SAFETY CRITICAL ADV AUTO SYS
AEL ZG621

Brake By Wire (BBW)
Hazard Analysis and Risk Assessment (HARA)

Sidheswar Ghosh: 2023HT65255

Item/ Function	Hazard ID	Hazard Description	Operating Mode	Guide word	Situation	Severity (S)	AIS Score	Justification	Exposure (E)	Justification	Probability	Controllability (C)	Justification	References	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