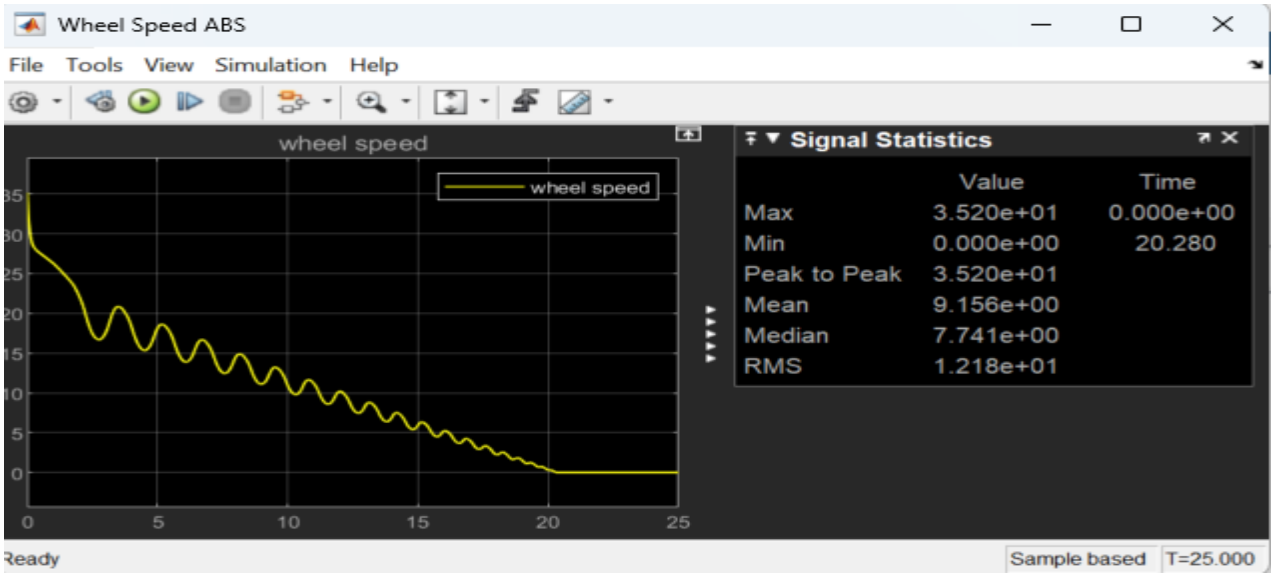
Sleep Statistics



Vehicle Speed Statistics



Wheel Speed Statistics



Tools

1. **MATLAB Simulink**: For modeling and simulating the Brake by Wire system, including sensors, actuators, and control logic.
2. **Hazard Analysis and Risk Assessment (**HARA): To identify probable hazards
3. **Fault Tree Analysis (FTA):** To identify potential causes of failure and assess the system's fault tolerance.
4. **Failure In Time (FIT) analysis**: To evaluate the reliability of hardware components.
5. **Safe Failure Fraction (SFF) Computation**: To assess the system's ability to handle faults safely.

Conclusion

The Brake by Wire (BBW) system implementation and analysis demonstrate the potential of electronic braking systems to enhance vehicle performance, safety, and reliability. The Hazard Analysis and Risk Assessment (HARA) and Fault Tree Analysis (FTA), critical safety hazards were identified and addressed, ensuring compliance with ISO 26262 standards for functional safety. Single Point Fault Metric (SPFM) and Multi Point Fault Metric (MPFM), were computed to evaluate the system's fault tolerance and diagnostic coverage. The results indicate that incorporating redundancy, robust diagnostics, and fault-tolerant design can effectively mitigate risks associated with single-point and multi-point failures.

***