공학석사학위논문

자율주행 차량의 고장 진단 및 대응 제어 전략

A fault diagnosis and maneuver control algorithm for autonomous vehicle

2018년 8월

서울대학교 대학원

기계항공공학부

이 종 민

Abstract

A fault diagnosis and maneuver control algorithm for autonomous vehicle

LEE JONG MIN

School of Mechanical and Aerospace Engineering

The Graduate School

Seoul National University

This paper proposes the concept of autonomous vehicle failsafe system structure. It contains vehicle hardware and software structure design for autonomous vehicle failsafe system. Also, it handles the contents fail detection and emergency braking strategy in case there is no driver intervention in the fault situation. According to the 2017 ' AUTOMATED DRIVE SYSTEM 2.0 ' report released by the National Highway Traffic Safety Commission (NHTSA), it states that deployment of the crash avoidance system is essential

to switch to a minimum hazardous condition in the event of a problem with the self-driving vehicle or the system cannot operate safely. Secondly, real-time monitoring of the normal operation of the self-driving system is required. Third, the monitoring of the autonomous driving system shall be such that the driver can regain adequate control of the vehicle or that the system can individually return to a minimum hazardous condition. Fallback strategies should also consider minimizing errors with driver awareness and decision making.

As mentioned above, establishing a failsafe system for autonomous driving is an essential element for autonomous driving. To achieve NHTSA stated standard, designed failsafe system. First, on the structural side, designed two actuators (PC and Autobox) to monitor each state. Fail detection part enabled to find autonomous vehicle sensor errors. The failsafe control part proposes a sliding mode control based control strategy that enables an emergency braking control strategy in case the upper control fails. The control parts divide into longitudinal and lateral controls. The proposed algorithm suggest proper respond ways for autonomous vehicle safe driving only utilize vehicle chassis information, even without perception and decision part information. The sliding mode control based longitudinal control is suggested in this paper. The safe driving distance is calculated in real time and transmitted to the reference model. The reference model calculates reference acceleration, reference velocity, and

the reference station. The sliding mode control based longitudinal acceleration control algorithm tracking the reference values in an emergency situation. For lateral control, it is suggested that the desired path transmitted to a lateral controller which using dead reckoning method.

Keywords: Fail-Safe, Fail safe system, Autonomous driving, Fault detection, Dual system, Fault Reconstruction, Fault control, Failsafe control

Student Number: 2016-20709

List of Figures

Contents

Chapter 1

Introduction

1.1. Background and Motivation

Autonomous vehicle research aspect of failsafe and a fallback system is a very necessary and important study. Autonomous vehicles are composed of various sensors, computers, actuators and other types of equipment, and these equipment are configured to communicate together. In terms of fault diagnosis, each of them also needs real-time monitoring and also needs maneuver to be configured in the event of a failure. The algorithm proposed in this paper is an algorithm in the control part that makes an emergency stop when the fault is determined by fault diagnosis system when there is no driver intervention. The control classification was divided into two control categories, longitudinal control, and lateral control. Even if an error occurs that vehicle does not receive normal data from the upper controller that designed to recognition and

Fig.1.1.1 Waymo redundant safety-critical system

judgment components of the autonomous driving system, the proposed algorithm only uses the vehicle's chassis information to provide a way for autonomous vehicles to respond safely.

The vehicle hardware configuration is divided into upper controllers that responsible for recognition and judgment part and lower controller responsible for control of a vehicle. The lower controller consists of very robust hardware that allows for the safe longitudinal and lateral control in the event of errors in the upper controller. Therefore, during the autonomous driving phase proposed

by SAE International, level 4 suggests: the driving mode-specific performance by an automated driving system complete driving task, even if a human driver does not respond appropriately to a request to intervene. The hardware configuration was configured so that the autonomous vehicle could perform the failsafe system task without proper driver intervention.

Although there are not many prior studies on the fault diagnosis system of autonomous driving systems was completed, the development of the failure diagnosis system of non-automated vehicles has already been carried out in terms of the failsafe system. YH.J developed the vehicle sensor fault diagnosis and acceptance algorithm and conducted the residual and adaptive threshold fault diagnosis without additional hardware. [JEONG'15] KS. O conducted a

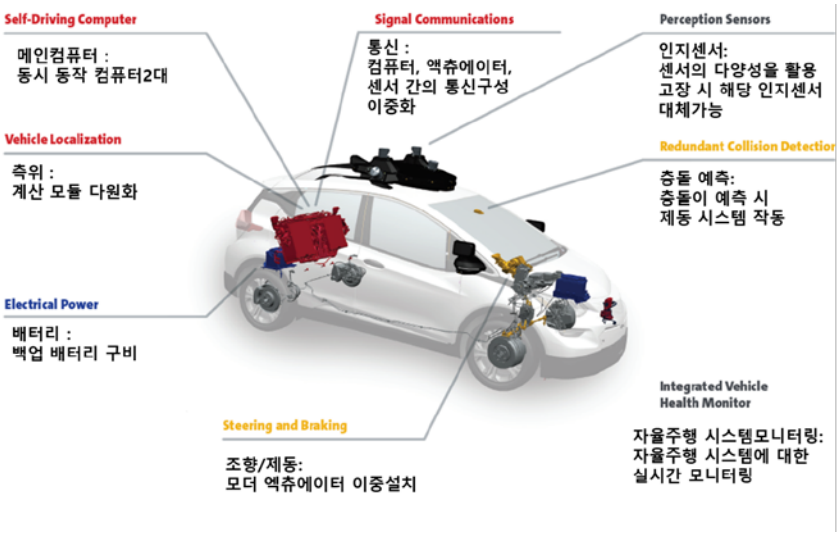


Fig.1.1.2 GM cruise safety system

study on the predictive fault diagnosis algorithm using sliding mode observers. [OH'17] Advanced research in failsafe and system construction methods was consulted by overseas automotive OEMs. Google Waymo self-driving vehicles have applied fallback systems. Fig.1.1.1 is Waymo safety-critical system description. Waymo vehicle's redundant system composed of backup computing, backup braking, backup steering, and a backup power system. [Waymo'17] Fig.1.1.2 is GM CRUISE autonomous vehicle safety system. Similar to Google Waymo, CRUISE has a backup computer, backup actuator, signal communication redundant and data accumulation system. [GM'18]

1.2. Thesis Outline

This dissertation is structured in the following manner. Chapter 1, introduced a fail-safe system of Waymo, GM cruise autonomous vehicle, which are the close to commercialization in the world market. Part of the classification of fault diagnosis for autonomous vehicles proposed in Chapter 2. The part of failsafe control is configured in Chapter 3. Chapter 3 covers the definition of defined failsafe control, methodology, and vehicle test results for failsafe control.

Chapter 2

Hardware-based fail detection classification

Fig.2.1 is hardware & module based classification of an autonomous vehicle fail detection and maneuver system. Hardware divide into Actuator, Sensor, Upper controller, CAN network and Lower controller. Actuator classifies as steering and throttle/brake. Sensor part composed of Lidar, Radar, and Vision (mono camera). The upper controller contains logic for perception and judgment of entire autonomous driving algorithms and calculates at regular intervals and transmits the calculated values to the lower-controller over real-time communication. CAN communication refers to the overall communication of the vehicle, including many sensors and actuators, vehicle inter communication, and uses a

method to conduct real-time monitoring of their values. The Lower Controller consists of algorithms that calculate the relative sub-controller of the overall configuration, the algorithm for path tracking, or the control input that enters longitudinal control in the event of failure.

Hardware	Module	FailSafe diagnosis algorithm 구비 정도 (○,△,X)	FailSafe diagnosis algorithm		Maneuver strategy
Actuator	Steering	O	- Steering health monitoring system (Yaw rate estimation / Adaptive threshold) [*]		Warning to Driver[*]
	Throttle/ Brake	O	- Ax estimate based throttle/brake health monitoring system [*]		
Sensor	Lidar	O	- Hardware failure	- Sliding mode observer based relative acceleration reconstruction & predictive diagnosis algorithm [**]	
	Radar	O	- Hardware failure(Blocked, over temperature, etc.) [*]		
	Vision	X	-		
Lower controller	Lower Controller	O	- Alive counting with upper controller [*]		
CAN	CAN Signal	O	- Labview VI(Virtual instrument) signal error check [*]		Warning to Driver[*] & SMC based Deceleration and stop[*]
	CAN Status	O	- CAN state values (Chassis CAN values) holding check [*]		
Upper Controller	Upper controller	O	- Alive counting with lower controller[*]		

* vehicle test complete

**simulation test complete

Fig.2.1. Architecture of the fault detection algorithm

2.1. Sensor fail detection

The hardware fault detection method of the sensor is shown as Fig.2.1.1. The manufacturer sends a corresponding fault signal from the sensor itself in the

4E0	CAN_TX_COMM_ERROR	Indication that the sensor has detected a communication error	False/True	bool	0: False 1: True	False	50ms	MMR
4E1	CAN_TX_XCVR_OPERATIONAL	Sensor Status Radiating 0 = not radiating 1 = radiating	0 to 1	n/a	1	0	50ms	MMR
4E1	CAN_TX_INTERNAL_ERROR	Sensor Status Failed 0 = not failed 1 = failed	0 to 1	n/a	1	0	50ms	MMR
4E1	CAN_TX_RANGE_PERF_ERROR	Sensor Status Blocked 0 = not blocked 1 = blocked	0 to 1	n/a	1	0	50ms	MMR

Fig.2.1.1 Delphi Radar error message

6.1 Error register 1

Bytes	LUX error	Description	Comment
Bit 0	E-SP	internal error	contact support
Bit 1	E-Motor_1	motor fault	contact support
Bit 2	E-Buffer_1	scan buffer transmitted incompletely	decrease scan resolution/frequency/range; contact support
Bit 3	E-Buffer_2	Scan buffer overflow	decrease scan resolution/frequency/range; contact support
Bit 4	E-Meas_1	APD voltage failed	contact support
Bit 5		reserved	
Bit 6		reserved	
Bit 7		reserved	
Bit8…9	E-Temp	Bit 9: APD Over Temperature Bit 8: APD Under Temperature Bit 8 and 9: APD Temperature Sensor defect	provide cooling provide heating contact support
Bit 10	E-Motor_2	motor fault	contact support
Bit 11	E-Motor_3	motor fault	contact support
Bit 12	E-Motor_4	motor fault	contact support
Bit 13	E-Motor_5	motor fault	contact support
Bit14…15		reserved	

6.2 Error register 2

Bytes	LUX error	Description	Comment
Bit 0	E-IF_internal_1	no scan data received.	contact support
Bit 1	E-IF_internal_2	internal communication error	contact support
Bit 2	E-IF_internal_3	incorrect scan data	contact support
Bit 3	E-Configuration_1	FPGA not configurable	contact support
Bit 4	E-Configuartion_2	incorrect configuration data	load correct configuration values
Bit 5	E-Configuration_3	configuration contains incorrect parameters	load correct configuration values
Bit 6	E-Timeout_1	data processing timeout	decrease scan resolution or scan frequency
Bit 7	E-Timeout_2	reset the computation of the environmental model	contact support
Bit8…15	reserved		

6.3 Warning register 1

Bytes	LUX warning	Description	Comment
Bit0	W-CMD	internal communication error	
Bit1	W-Range_1	internal warning	
Bit2	W-Range_2	internal warning	
Bit3	W-low_temperature	temperature too low	warning of insufficient temperature
Bit4	W-high_temperature	temperature too high	warning of exceeding temperature
Bit5	W-Motor_1	internal warning	
Bit6	W-Motor_2	internal warning	
Bit 7	W-Sync	synchronization error	check synchronization- and scan frequency
Bit7…15	RES 7…15	reserved	

6.4 Warning register 2

Bytes	LUX warning	Description	Comment
Bit0	W-IF_CAN	CAN Interface blocked	check CAN bus and CAN connection
Bit1	E-IF_ETH	Ethernet Interface blocked	check Ethernet connection
Bit2	W-CANdata	incorrect CAN message received	check CAN data
Bit3	W-IF_internal_1	incorrect scan data	contact support
Bit4	W-ETHdata	unknown or incomplete data	check Ethernet data
Bit5	W-Command	incorrect or forbidden command received	check command
Bit6	W-Flash	memory access failure	restart ibeo LUX, contact support
Bit7	W-Overflow_1	internal overflow	contact support
Bit8	W-EgoMotion	vehicle data update missing	check CAN vehicle data
Bit9	W-Mounting Position	incorrect mounting parameters	correct mounting position according to OM
Bit10	W-CalcFrequency	no object computation due to scan frequency.	set the scan frequency to 12.5 Hz to receive objects
Bit11…15	reserved		

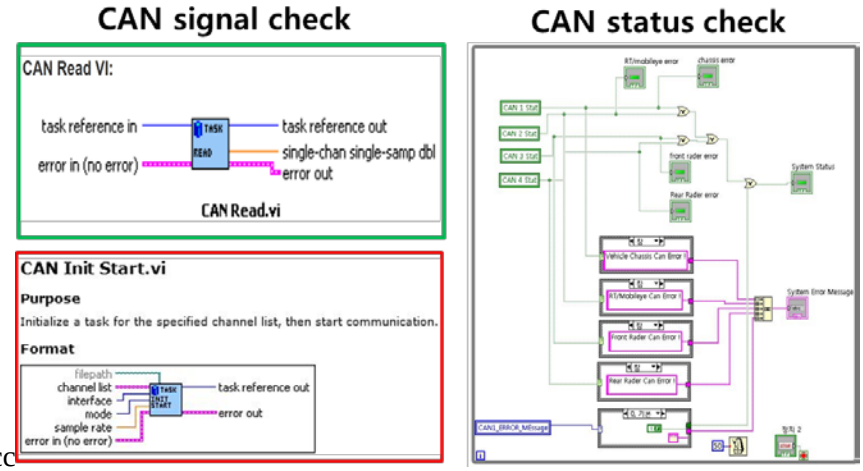
Fig.2.1.2 Lidar IBEO LUX error message

event of a fail. Delphi's radar has signals that can find many faults such as sensor communication error, sensor status failed, status blocked, and status over

temperature, etc. Communication settings allow users to read the appropriate information. The figure 2.1.2 is about Ibeo LUX Ridar error and warning messages. Error contents internal error, a motor error, temperature rise, data loss, internal communication error, incorrect scan data, etc. The warning signal that is sent to the user can receive error messages such as internal communication, temperature increase, etc.

2.2. Communication & controller fail detection

Inside the vehicle, communication is via the CAN bus (Controller Area Network) communication protocol is a standard communication specification designed to enable multiple devices to communicate with each other without a host computer. In order to detect errors in CAN signals, it is important to identify characteristics of CAN signals. Using the characteristics that the last value in the event of CAN failure is maintained by the host controller, utilized PC LabVIEW signal processing program, which is a higher control of an autonomous vehicle, can recognize an error about a CAN state that is judged to be a CAN error when the same value is received. The LabVIEW program itself can also detect errors on the CAN signal using a virtual instrument (VI) that detect for CAN errors. VI could find an error where the internal CAN state value is fixed. The upper controller refers to a PC and the lower controller (micro-autobox) that is responsible for control. Fault finding system that recognizes if one system fails while the PC to autobox system sends and receives data over CAN communication in real time.



CC

Fig.2.2.1. CAN signal check & CAN status check

Chapter 3

Failsafe control

3.1. Failsafe control description

In configuring the diagnostic system, to meet the requirements of SAE International level 4 as Fig.3.1.1, the control part that makes an emergency stop when there is no driver intervention after the failure determined by the algorithm. A Fig.3.1.2 is a concept diagram of the failsafe module that proposed in this paper. The control part is divided into the longitudinal and the lateral part. Offer a way for autonomous vehicles to respond safely, using the vehicle's chassis information only, even if there is no information on the upper control part, i.e., the recognition and judgment part. The system error situation defined in this paper means network communication is blocked. In this situation, the last value in CAN network is only useful information. A failsafe module

proposed in this paper utilized the unique phenomenon of system error and used that useful

SAE level	Name	Narrative Definition	Execution of Steering and Acceleration/ Deceleration	*Monitoring* of Driving Environment	Fallback Performance of *Dynamic Driving Task*	System Capability *(Driving Modes)*
***Human driver* monitors the driving environment**						
0	No Automation	the full-time performance by the *human driver* of all aspects of the *dynamic driving task*, even when enhanced by warning or intervention systems	Human driver	Human driver	Human driver	n/a
1	Driver Assistance	the *driving mode*-specific execution by a driver assistance system of either steering or acceleration/deceleration using information about the driving environment and with the expectation that the *human driver* perform all remaining aspects of the *dynamic driving task*	Human driver and system	Human driver	Human driver	Some driving modes
2	Partial Automation	the *driving mode*-specific execution by one or more driver assistance systems of both steering and acceleration/ deceleration using information about the driving environment and with the expectation that the *human driver* perform all remaining aspects of the *dynamic driving task*	**System**	Human driver	Human driver	Some driving modes
***Automated driving system* ("system") monitors the driving environment**						
3	Conditional Automation	the *driving mode*-specific performance by an *automated driving system* of all aspects of the dynamic driving task with the expectation that the *human driver* will respond appropriately to a *request to intervene*	System	**System**	Human driver	Some driving modes
4	High Automation	the *driving mode*-specific performance by an automated driving system of all aspects of the *dynamic driving task*, even if a *human driver* does not respond appropriately to a *request to intervene*	System	System	**System**	Some driving modes
5	Full Automation	the full-time performance by an *automated driving system* of all aspects of the *dynamic driving task* under all roadway and environmental conditions that can be managed by a *human driver*	System	System	System	**All driving modes**

Fig.3.1.1 SAE International standard J3016, Levels of vehicle automation

Information to predict and control. System error – supervisor part contains prediction contents. Prediction divides into 4 situations, front vehicle not exist, front vehicle exists, pedestrian intervention, surround vehicle intervention (next lane vehicle intervention). A Fig.3.1.3 is a description of supervisor part situation.

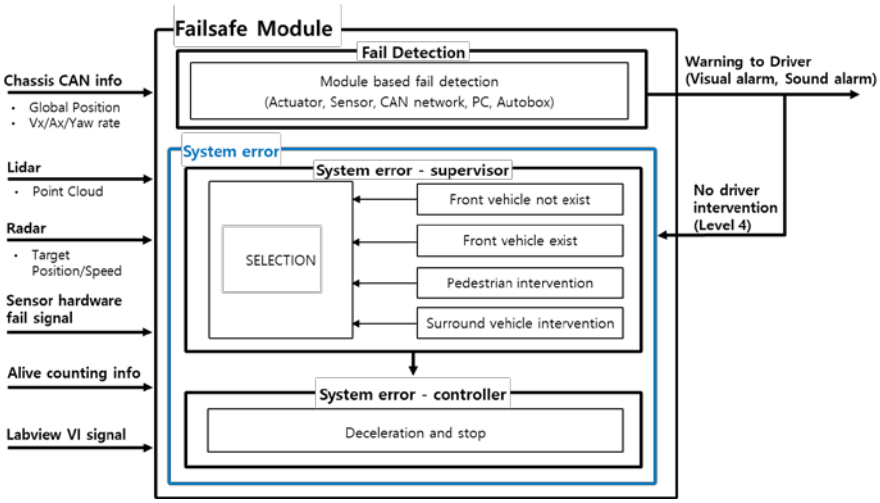


Fig.3.1.2 Failsafe module concept diagram

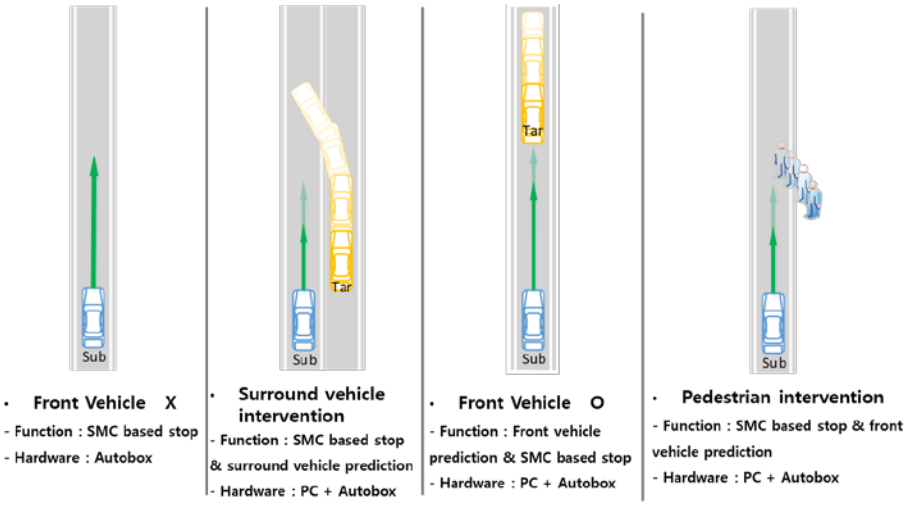


Fig.3.1.3 System error – supervisor part situation

After prediction, algorithm flow change to controller part. The method used for longitudinal control is to calculate the safe driving distance in real time and

transmit to reference deceleration model, and reference model calculates reference distance and reference velocity model for sliding mode control based deceleration and stop the algorithm. It is possible to make a stop within a safe distance through the above method. Lateral control consists of an algorithm that only uses the vehicle chassis information. This algorithm uses last information (desired path) of the upper controller to follow the path using DR to the lateral control algorithm.

The entire module was composed of the failure detection part that finds the failure of the total module, the failure detection part that carries out the classification for the failure, and the control model that is responsible for controlling deceleration with limited information.

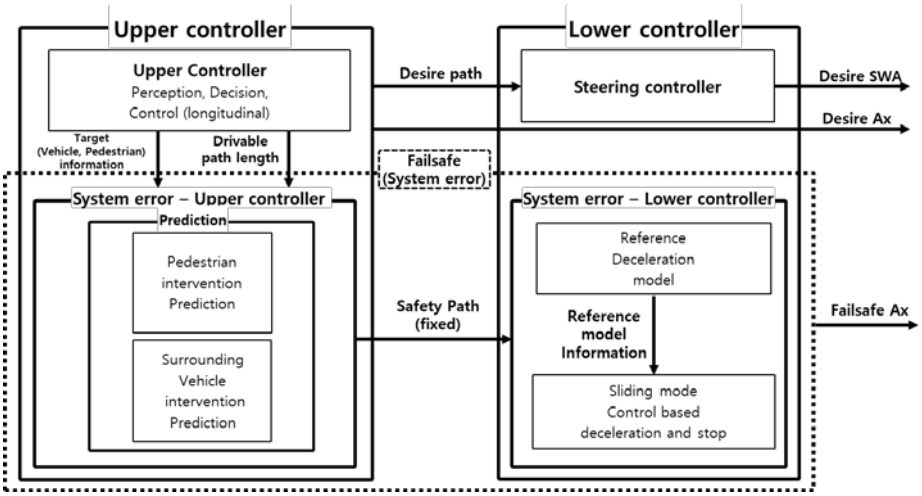


Fig.3.1.4 Failsafe hardware concept diagram

Fig.3.1.4 is hardware concept of the autonomous vehicle including the failsafe module. Considering autonomous vehicle hardware structure, the failsafe module was configured under normal circumstances, the algorithms of the perception, decision, and control algorithm operating in the upper controller. In order to prepare for a fault situation, the algorithms of the prediction in a fail-safe module using information from the upper controller calculate prediction algorithm in real-time. If an error is detected by the error-diagnosis module and no driver intervention is determined, the final information is used to predict and control. The last safety distance (in normal situation information) received from the upper controller is used in two ways. In the lateral direction, the dead

reckoning algorithm will be used to drive the safety path, and in the longitudinal direction, sliding mode control based deceleration and stop algorithm will be performed.

3.2. Methodology

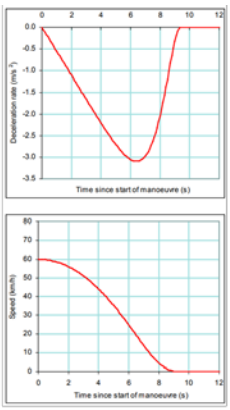


Fig. Reference model Ax & Vx

$$a(t) = ra_m\theta(1-\theta^m)^2$$

$$V(t) = V_0 + 3.6ra_m t_d\theta^2\left[\frac{1}{2} - \frac{2\theta^m}{(m+2)} + \frac{\theta^{2m}}{(2m+2)}\right]$$

$$S(t) = V_0 t/3.6 + ra_m t_d^2\theta^3 \cdot \left[\frac{1}{6} - \frac{2\theta^m}{(m+2)(m+3)} + \frac{\theta^{2m}}{(2m+2)(2m+3)}\right]$$

V_0 = initial speed(km/h)

a_m = maximum deceleration rate(m/s^2)

θ = time ratio($\theta = t/t_d$)

t_d = deceleration time

m = model calibration parameter

r = model parameter , $r = \frac{(1+2m)^{2+\frac{1}{m}}}{4m^2}$

Fig.3.2.1 Deceleration reference model

In this 3.2 chapter, describe System error – lower controller in Fig.3.1.3. More detail. System error – lower controller contains two parts, one is reference deceleration model another is SMC (sliding mode control) based deceleration and stop the algorithm.

The reference deceleration model [Rahmi'01] was determined by the general driver deceleration data which considering driver safety and ride comfort. The first-integrated velocity model and secondary integrated station model were used to construct an algorithm for stopping at safe distances. Pictures and formulas for longitudinal acceleration model, a longitudinal velocity model, and longitudinal distance model are illustrated in Fig.3.2.1 V_x is initial

velocity, a_m is maximum used deceleration, θ ($\theta = t/t_d$) is time ratio, t_d is deceleration time, m is a model variable parameter, r ($r = \frac{(1+2m)^{2+\frac{1}{m}}}{4m^2}$) is model parameter.

Define a time-varying sliding surface $S(t)$ by the scalar equation $s(\mathbf{x};t) = 0$, where $s(\mathbf{x};t) = e \cdot \left(\lambda + \frac{d}{dt}\right)^{n-1}$ and λ is a strictly positive constant. In this controller n =2 and he problem of keeping the scalar $s(t)$ at zero can be achieved by choosing proper control input u , the outside of $S(t)$, $\frac{1}{2}\frac{d}{dt}s(t)^2 \le -\eta\left|s(t)\right|$ and let equation $s(\mathbf{x};t) = 0$.

$$e(t) = S_{ref}(t) - S_{vehicle}(t) \tag{3.1}$$

$$s(t) = \dot{e}(t) + \lambda \cdot e(t) \tag{3.2}$$

$$V(s(t)) = \frac{1}{2}s(t)^2 \tag{3.3}$$

In (3.1) $e(t)$ is an error between the reference station and vehicle station. (3.3) is Lyapunov function. Differentiating the Lyapunov function

$$\dot{V}(s(t)) = s(t) \cdot \dot{s}(t) \tag{3.4}$$

For a stable system, the derivative of the Lyapunov function should be negative.

$$\dot{V}(s(t)) = s(t) \cdot \dot{s}(t) = -K \cdot |s(t)| < 0 \tag{3.5}$$

$$\therefore \ \dot{s}(t) = -K \cdot tan(s(t)) \tag{3.6}$$

$$\dot{s}(t) = \ddot{e}(t) + \lambda \cdot \dot{e}(t) = -K \cdot atan(s(t)) \tag{3.7}$$

$$u_{eq} = a_{x,ref} - \lambda \cdot \dot{e}(t) - K \cdot atan(s(t)) \tag{3.8}$$

design (3.2) sliding surface. Design sliding surface and calculate control input (3.8) tracking sliding surface. Control input u_{eq} is a longitudinal acceleration to vehicle SCC module.

3.3. Experimental vehicle configuration

The fail-safe module described above chapter is applied to the autonomous vehicle as Fig.3.3.1. As described in Fig.3.3.1 a number of algorithm and method have been applied to the actual autonomous vehicle. In Fig.3.3.2 has

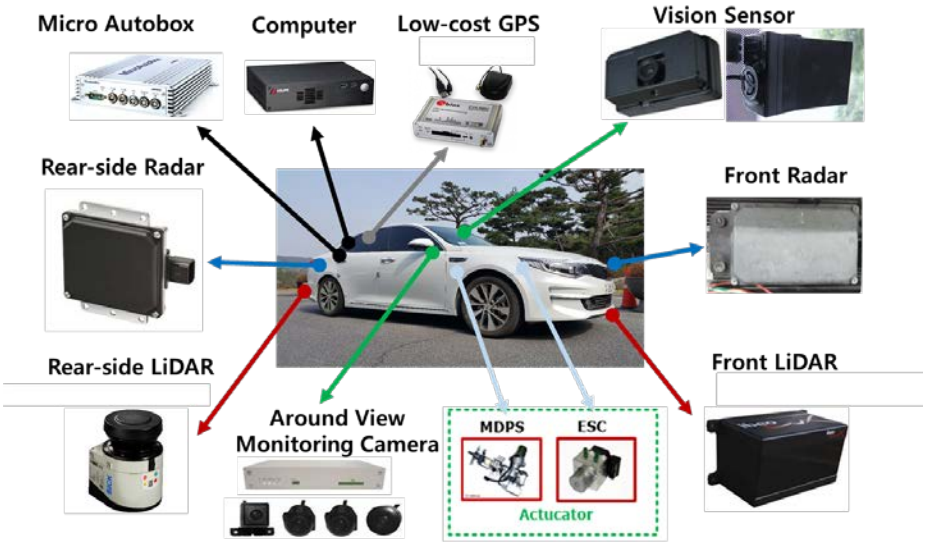


Fig.3.3.1. Autonomous vehicle hardware configuration

been constructed to allow the driver to recognize the warning situation in autonomous vehicles. In perception part, 1) Internal CAN communication error in the vehicle, 2) CAN value holding error (for multiple CAN channels), 3) sensor hardware error. These error warning system has been constructed to alert the driver.

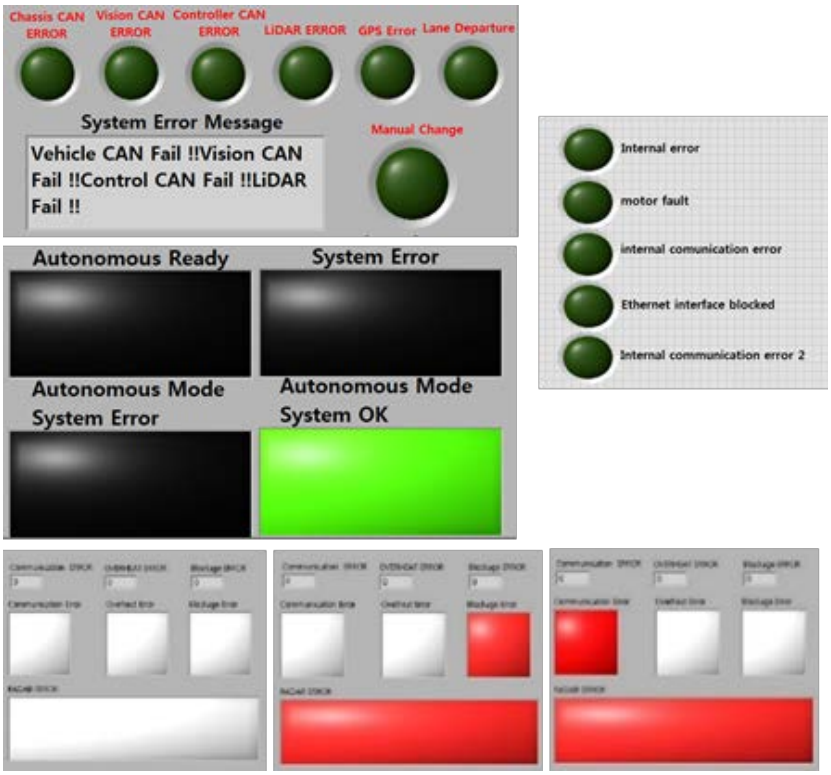


Fig.3.3.2 Visualized warning system

3.4. Vehicle SCC module description

SCC (Smart Cruise Control) module is the ADAS system of Hyundai Motor Company. Through the communication operation, longitudinal acceleration, which is the control input put into the SCC module. SCC module is a module that considers safety and ride comfort of drivers. If longitudinal acceleration or deceleration is inserted into the module, the actual input value and vehicle reacts has a time delay. To analyze the characteristics of the delay conducted SCC module delay test. The test method verifies the characteristics of the SCC module by inserting the deceleration value into the module as input during vehicle accelerates and cruising.

If the reference model referred to in chapter 3.2 is entered directly into the vehicle SCC module, it can be safely stopped within the specified distance of a simple configuration without the use of other control methods. Therefore, the output of the reference station and reference velocity utilized as control input. As a result, the problem of delay in SCC module extension time resulted in a value different from the value of the reference model to the output of the vehicle. The following chapter is the result of multiple experiments and test data showing that the SCC module has the nonlinear characteristic.

3.4.1. SCC module delay test result

As mentioned above, control inputs were applied in several situations to experiment with nonlinear characteristics of SCC module. The test scenario is set as follow. 1. 20km/h (minus one to minus five) deceleration to stop 2. 40km/h (minus one to minus three) deceleration to stop 3. 60km/h (minus one to minus three) deceleration to stop 4. Acceleration test

- **20km/h to 0km/h**

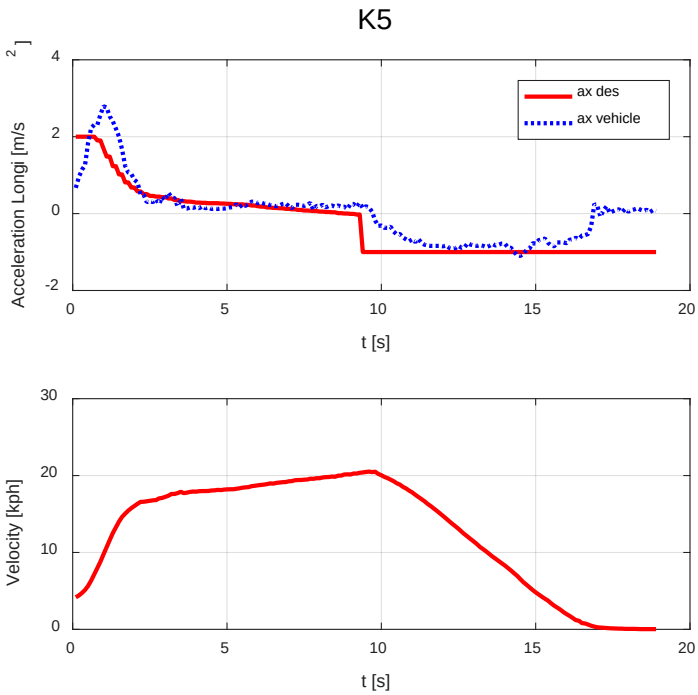


Fig.3.4.1.1 K5 deceleration test ($-1m/s^2$, 20kph)

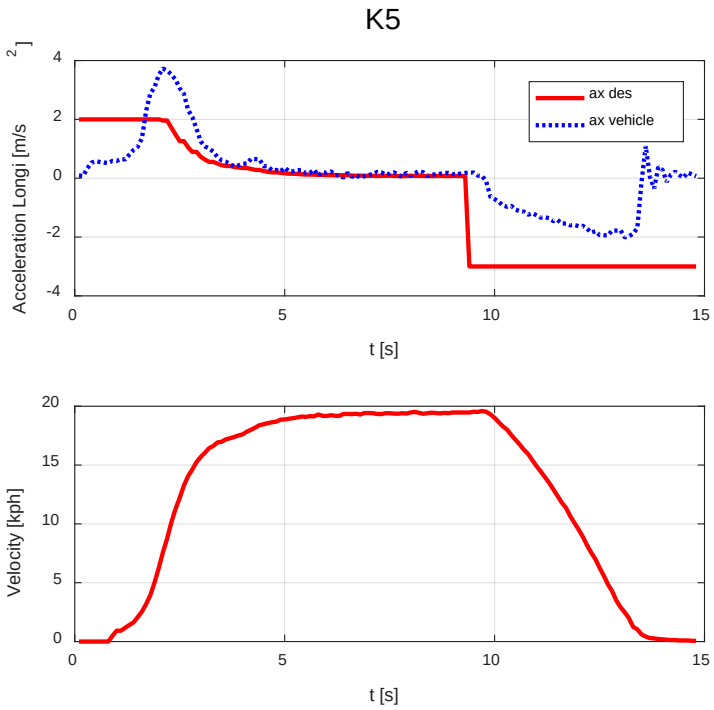


Fig.3.4.1.2 K5 deceleration test ($-3m/s^2$, 20kph)

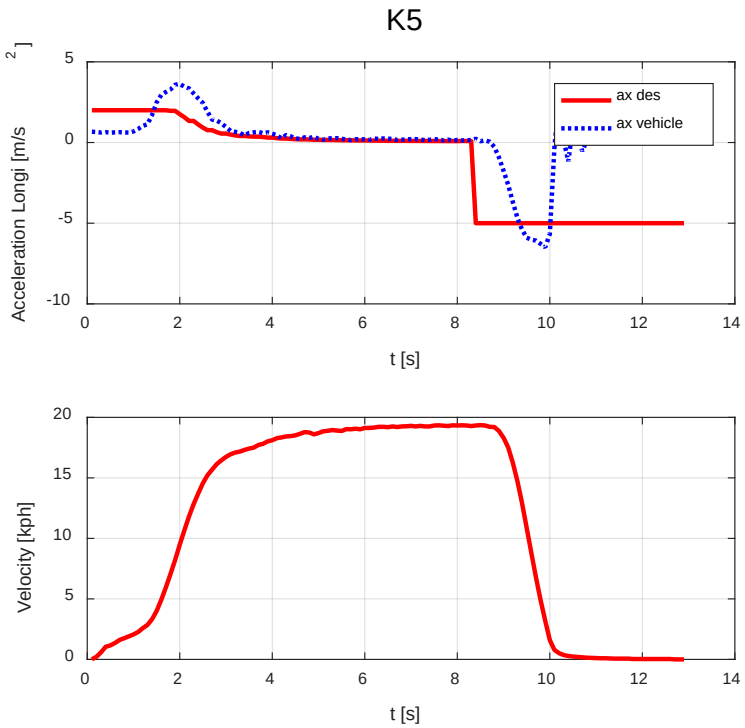


Fig.3.4.1.3 K5 deceleration test ($-5m/s^2$, 20kph)

- **40km/h to 0km/h**

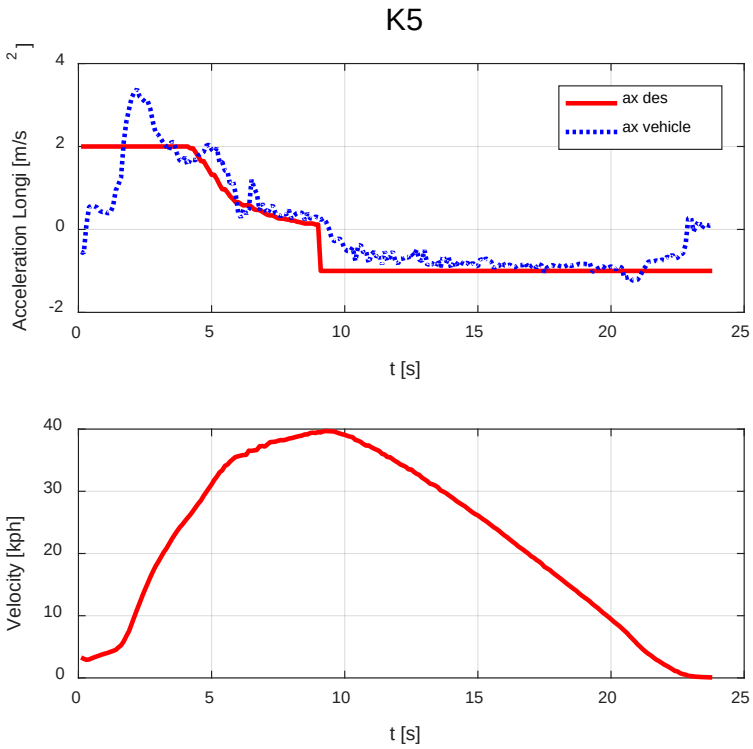


Fig.3.4.1.4 K5 deceleration test ($-1m/s^2$, 40kph)

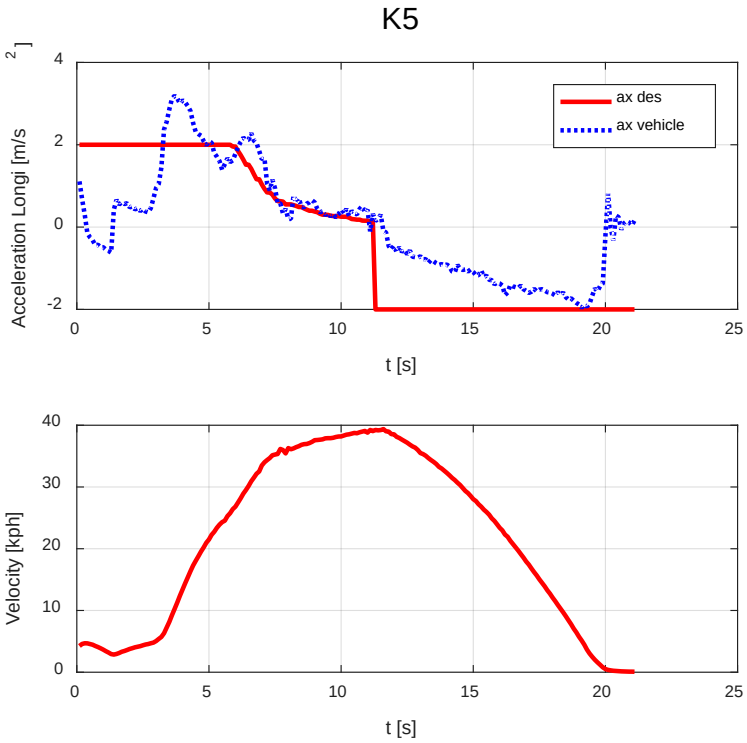


Fig.3.4.1.5 K5 deceleration test ($-2m/s^2$, 40kph)

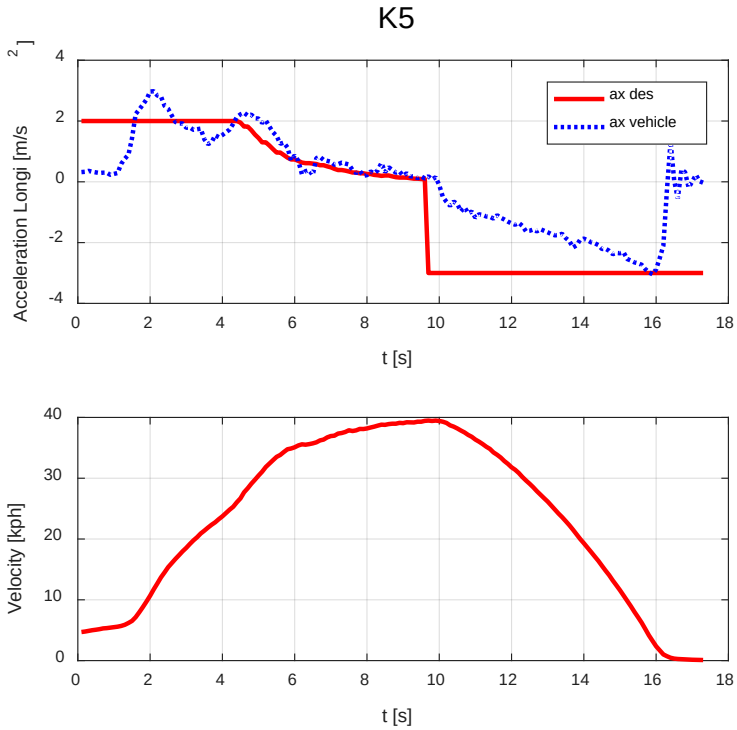


Fig.3.4.1.6 K5 deceleration test ($-3m/s^2$, 40kph)

- **60km/h to 0km/h**

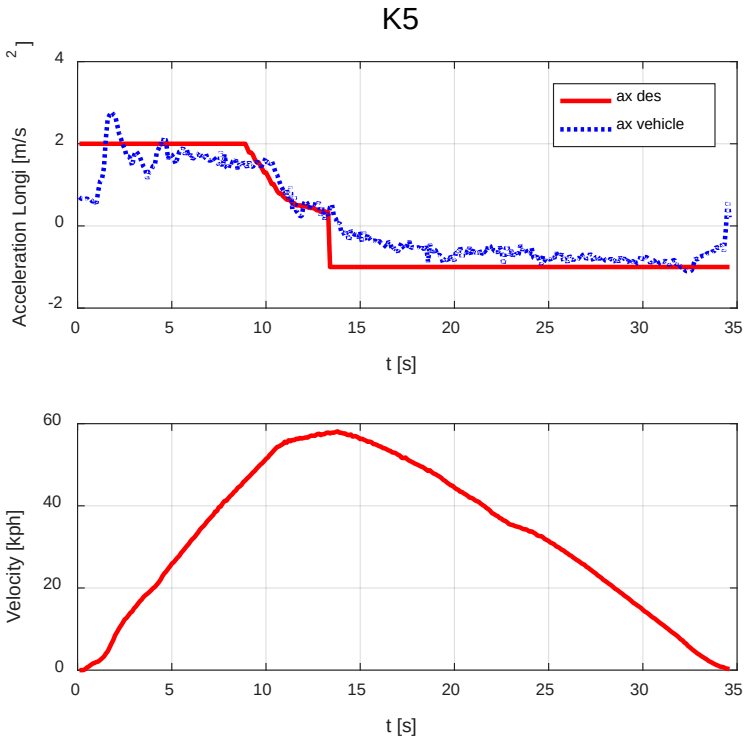


Fig.3.4.1.7 K5 deceleration test ($-1m/s^2$, 40kph)

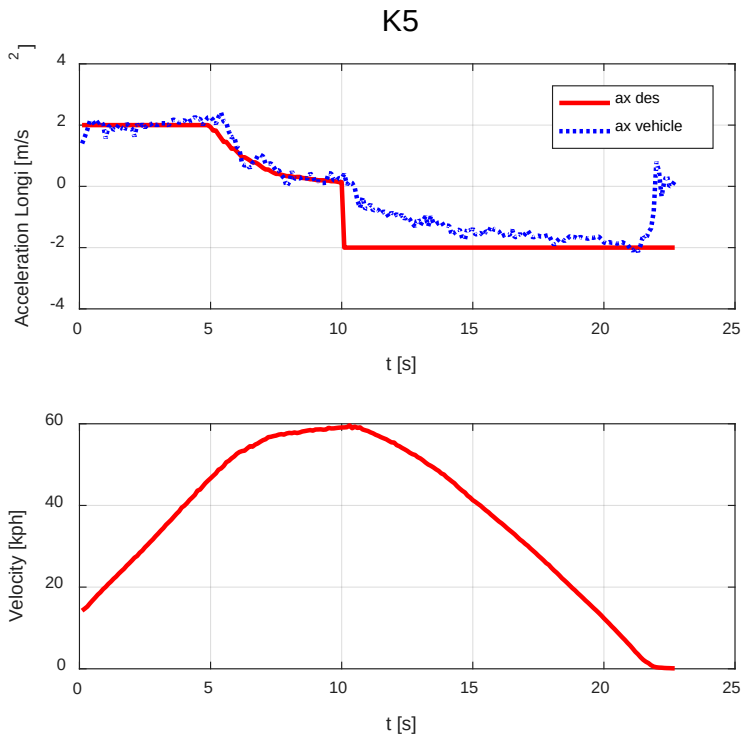


Fig.3.4.1.8 K5 deceleration test ($-2m/s^2$, 60kph)

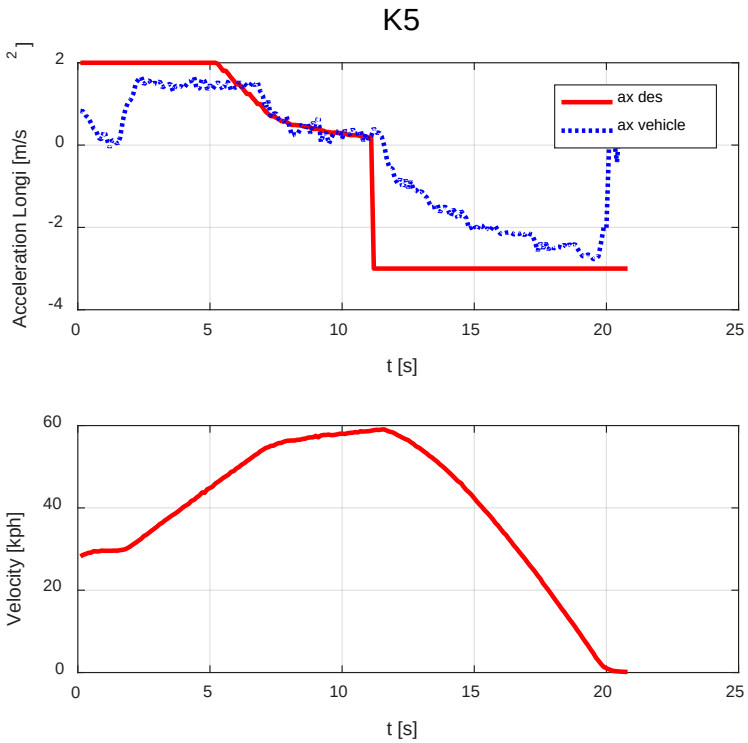


Fig.3.4.1.9 K5 deceleration test ($-3m/s^2$, 60kph)

In Fig.3.4.1.1 to Fig.3.4.1.9 is K5 vehicle deceleration test for check SCC module delay. Test content contains constant deceleration from $-1m/s^2$ to $-5m/s^2$ or from $-1m/s^2$ to $-3m/s^2$ when vehicle velocity close to 20 km/h, 40km/h and 60km/h. From test get a conclusion about SCC module delay as follow. First, module exists time delay about 0.1second to 0.5second. Second,

module deceleration control input is not severe so couldn’t reach command input as Fig.3.4.1.2

In conclusion, the SCC module exists time delay and nonlinear model characteristic.

3.5. SMC based deceleration vehicle test

For the failsafe control deceleration and stop vehicle test, the following methods were used to conduct the test. The whole vehicle test was conducted in autonomous mode, from beginning to end, and the experimental scenario was planned and conducted in low-speed area of 20 and 30 km/h. Fig.3.4.2.1 shows that the vehicle has been tested on autonomous mode from stop → accelerate → stops. The first figure in Fig.3.4.2.1 shows the vehicle accelerating to ACC mode up to 30 km/h and the sliding mode control based algorithm operating

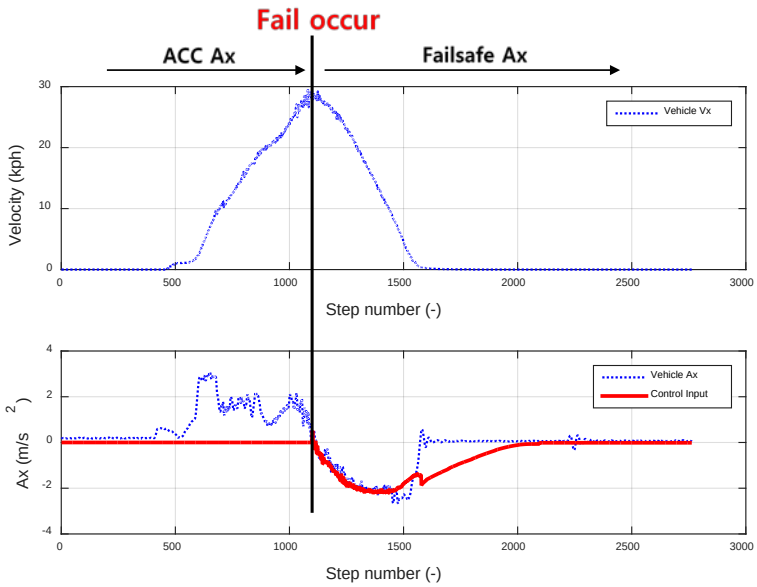


Fig.3.5.1 Vehicle test scenario – Acceleration to stop

when failure occurred. The second figure is a comparison of the longitudinal acceleration of the vehicle and the control input (longitudinal acceleration) into the vehicle SCC module.

3.6. Vehicle test result

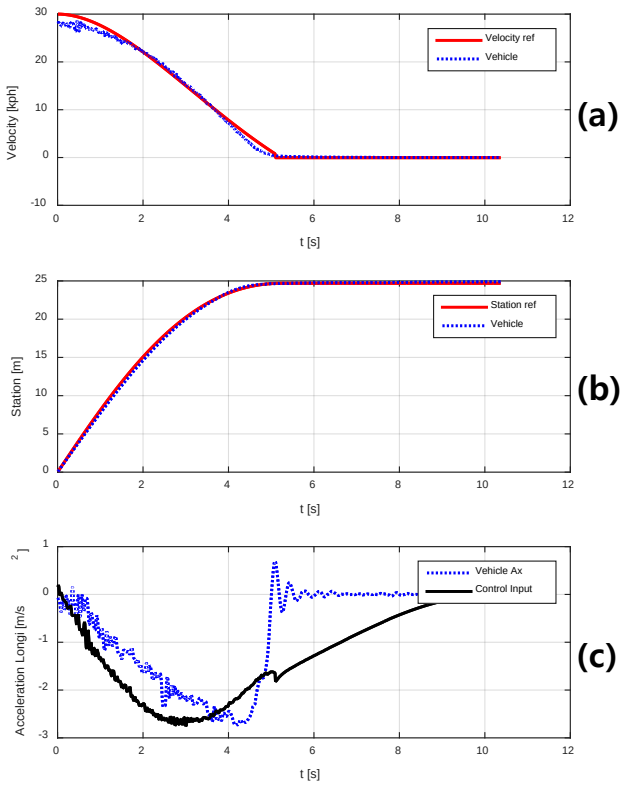


Fig.3.6.1. Vehicle test result

(a) Velocity (b) Station

(c) Control input & longitudinal acceleration

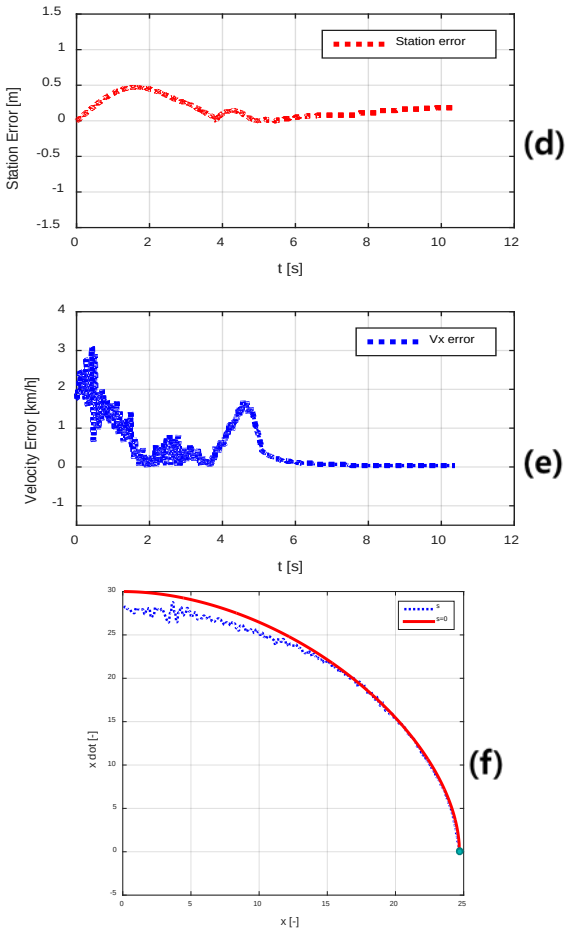


Fig.3.6.2. Vehicle test result

(d) Station error (e) Velocity error

(f) Sliding surface

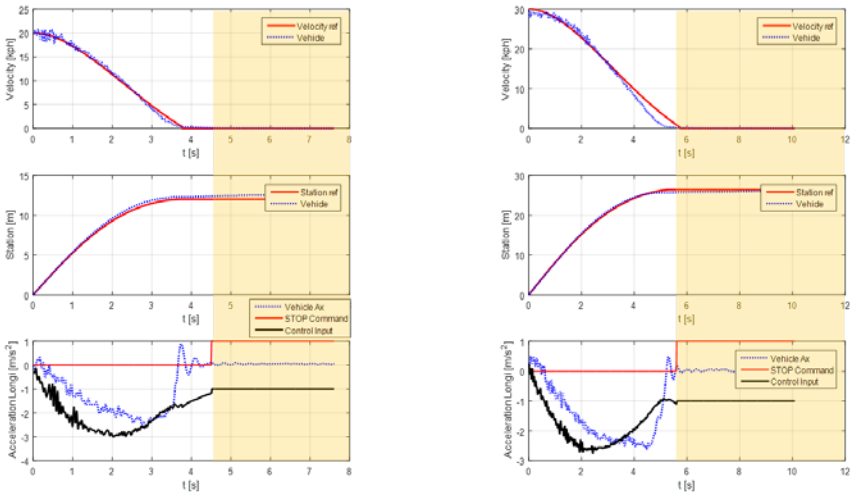


Fig.3.6.3. Sliding mode control deceleration vehicle test result

Fig.3.6.1 and Fig.3.6.2 are vehicle test near 30km/h. (a),(b),(c),(d),(e) and (f) are respectively the vehicle longitudinal velocity and reference model velocity profile, vehicle station and reference model station, vehicle acceleration and control input, station error, velocity error and sliding surface. The experiment result shows that the sliding surface follows well through the control input.

Fig.3.6.3 is 20 and 30 km/h situation vehicle test result. The yellow section addresses overload problems on SCC modules rather than algorithmic stops and consists of stopping with constant deceleration as the speed decreases for module safety.

Chapter 4

Conclusion

In this paper, in order to meet the requirements of autonomous driving phase proposed by SAE International, the hardware configuration was made to ensure that the driver could perform the autonomous vehicle task without driver proper intervention. In detection part, hardware (Actuator, Sensor, CAN signal, Upper controller, Lower controller) and module (Steering, Throttle/Brake, Lidar, Radar, GPS, CAN signal, CAN status, Chassis CAN) based failsafe diagnosis method and algorithm were proposed to detect fail situation. In decision and control part, when a failure of an autonomous vehicle is diagnosed and no driver intervention was detected, autonomous vehicle failsafe phase is a move to system error in Fig.3.1.4. In the phase of the system error (lower controller), reference station model and reference velocity model was calculated in real-time. Sliding mode controller based deceleration and stop algorithm tracking

designed sliding surface. The effectiveness of the proposed automated driving fails situation deceleration algorithm has been evaluated via test-data based simulations and vehicle tests. From the results, it has been shown that the proposed algorithm can provide the robust performance in low speed (20,30kph) condition.

Bibliography

[Waymo'17]Waymo, Safety Report: ON THE ROAD TO FULLY SELF-DRIVING, 10

[GM'18]GM, SELF-DRIVING SAFETY REPORT, 2018, 11

[JEONG'15]YH. JEONG and KJ LEE, 2015, "Virtual sensor based vehicle sensor fault tolerant algorithm," KSME, 1761-1766.

[OH'17]KS. OH, 2017, "Kinematic Model-based Predictive Fault Diagnosis Algorithm of Autonomous Vehicles using Sliding Mode Observer ", KSME, Vol41 No.10, 931-940.

[B. Kim 2014] Kim, B., & Yi, K.: Probabilistic and holistic prediction of vehicle states using sensor fusion for application to integrated vehicle safety systems. IEEE Transactions on Intelligent Transportation Systems, Vol. 15, No. 5, pp. 2178-2190, 2014

[B. Kim 2015] Kim, B., Yi, K., Yoo, H. J., Chong, H. J., & Ko, B.: An IMM/EKF approach for enhanced multitarget state estimation for application to integrated risk management system. IEEE Transactions on Vehicular Technology, Vol. 64, No. 3, pp. 876-889, 2015

[B. Kim 2015] Kim, B., Son, Y., & Yi, K.: Probabilistic threat assessment with environment description and rule-based multi-traffic prediction for integrated risk management system. In Intelligent Vehicles Symposium (IV), 2015 IEEE. IEEE., pp. 642-647, June 2015

[T. Kim 2014] Kim, T., & Jeong, H. Y.: A novel algorithm for crash detection under general road scenes using crash probabilities and an interactive multiple model particle filter. IEEE Transactions on Intelligent Transportation

Systems, Vol. 15, No. 6, pp. 2480-2490, 2014

[J.LEE 2014] LEE, J., CHOI, J., YI, K., SHIN, M. & KO, B. 2014. Lane-keeping assistance control algorithm using differential braking to prevent unintended lane departures. Control Engineering Practice, 23, 1-13.

[Tobias 2017] Tobias Kessler, Pascal Minnerup, David Lenz, Alois Knoll.: Systematically Comparing Control Approaches in the Presence of Actuator Errors. In Intelligent Vehicles Symposium (IV), IEEE. pp. 11-14, 2017

[Jin 2009] Jin Li-sheng, Fang Wen-ping, ZHang Ying-nan, Yang Shuang-bin, Hou Hai-jing. : Research on safety lane change model of driver assistant system on highway. In Intelligent Vehicles Symposium (IV), IEEE, June 2009

[Markus 2010Markus Hörwick and Karl-Heinz Siedersberger, Strategy and The architecture of a Safety Concept for Fully Automatic and Autonomous Driving Assistance Systems., In Intelligent Vehicles Symposium (IV), IEEE, June 2010

초 록

자율주행 차량의 고장 진단 및 대응 제어 전략

본 연구는 자율주행 차량의 고장 진단 시스템 구조에 대해 연구하였다. 이 연구에는 자율주행 차량 고장안전 시스템 구조를 가지기 위해 차량의 하드웨어, 소프트웨어 및 통신구조도 구성하였다. 또한 운전자가 고장 발생에도 불구하고 개입하지 않을 경우 고장감지 및 비상 제동 알고리즘을 사용하여 정차한다. 미국 도로 교통 안전 위원회(NHTSA)가 발표한 'AUTOMATED DRIVE SYSTEM 2.0'보고서에 따르면 자율주행 차량에 문제가 발생하였을 경우 위험을 최소화 하는 모드로 변경해야 하는 것이 필수적이라고 명시하였다. 두 번째로, 자율주행 시스템의 실시간 모니터링을 통해 정상작동 상태인지에 대한 확인이 필요하다고 언급하였다. 셋째, 자율주행 모니터링은 운전자가 차량을 적절하게 제어할 수 있도록 또는 시스템이 개별적으로 최소 위험 조건으로 돌아갈 수 있도록 해야 한다. 또한 fallback 전략은 운전자의 인지와 판단에 대한 오류 최소화를 고려해야 한다. 위에서 언급한 바와 같이, 자율주행을 위한 고장안전 시스템 구축은 자율주행에 필수적인 요소이다. NHTSA 가 명시한 표준에 기준하여 시스템을 설계하였다.

차량의 구조적 측면에서 각 상태를 모니터링 할 수 있게 두개의

액추에이터(PC및 Autobox)를 설계하였고 그 제어기 안에 필요 알고리즘이나 통신이 진행된다. 또한 고장 감지 부분을 구성하여 고장을 찾게 된다. 고장안전 제어 부분을 도입하여 두 개로 나눈 엑추에이터 중 상위제어기인 PC 에서의 오류가 발생하였을 때 제안된 슬라이딩 모드 제어 기반으로 종 방향 제어를 사용하여 비상시 차량이 긴급제동 및 정차에 이르게 된다. 긴급제동제어는 종 방향, 횡 방향으로 나눠져 있고 제안된 알고리즘은 인지 및 판단 부분이 작동하는 상위제어기에서 오류가 났을 시 그 정보를 사용하지 못하더라도 차량 샤시 정보만을 활용하여 제어하여 정차하는 방법을 제시한다. 안전 주행 거리는 실시간으로 계산되어 SMC 에서 사용되는 레퍼런스 모델로 넘어가게 되고 그 레퍼런스 모델은 레퍼런스 가속도, 레퍼런스 속도 및 레퍼런스 스테이션을 계산합니다. 비상 상황에서 기준 값을 추적하는 슬라이딩 모드 제어 기반 종 방향 가속도 제어 알고리즘 그리고 횡 방향 제어를 위해 DR 을 사용하여 안전거리 영역 안에서 주행을 실시하는 제어부분으로 구성되어있다. Carsim 과 MATLAB/Simulink 기반 시뮬레이션 평가를 수행하고 또한 자율주행 차량을 이용한 실차실험으로 검증을 완료하였다.

주요어: 페일세이프, 고장안전, 고장안전 시스템, 자율주행, 고장진단, 고장안전 제어, 고장 제어,

학 번: 2016-20709