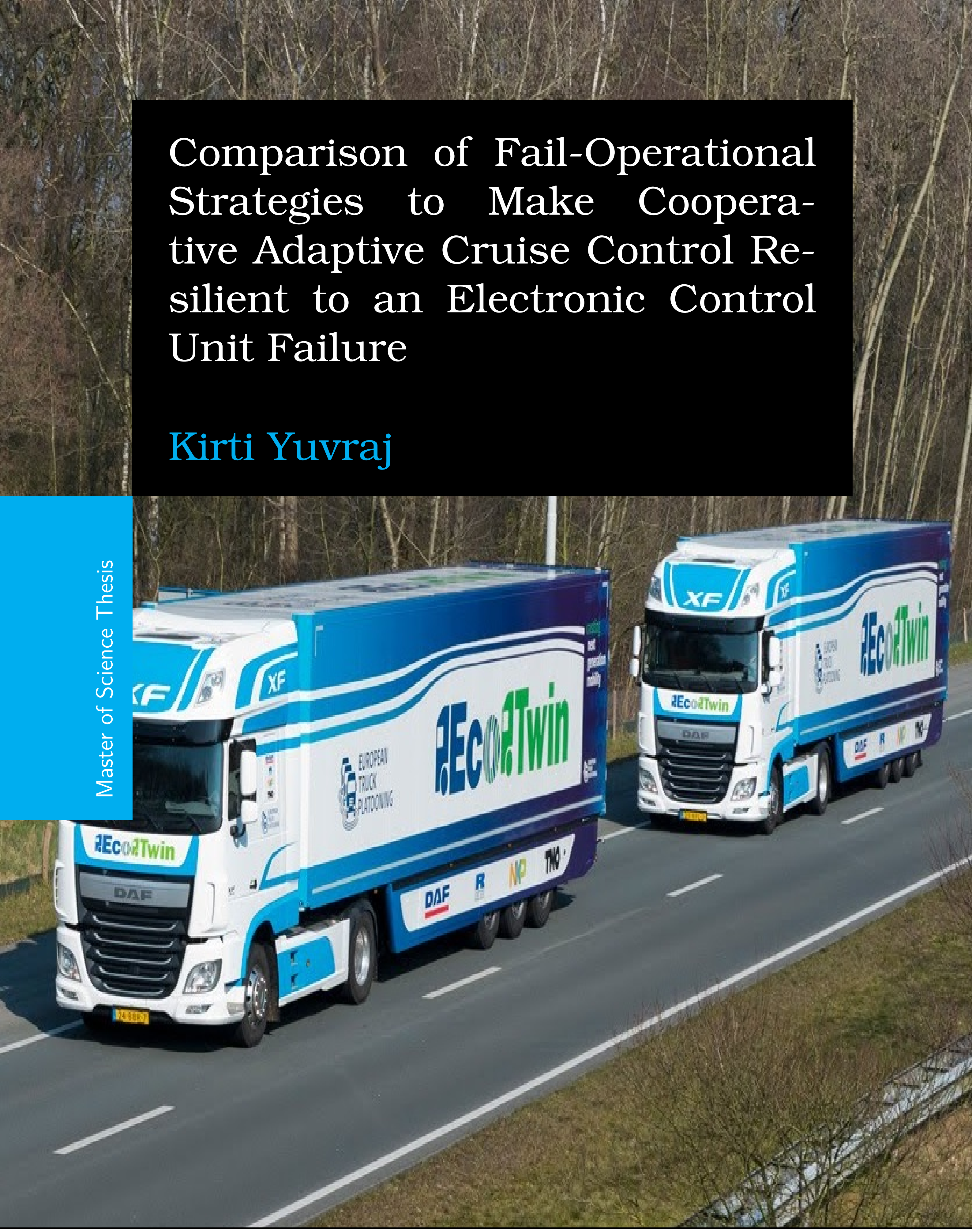
Comparison of Fail-Operational Strategies to Make Cooperative Adaptive Cruise Control Resilient to an Electronic Control Unit Failure

Kirti Yuvraj

Master of Science Thesis



Delft Center for Systems and Control

Comparison of Fail-Operational Strategies to Make Cooperative Adaptive Cruise Control Resilient to an Electronic Control Unit Failure

Master of Science Thesis

For the degree of Master of Science in Systems and Control at Delft University of Technology

Kirti Yuvraj

January 22, 2018

Faculty of Mechanical, Maritime and Materials Engineering (3mE) · Delft University of Technology

The work in this thesis was supported by TNO, Helmond. Their cooperation is hereby gratefully acknowledged.

Delft University of Technology
Department of
Delft Center for Systems and Control (dcsc)

The undersigned hereby certify that they have read and recommend to the Faculty of Mechanical, Maritime and Materials Engineering (3mE) for acceptance a thesis entitled

Comparison of Fail-Operational Strategies to Make Cooperative Adaptive Cruise Control Resilient to an Electronic Control Unit Failure

by

Kirti Yuvraj

in partial fulfillment of the requirements for the degree of

Master of Science Systems and Control

Dated: January 22, 2018

Supervisor(s): ____________________
dr.ir. Arturo T. Ruiz

____
dr.ir. Anil K. Madhusudhanan

Reader(s): ____________________
dr.ir. Hans Hellendoorn

____
dr.ir. Riccardo Ferrari

Abstract

With the tremendous increase of vehicles and limited infrastructure for its smooth movement, traffic jams have become a significant problem these days. To address this issue, significant research and development in the field of Intelligent Transportation System (ITS) is currently being carried out. One such technological development that allows grouping of vehicles into platoons, controlled by one leading vehicle has proved to be a fruitful and potential solution for the existing issue of traffic jams.

The state of the art technology that enables vehicle platooning is called Cooperative Adaptive Cruise Control (CACC). In CACC, the individual vehicles are grouped into platoons and allowed to automatically adjust their speeds using on-board sensors and vehicle to vehicle communication to maintain a desired and safe inter-vehicle distance. The specialty of CACC is that it enables to have small inter-vehicle distance between the vehicles which increases road throughput and reduces air drag on the vehicle. Consequently, traffic jams and fuel emissions are reduced.

However, a crucial challenge arrives due to its high dependency on mechatronic devices, as a fault in such devices could lead to unsafe conditions for the vehicles in a platoon. Hence, there is a need of making CACC application Fail-Operational, which means that the vehicles would continue to function safely under faults and failures of those devices. TNO in its EcoTwin III project has identified Electronics Control Unit (ECU) to be a very critical component and uses the concept of redundancy to provide the Fail-operational capability that can tolerate one failure of ECU. However, this implementation involves a transition period caused due to fault detection and switching of ECU. This transition period could jeopardize the safety of vehicles under conditions where a nominal ECU would have kept the vehicles safe.

Thus the objective of this MSc thesis is to address the problem of the transition period of a homogeneous platoon under ideal communication network conditions. In the first part, a model is proposed that captures the effect of the transition from primary ECU to the standby ECU on the platoon dynamics. This is done for both warm and hot standby strategies which depend on the functionality of the standby ECU. We see how this transition period affects the overall safety of the system under a worst-case scenario (emergency braking). In the second part, to improve the safety and exclude the effect of the transition period, a new method of implementation of existing control law is proposed. This technique exploits the benefit of using communicated data from the preceding vehicle for generating control input during the transition period.

Simulations are conducted for a two-vehicle platoon. The results show the effect of the transition period in a warm standby strategy will lead to collisions. The simulations also show that the hot standby strategy outperforms the warm standby one, though it cannot avoid collisions at large transition periods. On the other hand, the proposed new strategy shows the potential of using the communicated signal in preventing collision and shows significant improvements in comparison to other two strategies at the larger transition period.

Table of Contents

List of Figures

List of Tables

Acknowledgements

First and foremost, I would like to thank my supervisor, Arturo Tejada Ruiz for giving me the opportunity to carry out Master thesis under his supervision and helping me during the period. Elaborate and detailed discussions with him have contributed significantly to my understanding for carrying out research. Arturo, I would like to thank you for always being critical towards my work and showing me room for improvement. Further, I would want to give special thanks to my supervisor at TNO, Anil Kunnappillil Madhusudhanan. Your daily supervision and guidance have been very helpful. I would like to thank you for taking the time for Skype calls and helping me with my doubts even after joining another institution.

I would like to thank my parents, without their motivation and love I could not have reached here. Mom and Dad, I will forever be grateful for your sacrifice and support to help me follow my dreams. I would like to thank my sister and brother-in-law for all the love and support.

Dhruv, Som, Vimanyu, special thanks to you guys for helping and supporting me throughout the course. And lastly, I would like to thank Juhee Ryu for always being there through the ups and downs and cheering me up.

Delft, University of Technology
January 22, 2018

Kirti Yuvraj

Chapter 1

Introduction

An Intelligent Transportation System (ITS) is an active and advanced application of synergistic technologies striving to improve the efficiency of road transport, traffic management, mobility, and fuel consumption [3]. In this chapter, we introduce one such application known as vehicle platooning. Vehicle platooning is a method of grouping the vehicles such that the vehicles form a series following the preceding vehicle and traveling at a certain inter-vehicular distance, which depends on the vehicle speed [4]. Figure 1-1 shows a typical platoon of vehicles.

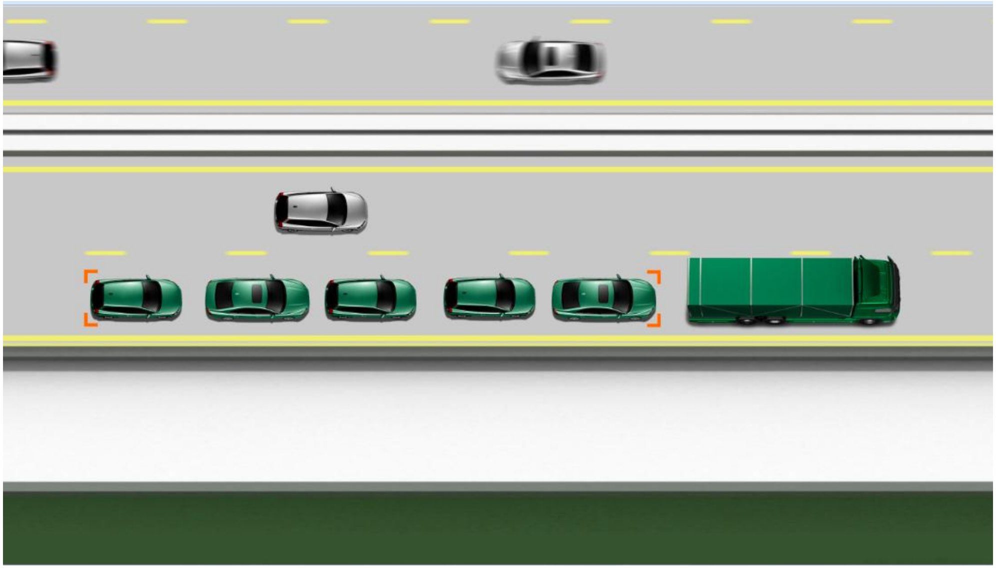


Figure 1-1: Platoon of vehicles [1]

Vehicle platooning results in lower fuel consumption, as the vehicles drive closer together at a constant speed with less braking and acceleration. This benefit has the potential to reduce the CO_2 emissions by up to 10 % [5]. Also, with conventional vehicles, most of the traffic

accidents are due to human error. Vehicle platooning helps in improving the safety, as the braking is automatic with almost negligible reaction time compared to human braking [5] [1]. It also optimizes the transport by using the roads more effectively, helping in faster transport and reduced traffic jams. And eventually, all these benefits correspond to huge economic benefits as well. The most popular technologies used for platooning are Adaptive Cruise Control (ACC) and Cooperative Adaptive Cruise Control (CACC). However, implementation of such sophisticated technologies for platooning has various challenges which will be discussed later in this chapter.
This chapter is organized as follows: Section 1-1 presents the currently available technologies for platooning viz. ACC and CACC. Section 1-2 presents the background and challenges for this thesis. Section 1-3 describes the research questions and finally, Section 1-4 presents the problem statement of this thesis, and, Section 1-5 concludes this chapter by presenting the outline of the thesis.

1-1 ACC and CACC

The following section explains the basic difference between ACC and CACC and what makes CACC superior to ACC. ACC and CACC allow automatic platooning of vehicles by controlling the longitudinal vehicle motion.

1-1-1 Adaptive Cruise Control (ACC)

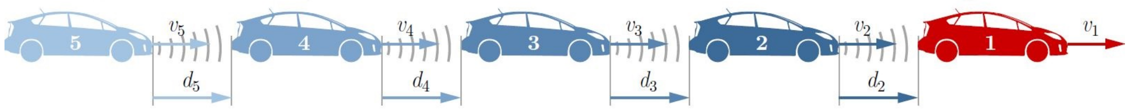


Figure 1-2: Platoon of vehicles using ACC

An ACC system employs sensors like radar or other on-board ranging sensor and actuators like brakes and throttle to implement the longitudinal control. The sensors measure the relative distance and relative velocity of the preceding vehicle. The system controls the vehicle speed such that the desired distance between vehicles is maintained by controlling either throttle or brake action [6]. ACC is an important part of the self-driving vehicles of the near future and currently, ACC system is mostly used as a driving comfort system [7] and are not been utilized extensively for a large platoon of vehicles. In today's time, almost every major vehicle manufacturer like Toyota, Mercedes, Volkswagen, etc. has one of its vehicles equipped with the ACC system. From the late 90s, there has been huge innovation and development in the technology which has contributed extensively in reducing the cost and increasing the safety of the system. The ACC system works in two modes: (a) the distance control mode also called as time gap control and (b) the speed control mode [6]. Figure 1-2 Shows a basic platoon of vehicles using an ACC system.

1-1-2 Cooperative Adaptive Cruise Control (CACC)

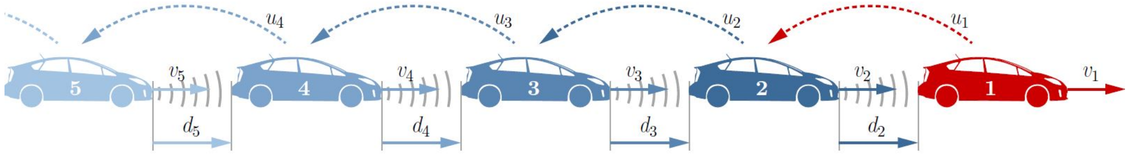


Figure 1-3: Platoon of vehicles using CACC [2]

CACC is an extension of ACC and the state of the art technology for vehicle platooning. CACC could also be seen as an improvement of ACC system [8]. The sensors employed in ACC system have a finite readout time and it can only detect the acceleration and deceleration of the preceding vehicle after it has occurred. These response delays directly affect the ability of the system to follow vehicles accurately and closely. However, by communicating the intended acceleration from the preceding vehicle to the following one, the response delays can be removed and allow platooning for smaller inter-vehicle distances [9]. This is the added advantage of CACC over ACC, as CACC uses data exchanged by the vehicles via wireless inter-vehicle communication along with on-board sensors [10]. The inclusion of wireless communication allows the vehicles to follow the preceding vehicles more closely while maintaining string stability. String stability means that the disturbances which are formed in a normal traffic situation due to braking and acceleration do not propagate in an amplified manner. Due to the vehicle-to-vehicle (V2V) exchange of data like acceleration, the following vehicle can react to the sudden disturbances quickly and more efficiently[11]. CACC technology can guarantee string stability for inter-vehicle time gap smaller than 1 sec. This advantage of CACC improves the road throughput, reduces aerodynamic drag hence reducing the fuel consumption. Figure 1-3 shows a basic platoon of vehicles using CACC system. CACC allows the vehicles to form a more compact platoon, which increases the road throughput and reduces the fuel consumption.

1-2 Background and Challenges

TNO has been a part of the development of the underlying CACC technology for several years and has been continuously working on developing strategies for the real-time implementation of CACC enabled platoon. TNO has partnered with several companies and partners to implement a safe, reliable and efficient truck platooning concept by 2020. The EcoTwin collaboration of TNO, DAF, NXP, and Ricardo has been the stepping stone towards the reality of platoons on the public roads. The technology enables at least three trucks connected with each other through data communication to platoon safely and automatically at 0.3 seconds apart. As the CACC technology demands several real-time signals, data communication and controlled actuation, implementing such a technology requires extensive use of mechatronics system comprising of integrated electronic sensors, information processing components, actuators, Electronic Control Units (ECU), etc. However, such system comes with some disadvantages, for example, lower reliability and different fault behavior of electronic and electrical components [12]. For example in a CACC enabled platoon of two vehicles, the failure of RADAR sensor in the follower vehicle will jeopardize the safety of the platoon as the faulty RADAR sensor could lead the follower vehicle to into or fall behind the preceding vehicle. In another instance, a fault in the ECU of any vehicle could completely disrupt the platoon because there will be no guarantee of the vehicle control. Hence, in the EcoTwin III project, functional safety standards like ISO 26262, CENELEC standards, EN 50126 (The Specification and Demonstration of Reliability, Availability, Maintainability, and Safety), EN 50128 (Communications, signaling and processing system) have been used [13]. Based on these standards, for the EcoTwin III project, several risk analysis and failure modes have been compiled. For example, a report on Fault Tree Analysis of EcoTwin III architecture was compiled by TNO, which listed potential hardware and software faults and recommendation for fault-tolerance. Such fault-tolerance recommendations aim to increase the reliability and safety of the system. When fault-tolerance allows the vehicle to function with the same or similar degree of performance under the presence of a fault in its critical components, the system is called fail-operational [14]. There has been some work done regarding developing of fault tolerance mechanism using on-board sensors by [15]. Also, TNO has implemented a fault-tolerant system aimed at making CACC application fail-operational against single ECU failure. This fault-tolerant system incorporates a redundancy strategy. But an extensive analysis of the system from a safety point of view is needed and is the focus of this thesis. Hence, the research questions of this thesis are presented in the next section.

1-3 Research Questions

It is clear that the failure of critical hardware could lead to a hazardous situation and a fault-tolerant system is a necessity in CACC. Fault-tolerance is achieved by having redundancy in the system and TNO has adopted one such system to make its CACC implementation resilient to an ECU failure. With such system, the following research questions were posed:

- Is the currently implemented CACC system acceptably safe for an ECU failure? Acceptably safe means that all the physically avoidable worst-case situations will not lead to collision considering a fault-tolerance system for ECU failure.
- Does the existing fault-tolerance system has any limitations?
- Can an existing fault-tolerance system be improved without the need for any additional hardware setup?

To answer the research questions, detailed knowledge of the CACC system, its control objective, and current TNO's implemented strategy is required, which is discussed in the Chapter 2.

1-4 Problem Statement

After establishing the theoretical structure and the hardware implementation regarding CACC including TNO's fault-tolerance system in Chapter 2, problem statement for this thesis has been formulated.

- In a fault-tolerance system, recovery time or transition period is a very important attribute of the system and hence, a maximum transition time needs to be identified during which the system has no control input.
- Further, the aim is to analyze the safety of the platoon during an emergency braking scenario with ECU failure and validate the performance of the current implementation of fault-tolerance system by TNO. In doing so, the safety criteria ($d_i(t) > 0$) needs to be evaluated at all times.
- This work will propose a new fault-tolerance implementation strategy to reduce the effect of transition duration based on the current TNO's hardware setup.

1-5 Thesis Outline

The thesis is organized as follows:

- Chapter 2 introduces the concepts of CACC control objectives and standard hardware implementation. Fault-tolerance system adopted by TNO is also discussed.
- Chapter 3 describes the analysis methodology considering a worst-case scenario. The limitations of TNO's fault-tolerance system is described in terms of transition period. A condition for platoon's safety is evaluated after the ECU failure. And a strategy is proposed for the improvement of the existing fault-tolerance system.
- Chapter 4 provides the simulations and plots to explain the theoretical analysis done in the previous chapter.
- Chapter 5 summarizes the thesis contribution and presents some remarks along with some recommendations.

Chapter 2

CACC system structure

In the previous chapter, some insights like features, benefits, and challenges about CACC were given. However, to address the goals and objectives, detailed information on CACC, its control structure, technology and its implementation is required, which is described in this chapter.

For this, Section 2-1 explains the control framework of the CACC system. Section 2-2 explains the longitudinal control of the vehicle, the mathematical aspects and the standard hardware requirements of the CACC system along with TNO's fault tolerance system. Finally, Section 2-3 presents the summary of this chapter.

2-1 Control framework of the CACC system

Figure 2-1 represents the control framework of a CACC system which consists of upper-level and lower-level controllers and are implemented in real-time ECUs [16] [17]. The CACC system box in Figure 2-1 is implemented within each following vehicle, here vehicle i, but it is shown outside the vehicle to improve readability. As shown in Figure 2-1, the upper-level controller integrates the sensor data and the preceding vehicle's intended acceleration to generate the desired acceleration u_i. This upper-level controller generally runs on a standalone ECU and communicates with the ECU on which lower-level controller is running. The control performance of the upper-level controller affects the lower-level directly [16].

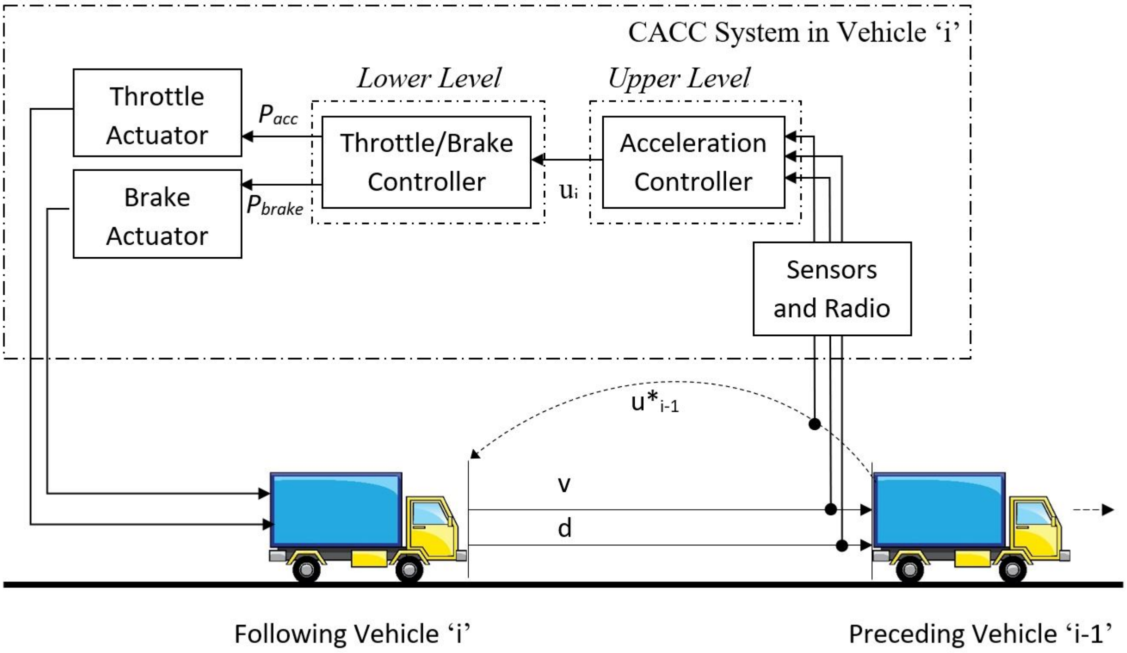


Figure 2-1: Hierarchical control framework of a CACC system

The lower-level controller calculates the required throttle angle and brake pressure depending on the desired acceleration u_i generated by the upper-level controller by calculating the torque needed on the axle shafts of the vehicle. The required torque is calculated using the following longitudinal equation of motion [17]:

$$m_v u_i = F_x - F_{Air} - F_{Roll} - F_{Slope}, \tag{2-1}$$

where m_v is the mass of the vehicle, F_x is the sum of longitudinal forces calculated at the road-tire interface, F_{Air} is the aerodynamic drag force, F_{Roll} is the rolling resistance force, and F_{Slope} is the road slope force [16]. With the combination of upper-level and lower-level controller, the Longitudinal motion of the vehicle in a CACC platoon is controlled. The next section describes the Longitudinal control in detail.

2-2 Longitudinal control in CACC

Longitudinal control in CACC allows vehicle platooning by controlling the longitudinal motion of the vehicle. To achieve this, control objectives have been defined which are mentioned in the Subsection 2-2-1. Subsection 2-2-2 explains the mathematical model required for longitudinal control. Subsection 2-2-3, finally explains a generic hardware implementation for CACC and an overview of the fault-tolerant system adopted by TNO.

2-2-1 Control Objectives

Following are the longitudinal control objectives of a CACC system [8], [18]:

- Reference or spacing policy: This objective defines a reference policy which is required to maintain a steady gap between vehicles [17]. The reference policy or the desired distance between vehicles is defined as:

  $$d_{r,i}(t) = r_i + hv_i(t), \quad 2 \leq i \leq m, \tag{2-2}$$

  where r_i is the desired standstill distance, v_i is the velocity of the follower vehicle and h is the headway time. This policy is also known as Constant Time-Gap (CTG) spacing policy [17]. In this, the desired inter-vehicle spacing is not constant but varies linearly with velocity.

- String stability: When the vehicle's controller ensures individual vehicle stability, the spacing error converges to zero when the preceding vehicle moves at constant velocity. However, in a normal traffic situation, the spacing error is non-zero due to acceleration and deceleration of the preceding vehicle. This spacing error propagates from vehicle to vehicle in a string of vehicles that use the same spacing policy and control law. The string stability of a string of vehicles refers to a property in which spacing errors are guaranteed not to amplify as they propagate upstream [19], [20], [18]. String stability is mostly studied in frequency domain where the amplification of either distance, velocity or acceleration error is measured using the transfer function. For example, let the position of the vehicle i be denoted with $Q_i(s)$ and position of the preceding vehicle $i-1$ be $Q_{i-1}(s)$ in Laplace domain of $q_i(t)$ and $q_{i-1}(t)$. The transfer function of input position $Q_{i-1}(s)$ to the output position $Q_i(s)$ is given as:

  $$\Gamma_i(s) = \frac{Q_i(s)}{Q_{i-1}(s)}. \tag{2-3}$$

  In order to ensure the string stability, the H_∞-norm of the transfer function (2-3) has to satisfy the following condition.

  $$||\Gamma_i(j\omega)||_{\mathcal{H}_\infty} \leq 1 \tag{2-4}$$

2-2-2 Mathematical model of a CACC system

To achieve the above-mentioned control objectives, a controller is designed using the vehicle longitudinal model which is explained below.

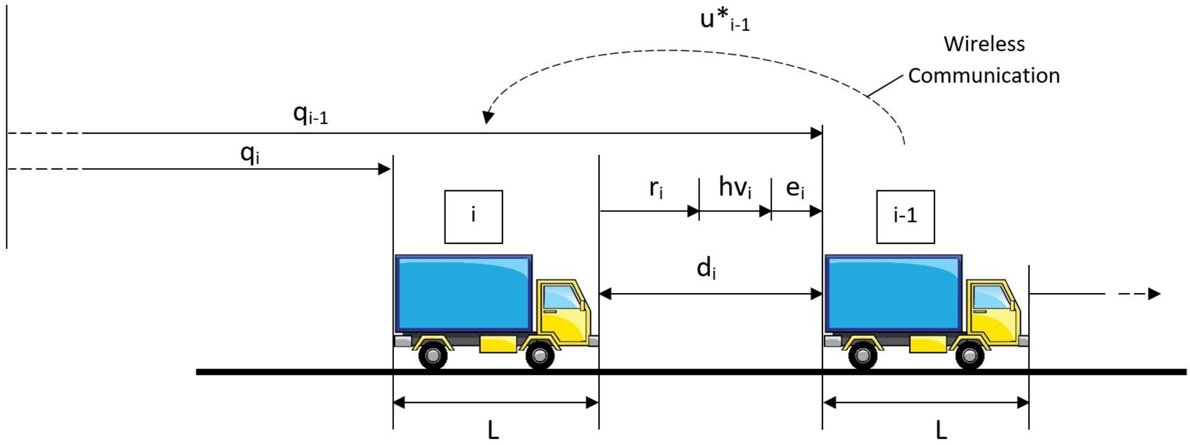


Figure 2-2: A platoon of vehicles equipped with CACC

The control law for CACC is based on the formulation of the error dynamics which is defined as considering a platoon of 2 vehicles, depicted in Figure 2-2, with d_i being the distance between vehicle i and its preceding vehicle $i-1$, and v_i is the velocity of vehicle i. The primary objective of the following vehicle i in the platoon is to follow the lead vehicle at the desired distance mentioned by Equation 2-2. Now, the actual distance between the two vehicles, d_i, expressed regarding their absolute positions (defined up to the rear of the vehicle), and L_i is the length of the i^{th} vehicle, is given by [8]:

$$d_i(t) = q_{i-1}(t) - q_i(t) - L_i. \tag{2-5}$$

The spacing error $e_i(t)$ is defined as:

$$\begin{aligned} e_i(t) &= d_i(t) - d_{r,i}(t) \\ &= (q_{i-1}(t) - q_i(t) - L_i) - (r_i + hv_i(t)). \end{aligned} \tag{2-6}$$

To achieve the first control objective, the following relation should hold:

$$\lim_{t\to\infty} e_i(t) = 0. \tag{2-7}$$

The vehicle model used in this thesis has been adopted from [8] which consists of three states: the inter-vehicle distance d_i, the speed v_i of the vehicle i and a_i be its acceleration. The vehicle model is represented in state space as:

$$\begin{pmatrix} \dot{d}_i \\ \dot{v}_i \\ \dot{a}_i \end{pmatrix} = \begin{pmatrix} v_{i-1} - v_i \\ a_i \\ -\frac{1}{\tau}a_i + \frac{1}{\tau}u_i \end{pmatrix}, \tag{2-8}$$

where u_i is the external input, which is the desired acceleration of the vehicle i, and τ is the time constant, which is considered same for both the vehicles and represents the engine dynamics. The control law for CACC is based on the formulation of the error dynamics which is defined as [8] [21]:

$$\begin{pmatrix} e_{1,i} \\ e_{2,i} \\ e_{3,i} \end{pmatrix} = \begin{pmatrix} e_i \\ \dot{e}_i \\ \ddot{e}_i \end{pmatrix} = \begin{pmatrix} q_{i-1} - q_i - L_i - r_i - hv_i \\ v_{i-1} - v_i - ha_i \\ a_{i-1} - a_i - h\dot{a}_i \end{pmatrix}, \tag{2-9}$$

$$\begin{aligned} \dot{e}_{3,i} = \dddot{e}_i &= \dot{a}_{i-1} - \dot{a}_i - h\ddot{a}_i \\ &= (-\frac{1}{\tau}a_{i-1} + \frac{1}{\tau}u_{i-1}) - (-\frac{1}{\tau}a_i + \frac{1}{\tau}u_i) - h((-\frac{1}{\tau}\dot{a}_{i-1} + \frac{1}{\tau}\dot{u}_i)) \\ &= (-\frac{1}{\tau}a_{i-1} + \frac{1}{\tau}a_i + \frac{h}{\tau}\dot{a}_i) + (-\frac{1}{\tau}u_i - \frac{h}{\tau}\dot{u}_i) + \frac{1}{\tau}u_{i-1} \\ &= -\frac{1}{\tau}e_{3,i} - \frac{1}{\tau}\underbrace{(h\dot{u}_i + u_i)}_{\xi_i} + \frac{1}{\tau}u_{i-1}. \end{aligned} \tag{2-10}$$

The representation of error dynamics in state space is given as:

$$\begin{pmatrix} \dot{e}_{1,i} \\ \dot{e}_{2,i} \\ \dot{e}_{3,i} \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & -\frac{1}{\tau} \end{pmatrix} \begin{pmatrix} e_{1,i} \\ e_{2,i} \\ e_{3,i} \end{pmatrix} - \begin{pmatrix} 0 \\ 0 \\ \frac{1}{\tau} \end{pmatrix} \xi_i + \begin{pmatrix} 0 \\ 0 \\ \frac{1}{\tau} \end{pmatrix} u_{i-1}. \tag{2-11}$$

Here, the u_{i-1} term is the intended acceleration of the preceding vehicle $i-1$ which is considered as a disturbance to the error system. To reject the disturbance and to obtain the control objectives, the following control law, ξ_i, is designed which comprises a feedback and a feedforward term [8].

$$\xi_i = \underbrace{K \begin{pmatrix} e_{1,i} \\ e_{2,i} \\ e_{3,i} \end{pmatrix}}_{Feedback} + \underbrace{u^*_{i-1}}_{Feedforward} . \tag{2-12}$$

Here $K = (k_p \quad k_d \quad k_{dd})$ is the tuning parameter which has a great impact on the dynamics of the vehicle. The feedforward variable u^*_{i-1} is the intended acceleration of the preceding vehicle and the superscript (*) represents that it is obtained through the wireless communication. The use of (*) helps the reader to identify the wirelessly communicated signal from the disturbance signal which is given as u_{i-1}. Note that, from Equation 2-10:

$$\xi \triangleq h\dot{u}_i + u_i. \tag{2-13}$$

Now by combining the Equations (2-12) and (2-13), we obtain the time derivative of control input u_i [8].

$$\begin{aligned} \dot{u}_i &= -\frac{1}{h}u_i + \frac{1}{h}\xi_i \\ &= -\frac{1}{h}u_i + \frac{1}{h}u^*_{i-1} + \frac{1}{h}(k_p e_{1,i} + k_d e_{2,i} + k_{dd} e_{3,i}). \end{aligned} \tag{2-14}$$

The stability criteria of the system can be fulfilled for values of K, when the system matrix given by Equation 2-11 satisfies the Routh-Hurwitz stability criterion [8]. The control input

u_i is the intended acceleration of vehicle i to maintain the desired distance from vehicle $i-1$ successfully. With particular values of K the stability of the system can be achieved but the controller gain, K, does not necessarily ensure string stability. The CACC system is transformed to Laplace domain to find out the controller such that the platoon has string stability.

Figure 2-3 shows the block scheme of controlled vehicle i including the preceding vehicle $i-1$. Here $G_i(s)$ is the transfer function of the vehicle's longitudinal dynamics in Equation 2-9, expressed in the Laplace domain. $H_i(s) = 1 + hs$ is the signal conditioning block to implement the spacing policy given in Equation 2-2.

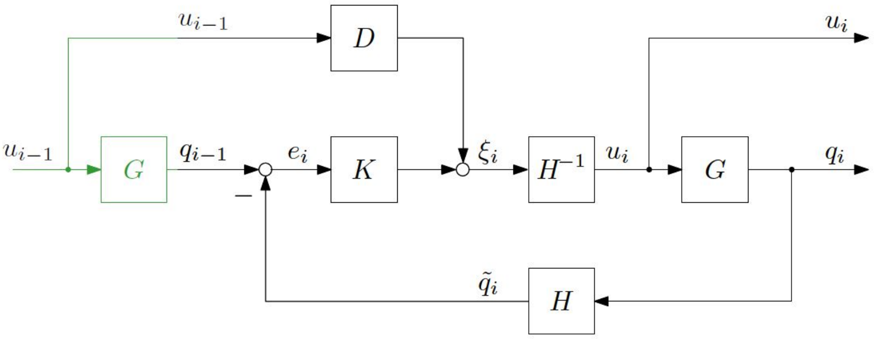


Figure 2-3: Block scheme of controlled vehicle i including the preceding vehicle

The vehicle model of all the vehicles in the platoon are considered as same. Hence, $G_i(s)$ is equal to G_{i-1} and is represented as a transfer function from input $u_i(s)$ to the output position $Q_i(s)$ as mentioned in [22]:

$$G(s) = G_{i-1} = G_i(s) = \frac{Q_i(s)}{U_i(s)} = \frac{1}{s^2(\tau s + 1)}, \tag{2-15}$$

Referring Figure 2-3, the Equation 2-3 is given as:

$$\Gamma_i = \frac{Q_i}{Q_{i-1}} = \frac{G(s)K(s) + D(s)}{H(1 + G(s)K(s))}, \tag{2-16}$$

where D(s) is the delay in communication. The controller gains K in the Equation 2-18 are obtained such that Equation 2-4.

2-2-3 Hardware implementation

In general, the following sensors and actuators are used to implement CACC in a vehicle. Table 2-1 and 2-2 shows the list of sensors and actuators required for the longitudinal control of a platoon [23] [24].

Table 2-1: Set of sensors and their functions

Sensor	Function
Radio	Communicate preceding vehicle intended acceleration
RADAR and Camera	Measure distance and relative velocity from preceding vehicle
GPS	Determine real time global position
Accelerometer	Measure longitudinal acceleration of the vehicle
Wheel Speed Sensor	Measure velocity
Throttle Angle sensor	Measure throttle Angle
Brake Pressure Sensor	Measure brake-line pressure

Table 2-2: Set of actuators and their functions

Actuator	Function
Throttle	Throttle the engine to produce desired torque
Brake	Brake torque for Longitudinal control

Table 2-3: Set of system components and the information lost due to its failure

Sensor Fault	Information Lost
Radio	u_{i-1}
RADAR and Camera	e_i , $v_{i-1} - v_i$
GPS	e_i , v_i
Accelerometer	a_i
Wheel Speed Sensor	v_i , a_i
ECU for upper-level controller	u_i

Now, Table 2-3 presents the list of hardware components and their relation to the elements in the model explained in the Subsection 2-3-2. This table makes clear the loss of information due to a failure in the respective component. Also, several other actuators, sensors used for lateral control, ECU for lower-level control and other functions of ECU for upper-level control like world model and sensor fusion are not considered because of their exclusion from the scope of the thesis. From Table 2-3, it can be seen that with the loss of the ECU, control input required for longitudinal control is lost. Several sensors correspond to the same type of information via sensor fusion and are used for accurate measurement of physical parameters. In a CACC platoon, the consequences of any component failure depend on many factors such as the exact hardware and software implementation, the situation of the platoon and other environmental conditions. Hence, a systematic analysis of hazards and risks associated with the platoon should be performed at the design time. The conclusion of that analysis will help in identifying the critical components, for example, having with lower reliability or higher failure rates. And hence countermeasures for those critical components are designed and incorporated to mitigate the occurrence of hazard due to its failure. Although such analysis is out of the scope of the thesis, an internal TNO analysis report on the implementation of TNO EcoTwin III suggests the ECU running upper-level controller requires special attention which is explained with the help of Figure 2-4. Figure 2-4 shows the architecture of a basic implementation of CACC system with two ECUs, namely, ECU 1 which contains upper-level controller and ECU 2 which contains the lower-level controller, also connected to sensors and radio to receive sensor and radio data. In Figure 2-4, it can be seen that ECU 1 receives the sensor and radio data from ECU 2 and computes the control input u_i which is communicated to the lower-level controller running on ECU 2 for generating the desired torque for throttle or brake, explained in Section 2-1. Once the ECU 1 fails permanently and stops generating the control input (assuming the ECU 1 fails silent and outputs 0), the lower-level controller then starts tracking 0 and maintains the acceleration of the vehicle i at 0. Due to this, the velocity of the vehicle does not change and it maintains its previous state of motion. Under this circumstance, the driver is required to take control of the vehicle i.

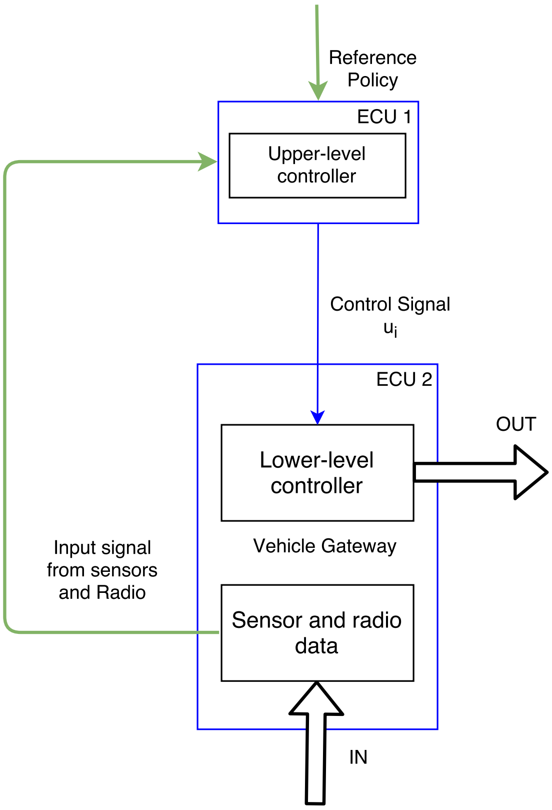


Figure 2-4: Basic control architecture for CACC

Platooning with CACC aims at reducing the inter-vehicle distance considerably. When there is an ECU failure, the system cannot depend on the driver as a fall-back because the reaction time of a driver may vary from hundreds of milliseconds to 7 seconds [25] [26], which is much greater than the desired inter-vehicle time gap of around 0.5 seconds. This implies that there shall be additional components that ensure the safety of the vehicle until the driver takes control. These additional components shall act as the fall-back and make the system fault-tolerant against an ECU failure. TNO has adopted such a fault-tolerant system in their EcoTwin III project where two additional ECUs (ECU 3 and ECU 4) have been added to the system which is shown in Figure 2-6. In this thesis failure of ECU is considered to be fail-silent and the output from the ECU is considered to be 0.

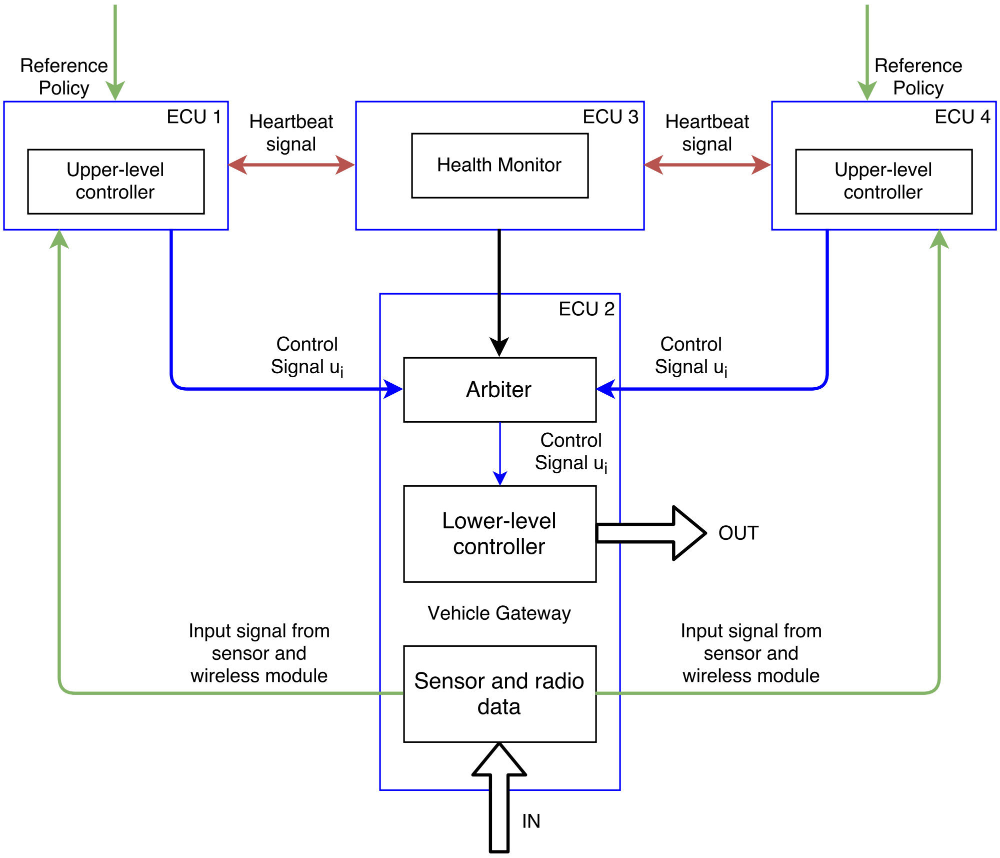


Figure 2-5: Control architecture with fault-tolerance for CACC

The main feature of the fault-tolerant architecture is the inclusion of a Health Monitor (running on ECU 3), an additional ECU called as safety ECU (ECU 4) and an Arbiter. Following are the functions of these components.

- Safety ECU: The Safety ECU (ECU 4) considered as a spare ECU to ECU 1. It gets inputs from all the sensors and radio and does all the processing work similar to the Primary ECU. The desired input for the lower-level controller is computed and sent to the Arbiter.
- Health Monitor: The Health Monitor checks all the software and hardware components. It receives periodic signals from both the ECUs called Heartbeat and checks for its availability. The Health Monitor adopts a fault detection protocol in which it waits to receive a required number of Heartbeats in a given time. This Heartbeats signal is a message sent from an originator to a destination to identify whether the originator has failed or no longer available. If the Health Monitor does not receive the required number of Heartbeats, then it generates a command to the Arbiter to switch the control input coming from ECU 1 to ECU 4 and alerts the driver.

- Arbiter: This is a software feature (running on ECU 2) which acts as a switch. It receives the command from the Health Monitor about the status of the ECUs. Depending on the command, the arbiter will execute a software switch for the selection of signals from the ECUs. For example, if the Primary ECU fails, the command generated by the Health Monitor will require the arbiter to switch to the safety ECU signals and allow the lower-level controller to access the signals coming from the Safety ECU instead of the primary ECU.

In TNO's implementation, it seems that a standby ECU is used to switch when the primary ECU fails. For doing that there is some amount of time spent on detection of fault and initiating switching by the health monitor. We call this duration of time as the transition period.

2-3 Summary

This chapter introduced the basics of CACC by explaining the theoretical and hardware structure. TNO's fault-tolerance system for an ECU failure has also been discussed. In this system, health monitor continuously monitors the ECUs for faults and initiates switching of standby ECU whenever fault occurs in the primary ECU. It was found that there exists a transition period during which the detection of fault and switching of signal from ECUs takes place. A more thorough analysis is done to obtain the maximum transition period in the next chapter.

Chapter 3

Analysis of Fault-Tolerant CACC Designs

In the previous chapter, theory on CACC and its implementation methodology for longitudinal control are briefly discussed. Information about the TNO's fault-tolerance system hardware setup for ECU failure is also presented. Hence in this chapter, further analysis will be made on the implemented fault tolerance system to study the effect of loss of control input during ECU failure on the platoon's safety. Also, a new strategy is proposed which is an improvement on TNO's current implementation strategy considering the same hardware setup.
This chapter is organized as follows: Section 3-1 defines the scope for the analysis. Section 3-2 defines the method used to provide the CACC system with fail-operational capability against an ECU failure. Section 3-3 proposes a strategy to make the CACC system fail-operational against an ECU failure.

3-1 Scope for the Analysis

Before getting into the details of CACC, we define the scope of the thesis. This is due to the complexity of the system and to avoid confusion. The following factors have been defined to limit the scope.

- The main focus is on the upper-level controller and not on the lower-level controller of the system.
- Only the longitudinal vehicle control has been considered.
- Vehicle-to-vehicle communication, vehicle's internal communication, sensors, and actuators do not have a delay or fail.

- The vehicle model considered does not contain lateral vehicle dynamics [27] [28] and road-tire friction [29].
- Variations in Weather conditions are not considered.
- Platoon of only two vehicles is considered

Next section defines the worst case scenario which is the basis for our investigation of the fault-tolerant system. If the vehicle is safe in worst case scenario, then it is also safe in normal situations.

3-2 Worst case scenario

To analyze the safety of the platoon, it has to be done under extreme situation. We call that extreme situation as the worst case scenario. In our case, the loss of ECU and emergency braking by the lead vehicle are the extreme situations. We believe that in an accident-free scenario, emergency braking is the extreme situation. And for the platoon, extreme braking along with ECU failure would be an extreme situation. Hence, the worst case scenario is defined as:

- The ECU that provides the longitudinal control input fails.
- At the same instance of ECU failure, the preceding vehicle brakes with maximum deceleration and finally comes to a standstill.

Before evaluating the fault-tolerant system in the worst case scenario, next subsection explains the individual component of the worst case scenario.

3-2-1 Emergency braking

The defined worst-case scenario has been chosen such that the disturbance caused due to the instant deceleration of preceding vehicle affects the most to the succeeding vehicle and its dynamics. To understand the dynamics of the preceding and succeeding vehicles, the following vehicle model has been chosen [8] From the Equation 3-1, it is clear that the velocity of the vehicle depends on the control input u_{i-1}. To perform an emergency braking action, a negative acceleration input u_{i-1} should be applied. Because the vehicle dynamics are assumed to be linear a continuous application of negative acceleration would yield negative vehicle speeds, which is not the case in reality, *i.e.* the vehicle does not move backward by applying brakes. Figure 3-1 shows how the velocity of the vehicle approaches negative value by applying a constant negative acceleration.

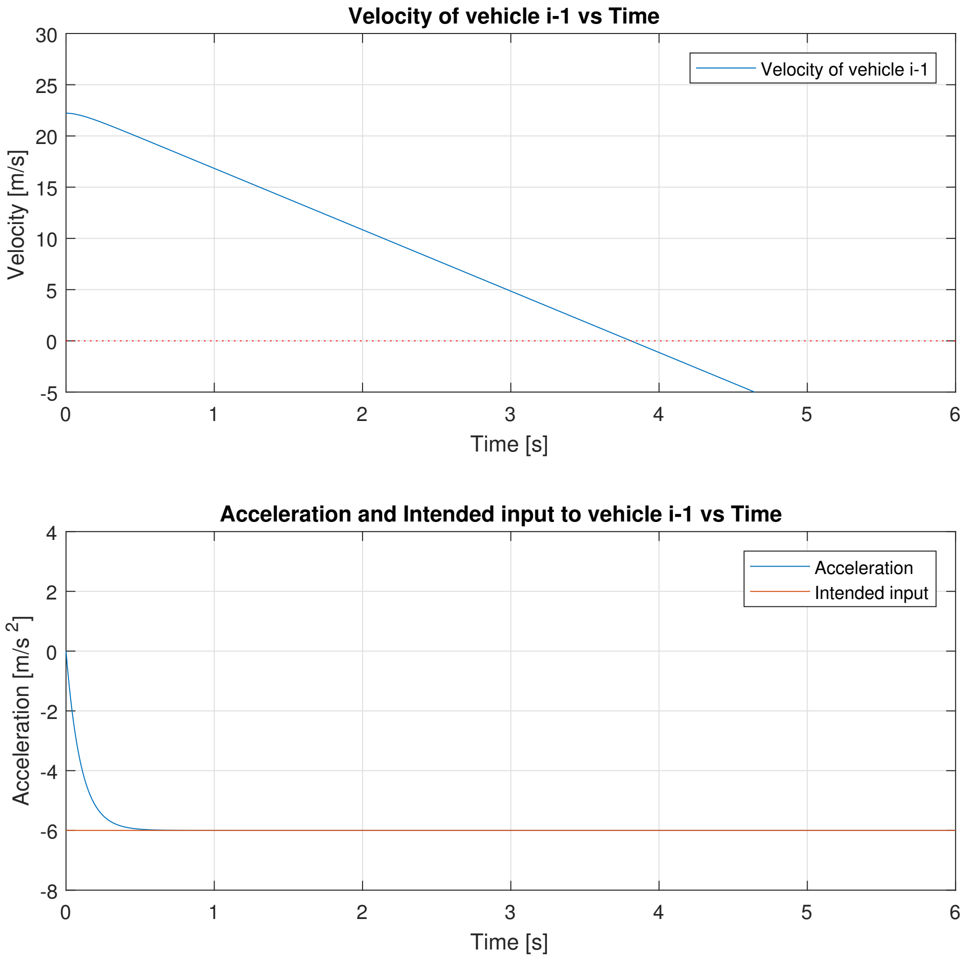


Figure 3-1: Top: Velocity of vehicle i-1 under constant deceleration. Bottom: Acceleration profile with respect to the input.

From Figure 3-1, it is clear that the negative acceleration input should be brought to zero to prevent the vehicle from going to negative speed. One way is to bring the input to zero as soon as the velocity becomes zero. However, by using this method, still, the speed of the vehicle becomes negative. This can be observed in Figure 3-2.

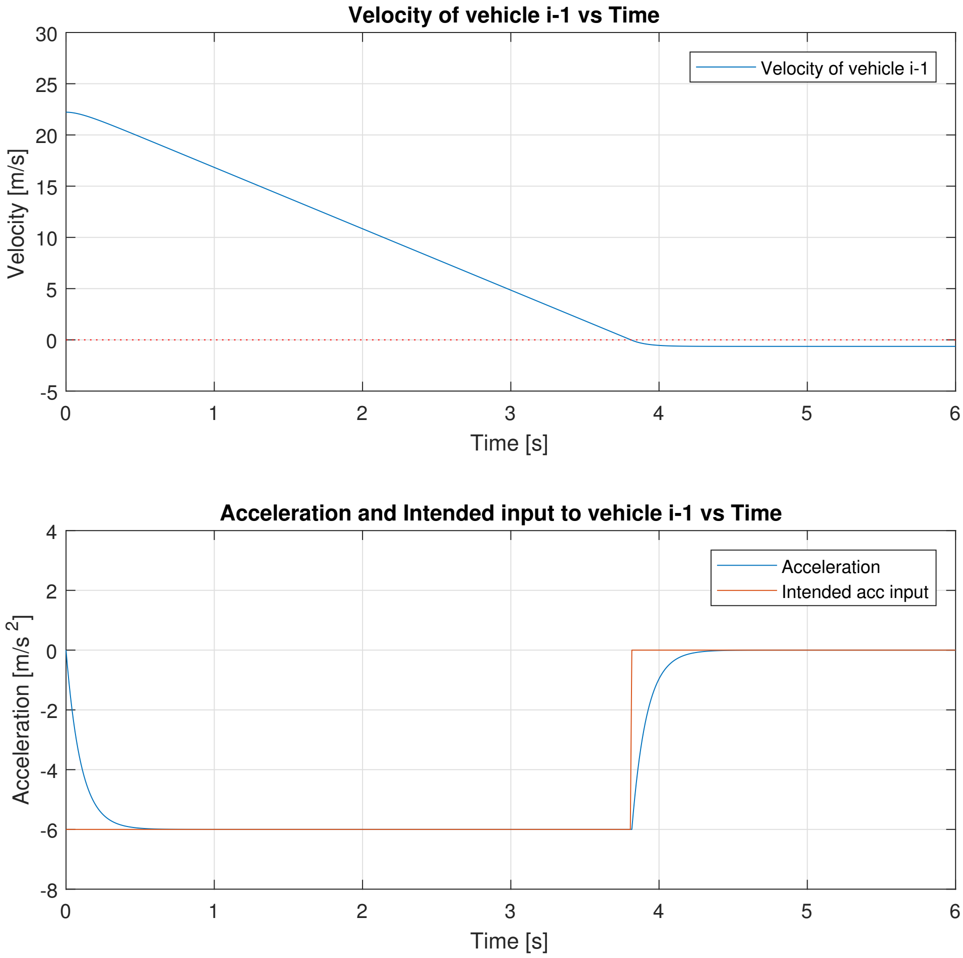


Figure 3-2: Top: Velocity of vehicle i-1 when deceleration stops when velocity becomes 0. Bottom: Acceleration profile with respect to the input.

Hence, the input u_{i-1} needs to be shaped so that the deceleration command stops when the vehicle speed is zero. The simplest way to do is to assume the deceleration commands last for only b seconds and then becomes zero. That is, the acceleration profile is given as:

$$u_{i-1}(t) = a_{min}[u(t) - u(t-b)], \quad t \geq 0, \tag{3-1}$$

where $u(t)$ and $u(t-b)$ are unit step function [30].

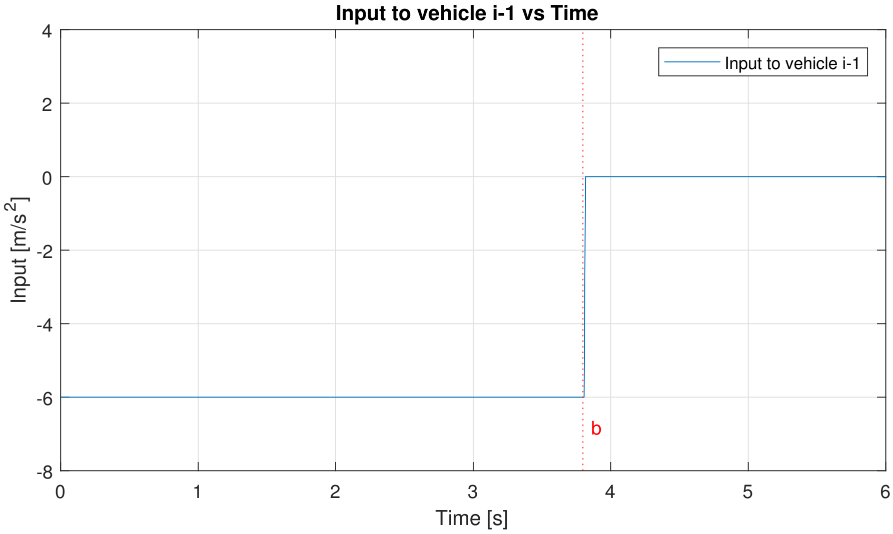


Figure 3-3: Input profile for vehicle i-1 where constant deceleration becomes 0 at time b

Using the vehicle model given in Equation 2-8 and Equation 3-1, we can write the following equation for vehicle i-1.

$$\dot{a}_{i-1}(t) = -\frac{1}{\tau}a_{i-1}(t) + \frac{1}{\tau}a_{min}[u(t) - u(t-b)] \tag{3-2}$$

Also, $\dot{v}_{i-1}(t) = a_{i-1}(t)$ and converting the Equation 3-2 in Laplace domain and obtaining an input response, following Equation is obtained in time domain:

$$v_{i-1}(t) = v_{i-1}(0) + a_{min}b - a_{min}\tau[e^{-\frac{(t-b)}{\tau}} - e^{-\frac{t}{\tau}}] \tag{3-3}$$

Where v_{i-1} is the absolute velocity of vehicle at time t, $v_{i-1}(0)$ is the initial velocity, a_{min} is the maximum deceleration.

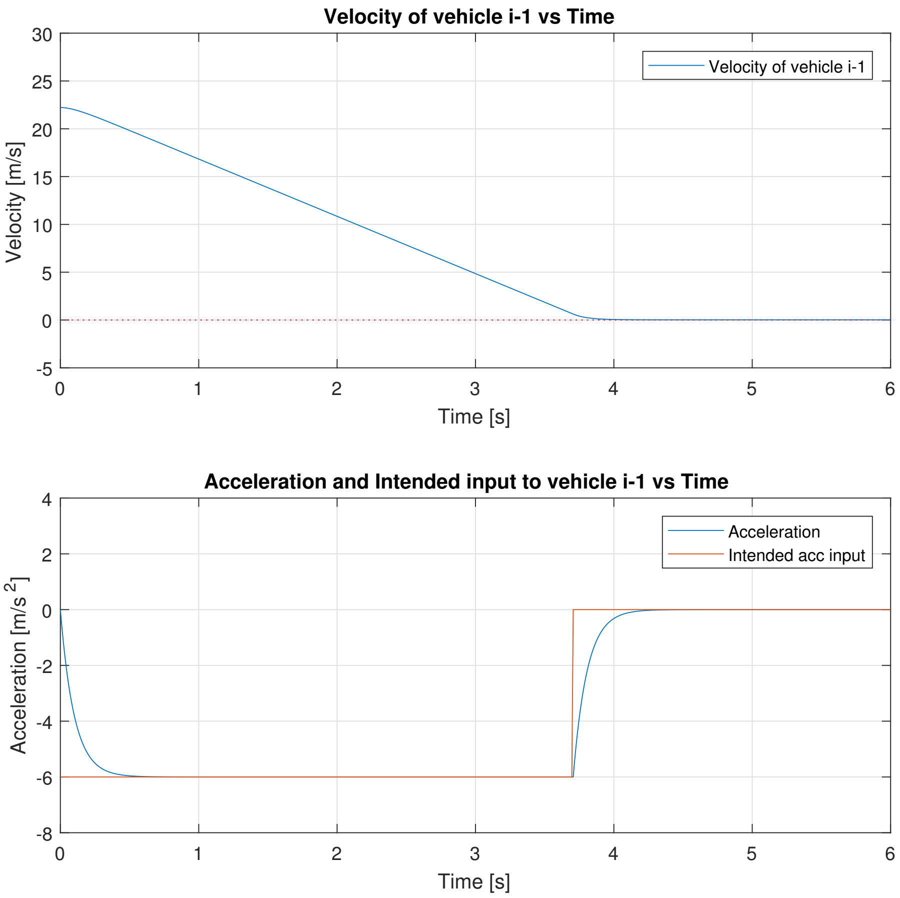


Figure 3-4: Top: Velocity of vehicle i-1 when deceleration stops at time b. Bottom: Acceleration profile of vehicle i-1 with respect to the input.

Using Equation 3-3, we can see that the speed of the vehicle $i-1$ goes to 0 when $t \to \infty$ and b is selected by using $v_{i-1}(0) - a_{min}b = 0$. However, for a numerical approximation to find a finite time of standstill *i.e.* $v_{i-1}(t) = 0$ when $v_{i-1}(t) \leq 0.2$.

3-2-2 ECU failure

As mentioned earlier, in the worst case scenario, the vehicle i loses its ECU containing upper-level controller and the vehicle $i-1$ applies brake at the same instance. The following subsection explains what happens when there is no control input from the vehicle i.

Considering the longitudinal equation of the vehicle from Equation 3-3 and $\dddot{q}_{i-1} = a_{i-1}$, the following equation can be written:

$$\dddot{q}_{i-1}(t) = -\frac{1}{\tau}\ddot{q}_{i-1}(t) + \frac{1}{\tau}u_{i-1}(t). \tag{3-4}$$

Taking Laplace trasform:

$$\begin{aligned}
& s^3Q_{i-1}(s) - s^2q_{i-1}(0) \\
& \quad -s\dot{q}_{i-1}(0) - \ddot{q}_{i-1}(0) = -\frac{1}{\tau}[s^2Q_{i-1}(s) - sq_{i-1}(0) - \dot{q}_{i-1}(0)] + \frac{1}{\tau}U_{i-1}(s), \quad \{\ddot{q}_{i-1}(0) = 0\}, \\
& \tau s^3Q_{i-1}(s) - \tau s^2q_{i-1}(0) \\
& \quad -\tau s v_{i-1}(0) = -s^2Q_{i-1}(s) + sq_{i-1}(0) + v_{i-1}(0) + U_{i-1}(s), \\
& (\tau s^3 + s^2)Q_{i-1}(s) = (\tau s^2 + s)q_{i-1}(0) + (\tau s + 1)v_{i-1}(0) + U_{i-1}(s), \\
& Q_{i-1}(s) = \frac{(\tau s^2 + s)}{\tau s^3 + s^2}q_{i-1}(0) + \frac{(\tau s + 1)}{\tau s^3 + s^2}v_{i-1}(0) + \frac{1}{\tau s^3 + s^2}U_{i-1}(s), \\
& Q_{i-1}(s) = \frac{q_{i-1}(0)}{s} + \frac{v_{i-1}(0)}{s^2} + \frac{1}{\tau s^3 + s^2}U_{i-1}(s).
\end{aligned} \tag{3-5}$$

Using input from the Equation (3-1) in Laplace form:

$$Q_{i-1}(s) = \frac{q_{i-1}(0)}{s} + \frac{v_{i-1}(0)}{s^2} + \frac{1}{\tau s^3 + s^2}\frac{a_{min}(1 - e^{-bs})}{s}. \tag{3-6}$$

Taking inverse Laplace:

$$q_{i-1}(t) = q_{i-1}(0) + v_{i-1}(0)t + \begin{cases} a_{min}(\frac{t^2}{2} + \tau^2 - \tau^2e^{-\frac{t}{\tau}} - \tau t), & 0 < t < b \\ -a_{min}(\frac{(t-b)^2}{2} + \tau^2 - \tau^2e^{-\frac{t-b}{\tau}} - \tau(t-b)), & t > b \end{cases} \tag{3-7}$$

Here $q_{i-1}(0)$ and $v_{i-1}(0)$ are the initial position and velocity of the vehicle $i-1$. $q_{i-1}(t)$ gives the absolute distance traveled by the lead vehicle $i-1$ in the presence of input $u_{i-1}(t)$. Similarly for vehicle i, the absolute distance traveled is given by the following equation:

$$Q_i(s) = \frac{q_i(0)}{s} + \frac{v_i(0)}{s^2} + \frac{1}{\tau s^3 + s^2}U_i(s). \tag{3-8}$$

But when there is a failure of ECU and control input is lost, $U_i(s) = 0$. Then the Absolute distance traveled by the vehicle i is given as :

$$q_i(t) = q_i(0) + v_i(0)t. \tag{3-9}$$

From Equation 3-9 we can see that the distance traveled by vehicle i is dependent only on its initial position $q_i(0)$ and initial speed v_i. Also, Where L is the length of the vehicle. When the vehicles are following at steady state and the error dynamics are $e_i(0) = 0$, from the Equation 2-6:

$$\begin{aligned} e(0) &= d_i(0) - d_{r,i}, \\ 0 &= q_{i-1}(0) - q_i(0) - L - r - hv_i(0). \end{aligned} \tag{3-10}$$

Therefore,

$$q_{i-1}(0) - q_i(0) - L = r + hv_i(0). \tag{3-11}$$

Now, the inter-vehicle distance is given by the following equation:

$$d_i(t) = q_{i-1}(t) - q_i(t) - L. \tag{3-12}$$

$$d_i(t) = r + hv_i(0)t + \begin{cases} a_{min}(\frac{t^2}{2} + \tau^2 - \tau^2 e^{-\frac{t}{\tau}} - \tau t), & 0 \leq t < b \\ -a_{min}(\frac{(t-b)^2}{2} + \tau^2 - \tau^2 e^{-\frac{t-b}{\tau}} - \tau(t-b)), & t \geq b \end{cases} \tag{3-13}$$

Equation 3-13 can be used to find out the time of collision *i.e.* time t when $d_i t = 0$ due to the loss of control input caused by ECU failure.

TNO has implemented a fault-tolerance mechanism and because of that, it is assumed that the control input of vehicle i is not lost permanently. Next section provides the analysis of the fault-tolerance mechanism under the existing hardware setup.

3-3 Implementation of fault tolerant system

Section 2-2-3 describes the hardware implementation of the fault-tolerance system adopted by TNO in the EcoTwin III project to avoid the loss of control input and provide fail-operational capability against ECU failure. The current fault-tolerance mechanism work as follows:

- The primary ECU is running at 100 Hz frequency and generates heartbeat messages to the health monitor every 10 ms. When a fault has occurred in the primary ECU, it stops sending heartbeat messages to the health monitor.
- The health monitor waits for 4 heartbeat signal taking 40 ms of time to confirm the occurrence of a fault in the primary ECU.
- The health monitor broadcast the command to arbiter every 100 ms.
- The arbiter receives the command from the health monitor and does a software switching, enabling the lower-level controller to access signal from the secondary ECU.
- The secondary or standby ECU then provides control input u_i to the lower-level controller.

The maximum transition period is now identified as 150 ms. Standby redundancy is a popular technique for designing fault-tolerant and reliable systems. It is broadly classified as cold, warm and hot standby[31] [32]. The cold standby implies that the redundant device is inactive and unpowered until it is switched on when the active unit fails. The recovery time with cold standby is highest but provides the highest reliability. The hot standby implies that the redundant device works in synchrony with the on-line unit and is ready to take over whenever a fault occurs. The recovery time with hot standby is the minimum but has higher failure rate compared to the cold standby. The warm standby is a trade-off between the cold and hot standby in terms of reliability, power consumption and recovery time [32]. The TNO's hardware implementation allows to have two standby philosophies *viz.* warm standby and hot standby depending upon the functioning of standby ECU, which are explained in following subsections.

3-3-1 Warm standby

Warm standby explains that the standby hardware is idle and not exposed to complete operational load. In this case, the standby ECU is considered to be powered on but does not compute the control inputs until it receives a command from the health monitor. Figure 3-5 shows the signal diagram during primary ECU failure. In the Figure 3-5, it can be seen that once the command is generated from the health monitor, secondary or standby ECU starts computing the control input u_i. However, a transition period of 150 ms is present when the lower-level controller does not receive valid control input u_i.

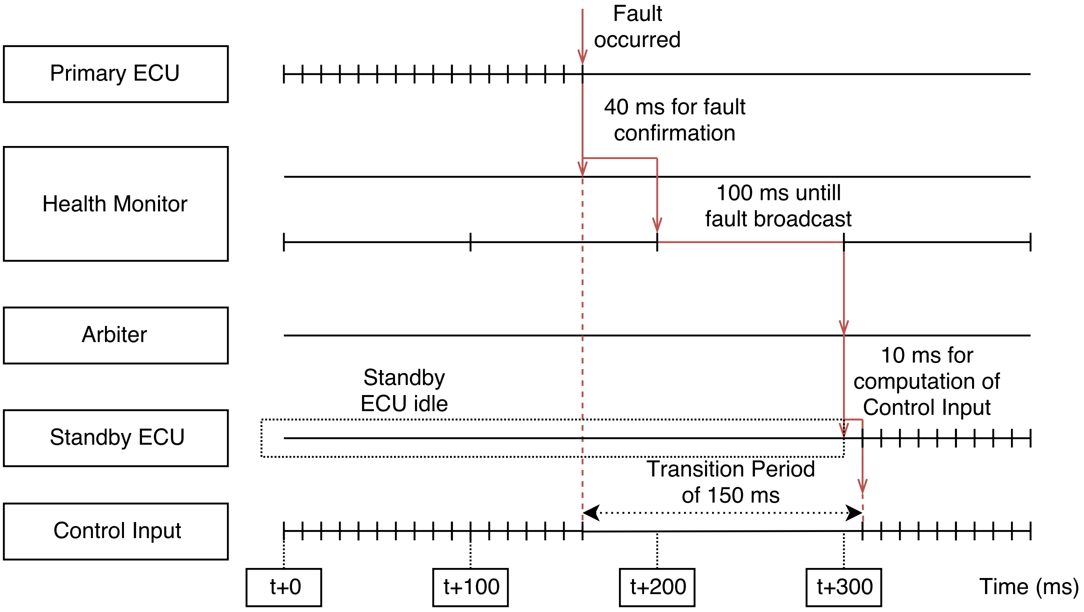

Fault occurred
Primary ECU
40 ms for fault confirmation
Health Monitor
100 ms untill fault broadcast
Arbiter
10 ms for computation of Control Input
Standby ECU idle
Standby ECU
Transition Period of 150 ms
Control Input
t+0
t+100
t+200
t+300
Time (ms)

Figure 3-5: Signal diagram during primary ECU failure under warm standby where standby ECU does not produce any output untill it receives a command from the health monitor.

To understand the effect of this warm standby philosophy on the platoon under worst case scenario, following approach has been used using the error dynamics described by Equation 2-11. The use of error dynamics helps in capturing the effect on the whole platoon rather than on a single vehicle. Considering following model from Equation 2-11

$$\begin{pmatrix}\dot{e}_{1,i}\\ \dot{e}_{2,i}\\ \dot{e}_{3,i}\end{pmatrix} = \begin{pmatrix}0 & 1 & 0\\ 0 & 0 & 1\\ 0 & 0 & -\frac{1}{\tau}\end{pmatrix}\begin{pmatrix}e_{1,i}\\ e_{2,i}\\ e_{3,i}\end{pmatrix} - \begin{pmatrix}0\\ 0\\ -\frac{1}{\tau}\end{pmatrix}\xi_i + \begin{pmatrix}0\\ 0\\ \frac{1}{\tau}\end{pmatrix}u_{i-1}. \tag{3-14}$$

When the primary ECU is working and producing the control input u_i, the dynamics of the platoon given by Equation 3-14 can be written as:

$$System : a \Rightarrow \dot{x}_i = A_c x_i + B_{c1}\xi_i + B_{c2}u_{i-1}. \tag{3-15}$$

And when the ECU fails, the dynamics of the platoon using Equation 3-15 under transition period can be written as:

$$System : b \Rightarrow \dot{x}_i = A_c x_i + B_{c2} u_{i-1}. \tag{3-16}$$

When the standby ECU is switched, $System : a$ is restored. The control objective of the platoon is guaranteed with the control law $\xi_i(t)$ when $t \to \infty$. Even though the system is stable after switching to standby ECU, due to the effect of the transition period on the platoon dynamics, one cannot guarantee a collision-free situation. For our analysis $System : a$ and $System : b$ are represented in discrete time with matrix A, B_1, B_2 and C. It is assumed that the initial error states are zero, i.e. $x_i(k_0) = 0$, followed by $u_i(k_0) = 0$. The following equations explain the evolution of states of $System : b$ during the transition duration, *i.e.* time taken to detect the fault and switch to secondary ECU when the primary ECU has failed. As described in the worst case scenario, the vehicle $i-1$ starts decelerating with a constant value u_{i-1} at k_0, this creates a disturbance in the dynamics of the platoon, assuming platoon is at steady state at k_0, *i.e.* $x_i(k_0) = 0$ and $u_i(k_0) = 0$.

$$\begin{aligned}
x_i(k_0+1) &= Ax_i(k_0) + B_2 u_{i-1}(k_0), \\
x_i(k_0+2) &= Ax(k_0+1) + B_2 u_{i-1}(k_0+1) \\
&= A[Ax_i(k_0) + B_2 u_{i-1}(k_0)] + B_2 u_{i-1}(k_0+1), \\
&= A^2 x_i(k_0) + AB_2 u_{i-1}(k_0) + B_2 u_{i-1}(k_0+1), \\
x_i(k_0+3) &= A^2 x_i(k_0+1) + AB_2 u_{i-1}(k_0+1) + B_2 u_{i-1}(k_0+2), \\
&= A^2[Ax_i(k_0) + B_2 u_{i-1}(k_0)] + AB_2 u_{i-1}(k_o+1) + B_2 u_{i-1}(k_0+2), \\
&\cdot \\
&\cdot \\
&\cdot \\
x_i(k_0+N) &= A^{N-k_0} x_i(k_0) + \sum_{m=k_0}^{N-1} A^{N-m-1} B_2 u_{i-1}(m).
\end{aligned} \tag{3-17}$$

During the transition duration, the control input u_i is given using Equation 2-14 and $\xi_i = 0$ (primary ECU is not working):

$$\begin{aligned}
u_i(k_0+1) &= 0, \\
u_i(k_0+2) &= 0, \\
&\cdot \\
&\cdot \\
&\cdot \\
u_i(k_0+N) &= 0.
\end{aligned} \tag{3-18}$$

Here N represents the number of samples corresponding to the transition duration. Using Equation 3-18 in the vehicle model given by Equation 2-8, the dynamics of the vehicle i is obtained. And because the control input u_i during the transition period is 0, the velocity and acceleration of the vehicle i remain unchanged. After N samples, as the secondary ECU switches, ($System : a$ is restored), and the initial states for $System : a$ are the final states of $System : b$. The evolution of states when standby ECU switches are given by following equations:

$$
\begin{aligned}
x_i(k_0+N+1) &= Ax_i(k_0+N) + B_1\xi_i(k_0+N) + B_2u_{i-1}(k_0+N), \\
x_i(k_0+N+2) &= Ax_i(k_0+N+1) + B_1\xi_i(k_0+N+1) + B_2u_{i-1}(k_0+N+1) \\
&= A[Ax_i(k_0+N) + B_1\xi_i(k_0+N) + B_2u_{i-1}(k_0+N)] \\
&+ B_1\xi_i(k_0+N+1) + B_2u_{i-1}(k_0+N+1) \\
&= A^2x_i(k_0+N) + AB_1\xi_i(k_0+N) + AB_2u_{i-1}(k_0+N) \\
&+ B_1\xi_i(k_0+N+1) + B_2u_{i-1}(k_0+N+1), \\
x_i(k_0+N+3) &= A^2x_i(k_0+N+1) + AB_1\xi_i(k_0+N+1) + AB_2u_{i-1}(k_0+N+1) \\
&+ B_1\xi_i(k_0+N+2) + B_2u_{i-1}(k_0+N+2) \\
&= A^2[Ax_i(k_0+N) + B_1\xi_i(k_0+N) + B_2u_{i-1}(k_0+N)] + AB_1\xi_i(k_0+N+1) \\
&+ AB_2u_{i-1}(k_0+N+1) + B_1\xi_i(k+2) + B_2u_{i-1}(k+2) \\
&= A^3x_i(k_0+N) + A^2B_1\xi_i(k_0+N) + A^2B_2u_{i-1}(k_0+N) + AB_1\xi_i(k_0+N+1) \\
&+ AB_2u_{i-1}(k_0+N+1) + B_1\xi_i(k_0+N+2) + B_2u_{i-1}(k_0+N+2), \\
&. \\
&. \\
&. \\
&. \\
x_i(k_0+N+P) &= A^{P-(k_0+N)}x_i(k_0+N) + \sum_{o=k_0+N}^{P-1} A^{P-o-1}[B_1\xi_i(o) + B_2u_{i-1}(o)].
\end{aligned}
\tag{3-19}
$$

And the control input is given using Equation 2-14 :

$$
\begin{aligned}
u_i(k_0+N+1) &= -\frac{1}{h}u_i(k_0+N) + \frac{1}{h}\xi_i(k_0+N) \\
&. \\
&. \\
&. \\
u_i(k_0+N+P) &= -\frac{1}{h^{P-(k_0+N)}}u_i(k_0+N) + \sum_{o=k_0+N}^{P-1} \frac{1}{h^{P-o-1}}\xi_i(o)
\end{aligned}
\tag{3-20}
$$

The control input given in Equation 3-20 is used to compute the dynamics of the vehicle i using Equation 2-8. Here P correspond to the number of samples since the activation time of $System : a$ until the vehicle i comes to standstill. It can also be observed from Figure 3-6, that after the transition period, the control input u_i starts at 0 and it takes time for the control input u_i to reach maximum control law ξ_i due to the inverse spacing policy $(1/H)$ shown in Figure 2-3. And due to this, the lower-level controller takes longer time to act on the vehicle dynamics.

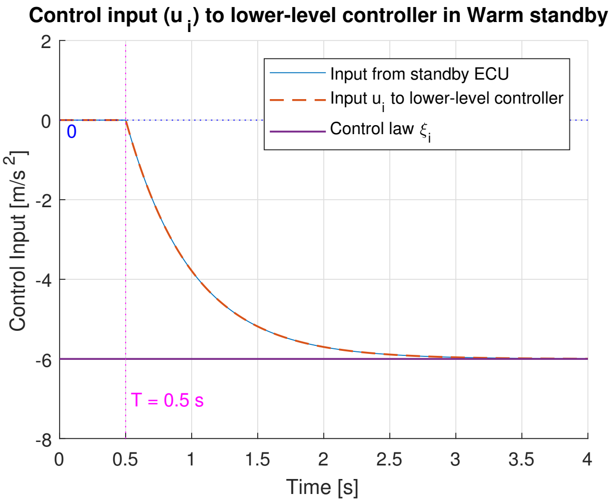


Figure 3-6: Control input in warm standby

A platoon is safe only when the inter-vehicle distance $d_i > 0$. Hence, the inter-vehicle distance d_i is checked at every sample. During the transition period, the velocity of the vehicle i is constant and the inter-vehicle distance d_i is keep decreasing. So the inter-vehicle distance d_i under transition duration is given as:

$$\begin{aligned} d_i(k_0+1) &= Cx_i(k_0+1) + r + hv_i(k_0), \\ d_i(k_0+2) &= Cx_i(k_0+2) + r + hv_i(k_0), \\ &. \\ &. \\ d_i(k_0+N) &= Cx_i(k_0+N) + r + hv_i(k_0) \end{aligned} \tag{3-21}$$

Here, C = [1 0 0], And distance between the vehicle under $SystemA$ is given as:

$$\begin{aligned} d_i(k_0+N+1) &= Cx_i(k_0+N+1) + r + hv_i(k_0+N+1), \\ d_i(k_0+N+2) &= Cx_i(k_0+N+2) + r + hv_i(k_0+N+2), \\ &. \\ &. \\ d_i(k_0+N+P) &= Cx_i(k_0+N+P) + r + hv_i(k_0+N+P) \end{aligned} \tag{3-22}$$

Whenever, d_i is found to be less than 0, it implies there is a collision.

3-3-2 Hot standby

TNO in its EcoTwin III projects has adopted hot standby strategy. As mentioned earlier, the hot standby is used to provide much faster recovery time. Which means that the standby ECU is not only powered up but also experiences the complete operational load like the primary ECU. It computes the control input u_i for the vehicle i in parallel to the primary ECU. Figure 3-7 shows the signal diagram during primary ECU failure. In the Figure 3-7, it can be seen that once the command is generated from the health monitor, the arbiter switches to the standby ECU.

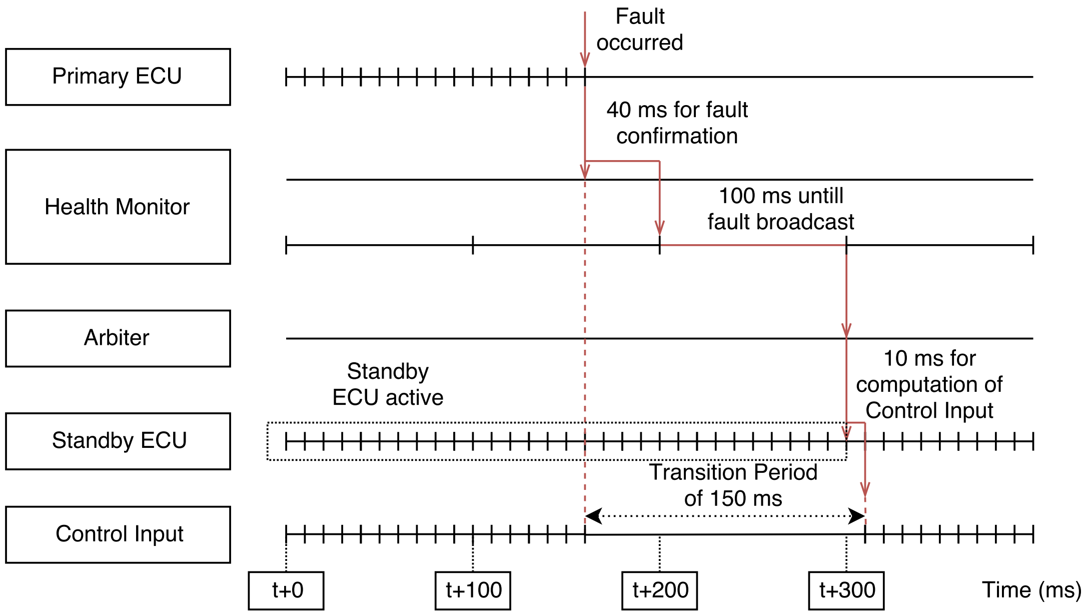


Figure 3-7: Signal diagram during primary ECU failure under hot standby where standby ECU produces output in parallel to the primary ECU.

In comparison to Figure 3-5, Figure 3-7 shows that the secondary ECU is generating the control input in parallel to primary ECU but due to the limitation in switching mechanism by health monitor and arbiter, the control input u_i is unavailable during the transition period of 150 ms for the lower-level controller. This again limits the performance of the fault tolerance system. However, one benefit of using hot standby is that, as the secondary ECU has already been generating the control input u_i in parallel to the primary ECU, the magnitude of the control input u_i available after switching is not affected by the inverse spacing policy $(1/H)$. This can be seen in Figure 3-8 that after transition period, the magnitude of control input u_i is higher (-3.79) compared to the control input generated in warm standby shown in Figure 3-6. Because of this the control input u_i reaches the maximum control law sooner, enabling the lower-level controller to act fast.

The evaluation of the states x_i, control input u_i and dynamics of the vehicle i during the transition period is same as in Equation 3-17 during transition duration, where the initial conditions are all the same. One thing is different and that is the calculation of u_i, when $System : a$ switches back from $System : b$, the initial control input for $System : a$ is $u_i(k_0 + N) \neq 0$. However, during the transition duration, the inter-vehicle distance d_i is same as Equation 3-21, but the Equation 3-22 gives a safer distance due to the availability of control input with larger magnitude.

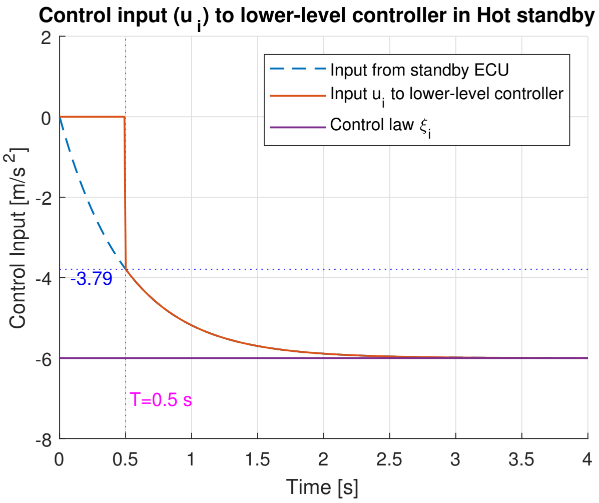


Figure 3-8: Control input in hot standby

Since, it can be observed that both the warm and hot standby suffers from the transition period as there is still no control input u_i present in that period. Hence, a new methodology of implementation is proposed which utilizes feedforward signal for generating control input u_i during transition period in the same hardware combination.

3-4 Proposed CACC Implementation

As mentioned earlier in the existing implementation, the primary ECU receives the sensor data along with preceding vehicle's intended acceleration u_{i-1} and performs all the processing and calculations to generate the desired control input u_i, given by the Equation 2-14. And this control input u_i is used by the lower-level controller to calculate the desired throttle angle and brake pressure explained in the section 2-1-2. For convenience lets call the primary ECU as ECU:1, standby ECU as ECU:4 and ECU on which lower-level controller is present be called as ECU:2. The proposed methodology suggests the following changes:

- The ECU:1 and ECU:4 receive only sensor values and output ξ_i.
- The communicated data about the intended acceleration u_{i-1} of the vehicle $i-1$ is fed directly to the ECU:2.
- The calculation of u_i is done at the Control input calculator running on the ECU:2. The desired control input u_i looks the same compared to warm and hot standby mode except it is calculated in a distributed manner as shown in Figure 3-9.

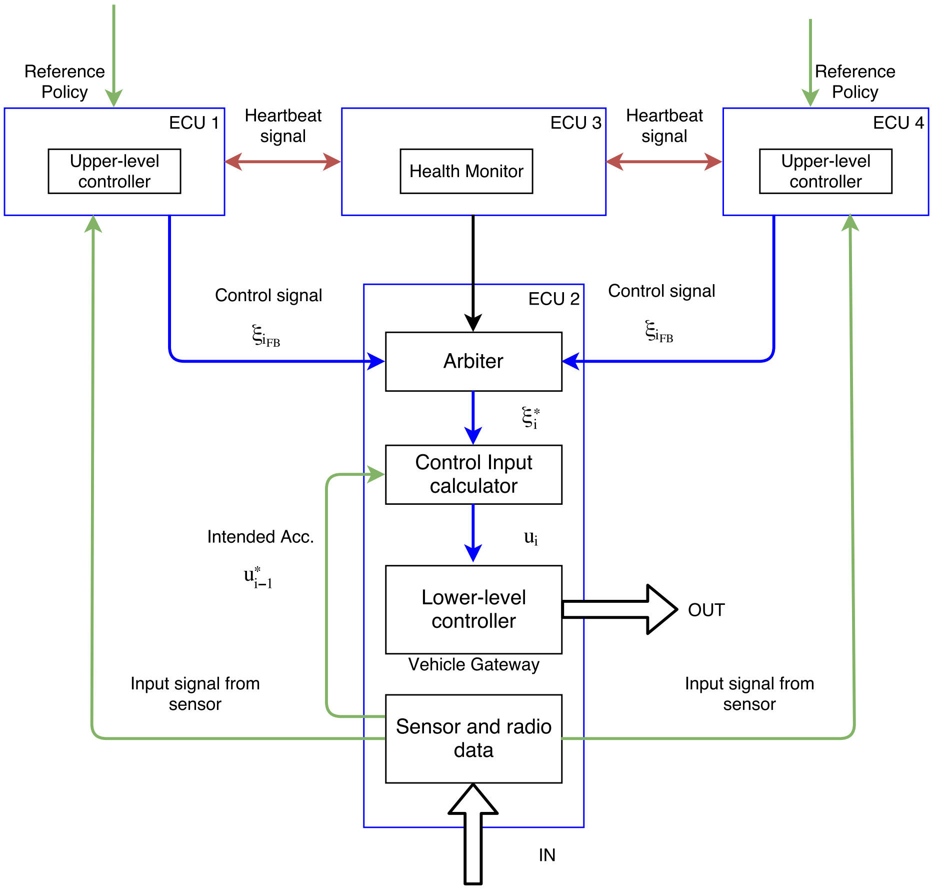


Figure 3-9: Schematic diagram of the proposed method.

In this, ξ is bifurcated into two parts i.e. a feedback (FB) part and a (FF) part.

$$\xi_i^* = \xi_{i_{FB}} + \xi_{i_{FF}} \tag{3-23}$$

The FB part is calculated in both primary and standby ECU and is given as:

$$\xi_{i_{FB}} = \underbrace{K \begin{pmatrix} e_{1,i} \\ e_{2,i} \\ e_{3,i} \end{pmatrix}}_{Feedback} \tag{3-24}$$

The FF part is the intended acceleration communicated via wireless radio and is given as:

$$\xi_{i_{FF}} = u_{i-1}^* \tag{3-25}$$

The system equation during transition duration is given in discrete time using Equation 3-14 as:

$$System : a^* \Rightarrow x_i(k_0+1) = Ax_i(k_0) + B_1\xi_i^*(k_0) + B_2u_{i-1}(k_0) \tag{3-26}$$

In transition duration $\xi_{i_{FB}} = 0$, $\xi_i^* = \xi_{i_{FF}}$ and the evaluation of the states are given as:

$$\begin{aligned}
x_i(k_0+1) &= Ax_i(k_0) + B_1\xi_{i_{FF}}(k_0) + B_2u_{i-1}(k_0) \\
x_i(k_0+2) &= Ax_i(k_0+1) + B_1\xi_{i_{FF}}(k_0+1) + B_2u_{i-1}(k_0+1) \\
&= A[Ax_i(k_0) + B_1\xi_{i_{FF}}(k_0) + B_2u_{i-1}(k_0)] \\
&+ B_1\xi_{i_{FF}}(k_0+1) + B_2u_{i-1}(k_0+1) \\
&= A^2x_i(k_0) + AB_1\xi_{i_{FF}}(k_0) + AB_2u_{i-1}(k_0) \\
&+ B_1\xi_{i_{FF}}(k_0+1) + B_2u_{i-1}(k_0+1) \\
x_i(k_0+3) &= A^2x_i(k_0+1) + AB_1\xi_{i_{FF}}(k_0+1) + AB_2u_{i-1}(k_0+1) \\
&+ B_1\xi_{i_{FF}}(k_0+2) + B_2u_{i-1}(k_0+2) \\
&= A^2[Ax_i(k_0) + B_1\xi_{i_{FF}}(k_0) + B_2u_{i-1}(k_0)] + AB_1\xi_{i_{FF}}(k_0+1) \\
&+ AB_2u_{i-1}(k_0+1) + B_1\xi_{i_{FF}}(k_0+2) + B_2u_{i-1}(k_0+2) \\
&= A^3x_i(k_0) + A^2B_1\xi_{i_{FF}}(k_0) + A^2B_2u_{i-1}(k_0) + AB_1\xi_{i_{FF}}(k_0+1) \\
&+ AB_2u_{i-1}(k_0+1) + B_1\xi_{i_{FF}}(k_0+2) + B_2u_{i-1}(k_0+2) \\
&. \\
&. \\
&. \\
x_i(k_0+N) &= A^{N-k_0}x_i(k_0) + \sum_{m=k_0}^{N-1} A^{N-m-1}[B_1\xi_{i_{FF}}(m) + B_2u_{i-1}(m)]
\end{aligned} \tag{3-27}$$

During the transition period, the control input u_i is calculated using Equation 2-14:

$$\begin{aligned}
u_i(k_0+1) &= -\frac{1}{h}u_i(k_0) + \frac{1}{h}\xi_{i_{FF}}(k_0+1) \\
&. \\
&. \\
u_i(k_0+N) &= -\frac{1}{h^{N-k_0}}u_i(k_0) + \sum_{m=k_0}^{N-1} \frac{1}{h^{N-m-1}}\xi_{i_{FF}}(m)
\end{aligned} \tag{3-28}$$

Here, N represents the number of samples corresponding to the transition duration. Using Equation 3-28 in the vehicle model given by Equation 2-8, the dynamics of the vehicle i is obtained. After N samples, as the standby ECU switches, and the initial states for the $System : a$ are the final states of $System : a^*$. The evolution of states when the standby

ECU switches are given as following:

$$\begin{aligned}
x_i(k_0+N+1) &= Ax_i(k_0+N) + B_1\xi_i^*(k_0+N) + B_2u_{i-1}(k_0+N) \\
x_i(k_0+N+2) &= Ax_i(k_0+N+1) + B_1\xi_i^*(k_0+N+1) + B_2u_{i-1}(k_0+N+1) \\
&= A[Ax_i(k_0+N) + B_1\xi_i^*(k_0+N) + B_2u_{i-1}(k_0+N)] \\
&+ B_1\xi_i^*(k_0+N+1) + B_2u_{i-1}(k_0+N+1) \\
&= A^2x_i(k_0+N) + AB_1\xi_i^*(k_0+N) + AB_2u_{i-1}(k_0+N) \\
&+ B_1\xi_i^*(k_0+N+1) + B_2u_{i-1}(k_0+N+1) \\
x_i(k_0+N+3) &= A^2x_i(k_0+N+1) + AB_1\xi_i^*(k_0+N+1) + AB_2u_{i-1}(k_0+N+1) \\
&+ B_1\xi_i^*(k_0+N+2) + B_2u_{i-1}(k_0+N+2) \\
&= A^2[Ax_i(k_0+N) + B_1\xi_i^*(k_0+N) + B_2u_{i-1}(k_0+N)] + AB_1\xi_i^*(k_0+N+1) \\
&+ AB_2u_{i-1}(k_0+N+1) + B_1\xi_i^*(k+2) + B_2u_{i-1}(k+2) \\
&= A^3x_i(k_0+N) + A^2B_1\xi_i^*(k_0+N) + A^2B_2u_{i-1}(k_0+N) + AB_1\xi_i^*(k_0+N+1) \\
&+ AB_2u_{i-1}(k_0+N+1) + B_1\xi_i^*(k_0+N+2) + B_2u_{i-1}(k_0+N+2) \\
&. \\
&. \\
&. \\
x_i(k_0+N+P) &= A^{P-(k_0+N)}x_i(k_0+N) + \sum_{o=k_0+N}^{P-1} A^{P-o-1}[B_1\xi_i^*(o) + B_2u_{i-1}(o)]
\end{aligned} \tag{3-29}$$

Using this methodology one can assure the presence of control input even during the transition time. And when the standby ECU kicks in, the control input u_i is given as:

$$\begin{aligned}
u_i(k_0+N+1) &= -\frac{1}{h}u_i(k_0+N) + \frac{1}{h}\xi_i^*(k_0+N+1) \\
&. \\
&. \\
u_i(k_0+N+P) &= -\frac{1}{h^{P-(k_0+N)}}u_i(k_0+N) + \sum_{o=k_0+N}^{P-1} \frac{1}{h^{P-o-1}}\xi_i^*(o)
\end{aligned} \tag{3-30}$$

The control input given in Equation 3-30 is used to compute the dynamics of the vehicle i using Equation 2-8. Here P correspond to the number of samples since the activation time of $System : a$ until the vehicle i comes to standstill. A platoon is said to be safe only when the inter-vehicle distance $d_i > 0$. Hence, the inter-vehicle distance d_i is checked at every sample. During the transition period, the feedforward signal is available for the lower-level controller and the velocity of the vehicle i decreases. The inter-vehicle distance d_i under transition duration is given as:

$$\begin{aligned} d_i(k_0+1) &= Cx_i(k_0+1) + r + hv_i(k_0+1), \\ d_i(k_0+2) &= Cx_i(k_0+2) + r + hv_i(k_0+2), \\ &. \\ &. \\ &. \\ d_i(k_0+N) &= Cx_i(k_0+N) + r + hv_i(k_0+N) \end{aligned} \tag{3-31}$$

The inter-vehicle distance after the standby ECU kicks in is given as:

$$\begin{aligned} d_i(k_0+N+1) &= Cx_i(k_0+N+1) + r + hv_i(k_0+N+1), \\ d_i(k_0+N+2) &= Cx_i(k_0+N+2) + r + hv_i(k_0+N+2), \\ &. \\ &. \\ &. \\ d_i(k_0+N+P) &= Cx_i(k_0+N+P) + r + hv_i(k_0+N+P) \end{aligned} \tag{3-32}$$

Here, $C = [1\ 0\ 0]$ are represented in discrete time and whenever d_i is found less than 0, it implies there is a collision.

3-5 Summary

In this chapter, The worst case scenario has been defined to analyze the performance of the fault-tolerance system. TNO's implemented system has a maximum transition period of 150 ms during which the control input u_i is 0 for the lower-level controller. Because of that the speed of the vehicle i does not change to track the desired inter-vehicle distance. Under the warm standby mode, the control input u_i is computed only after the command generated by the health monitor. In the hot standby mode which TNO has implemented, the standby ECU calculates the control input u_i in parallel to the primary ECU. Both the standby strategies suffer from the transition period where there is no control input for the lower-level controller. However, the control input in hot standby mode is less affected by the inverse policy $1/H$ which causes a delay in letting the control input u_i reach its maximum value. To reject the effect of transition duration on the vehicle, a new implementation strategy is proposed which uses the feedforward signal directly to compute the control input u_i which allows the lower-level controller to generate the desired action on the vehicle motion.

Chapter 4

Simulations and Results

The effect of loss of ECU and the response of fault-tolerant CACC systems are studied in this chapter using MATLAB simulations of a platoon of 2 vehicles (including lead vehicle). For this, plots and tables containing time to collision have been obtained. Tables 4-1 to 4-14 contain time to collision in seconds for combinations of parameters under which collision occurs ($d_i \leq 0$).
The Section 4-1 describes the simulation setup, Section 4-2 shows the effect of the worst-case scenario on the follower vehicle, Section 4-3 presents the response of the fault-tolerant CACC strategies. Finally, Section 4-4 concludes this chapter.

4-1 Simulation Setup

This section defines the assumptions and parameters considered for the analysis of the fault-tolerance design.

4-1-1 Assumptions

- The simulations are done for two vehicles (1 lead and 1 follower).
- The loss of control input due to ECU failure is only considered for vehicle i.
- Before the ECU failure, the platoon is at steady state which means the desired distance $d_{r,i}$ between the vehicles is equal to the actual distance d_i between the vehicles.
- The intended acceleration of the lead vehicle changes as described in Subsection 3-2-1 and a_{min} is the minimum acceleration value:

$$u_{i-1} = \{a_{min}, 0\} \tag{4-1}$$

- Saturation limits have been used in the control input, to keep the control input in the feasible range *i.e.* $max(u_i) = max(u_{i-1})$.

4-1-2 Parameters

- The drive-line constant in the vehicle model has been chosen to be $\tau = 0.1$.
- The parameters of the controller $K = [k_p \quad k_d \quad k_{dd}] = [0.2 \quad 0.7 \quad 0]$ have been chosen from [33] for all simulations.
- The initial error states, given by the Equation 3-16, are:

$$x_i = [0 \quad 0 \quad 0]^T. \tag{4-2}$$

- The headway time h considered when we obtained plots and tables:

	Plot	Time to collision table (4-1 to 4-14)
h (s)	0.3	0.3, 0.5

- The standstill distance r considered when we obtained plots and tables:

	Plot	Time to collision table (4-1 to 4-14)
r (m)	3	2, 3, 4, 5

- The steady state velocity (v_i and v_{i-1}) before worst case scenario is considered when we obtained plots and tables:

	Plot	Time to collision table (4-1 to 4-14)
v_i and v_{i-1} (km/h)	80	50, 60, 70, 80, 90, 100

- The minimum intended acceleration a_{min} is considered when we obtained plots and tables:

	Plot	Time to collision table (4-1 to 4-14)
a_{min} (m/s^2)	-6	-6, -7, -8, -9

- The sampling rate has been considered to be 0.01 s which is the case in the TNO implemented ECU.

4-2 Worst case scenario

As mentioned in the previous chapter, the worst case scenario is given as:

- The ECU containing upper-level controller fails.
- At the same instance of ECU failure, the preceding vehicle brakes with its maximum deceleration and finally comes to a standstill.

In the simulations, the platoon safety is studied by applying the worst case scenario. The following subsections present the vehicle safety with and without ECU failure.

4-2-1 Emergency braking without the ECU failure

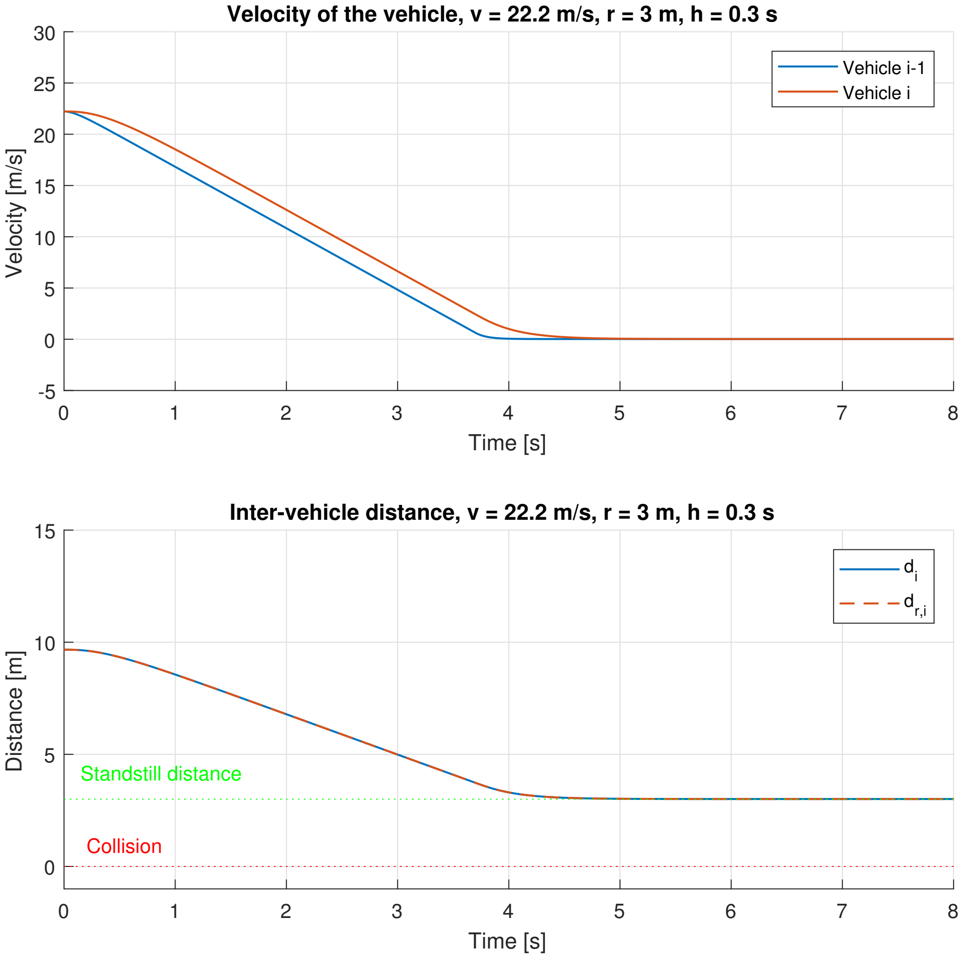


Figure 4-1: Fault free ECU, Top: Velocity of the vehicle $i-1$ and vehicle i. Bottom: inter-vehicle distance d_i and reference policy $d_{r,i}$

In Figure 4-1, a simulation has been carried out without the ECU failure to see the effect of the string stable controller, when the preceding vehicle brakes with an intended acceleration $u_{i-1} = [-6 \quad 0]$, the initial steady state speed $v_i = 80 \quad km/h$, stand still distance $r = 3 \quad m$ and headway time $h = 0.3 \quad s$. It can be seen that the distance between the vehicles follows the desired spacing policy and settles at the standstill distance which is shown with a green line. The inter-vehicle distance d_i never touches or crosses the red line which represents a collision. Figure 4-2, shows the affect of control input to the acceleration of the vehicles. It can be observed that the control input to the vehicle i is computed accordingly as soon as the vehicle $i-1$ applies brake or u_{i-1}.

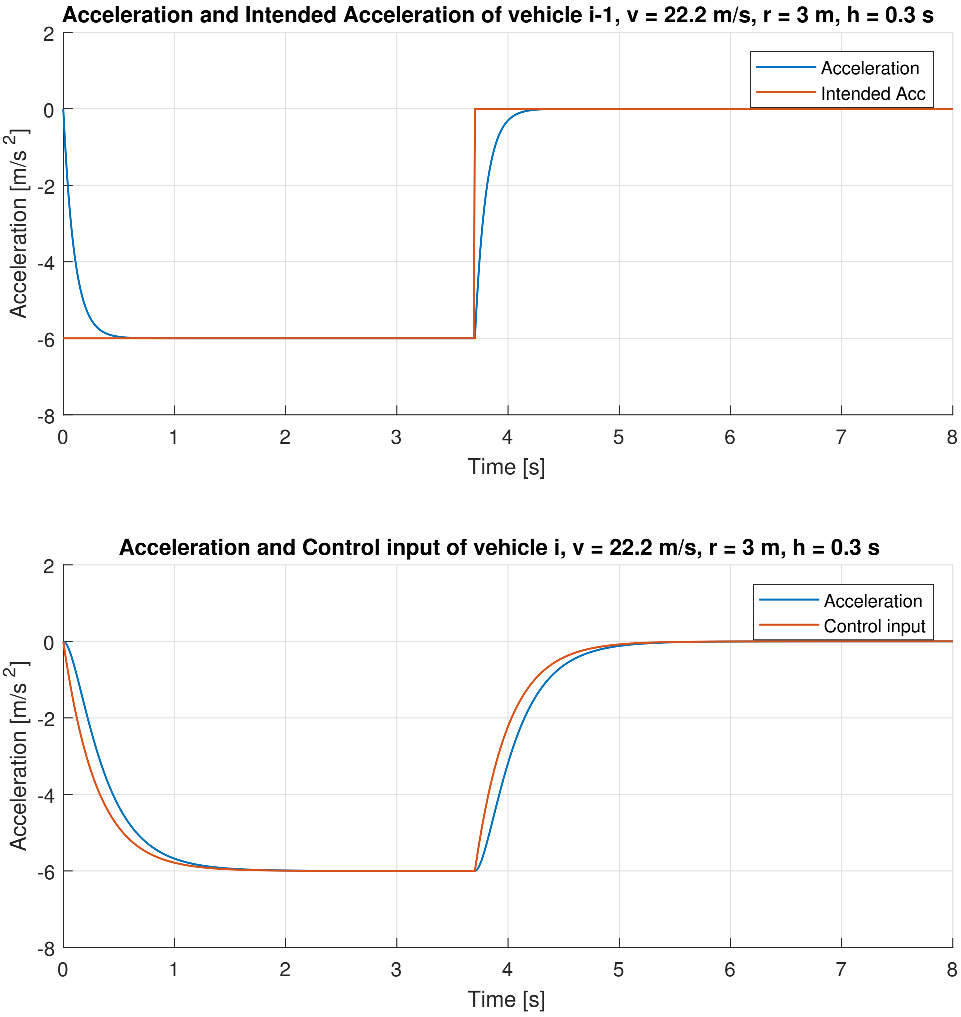


Figure 4-2: Fault free ECU, Top: input and acceleration of vehicle $i-1$. Bottom: control input and acceleration of vehicle i

This subsection explains that when the ECU of vehicle i is healthy and vehicle $i-1$ brakes with its maximum deceleration value, vehicle i was able to track the reference policy perfectly and no collision was observed.

4-2-2 Emergency braking with ECU failure

In the Figure 4-3, a simulation has been carried out with ECU failure to see the effect of the string stable controller, when the preceding vehicle brakes with an intended acceleration $u_{i-1} = [-6 \quad 0]$, the initial steady-state speed $v_i = 80 \quad km/h$, stand still distance $r = 3 \quad m$, headway time $h = 0.3 \quad s$. It can be seen that the distance between the vehicles decreases rapidly and reaches the collision line represented as the red line which means that the vehicle

i collides with the vehicle $i-1$ way before the preceding vehicle comes to a standstill.

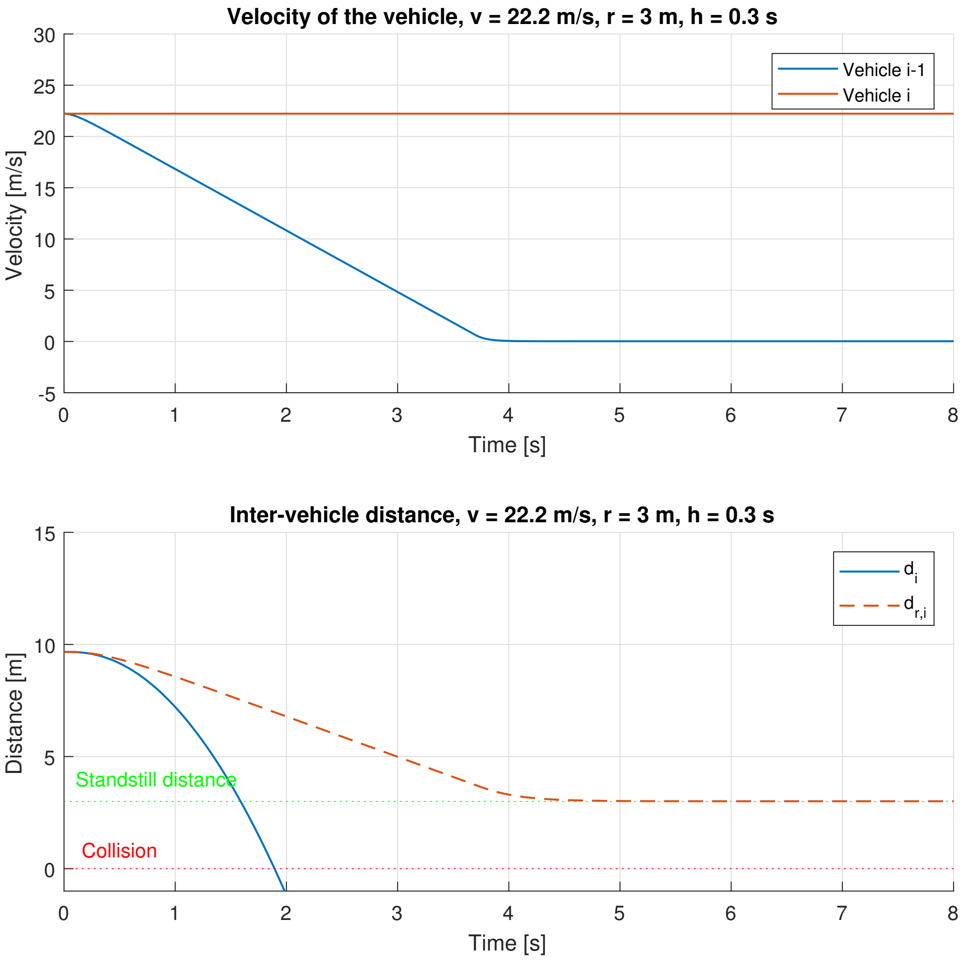


Figure 4-3: Faulty ECU, Top: velocity of vehicle $i-1$ and i. Bottom: inter-vehicle distance d_i and the reference policy $d_{r,i}$

From Figure 4-4, it can be observed that the control input to vehicle i is never computed and remains 0 (assuming the failure of ECU is fail-silent and outputs 0), which keeps the acceleration of vehicle i also to 0. Due to this, the velocity of the vehicle i does not decrease to avoid collision with vehicle $i-1$. One could also conclude that a collision is inevitable under the defined worst case scenario.

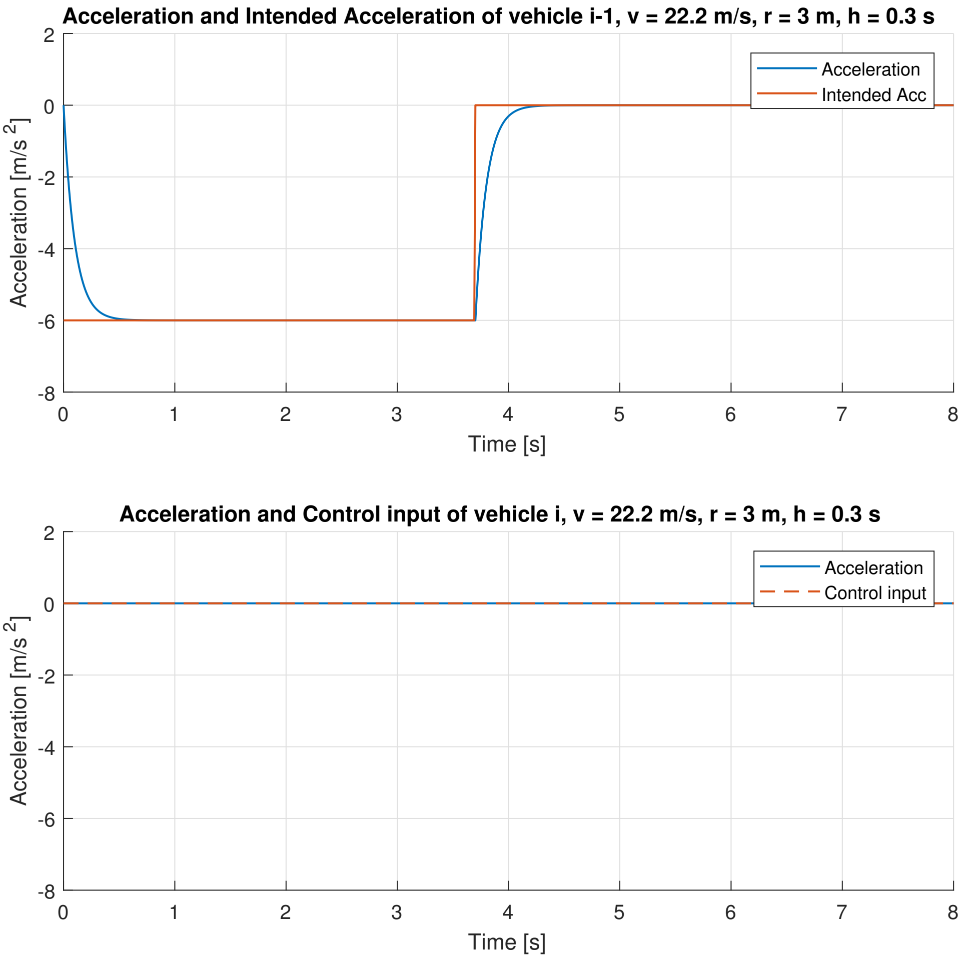


Figure 4-4: Faulty ECU, Top: input and acceleration of vehicle $i-1$. Bottom: control input and acceleration of vehicle i

This subsection explains that when the ECU of vehicle i fails and vehicle $i-1$ brakes with its maximum deceleration value, vehicle i collided with vehicle $i-1$. In the next section, simulations are carried out to see the fault-tolerant system during ECU failure.

4-3 Fault tolerant CACC strategy

The implementation of Fault tolerant CACC system has been discussed in the previous chapter and two types of standby philosophies are mentioned *i.e.* warm standby and hot standby. In both the types, there exists a transition period due to the time spent on fault detection and switching of the healthy ECU with the faulty one. In the following subsections, extensive simulations are carried out and time to collision tables are also included.

4-3-1 Warm standby

This subsection presents the simulations and results when the implementation of fault-tolerance system is under warm standby mode. As presented earlier, the control input for vehicle i by the secondary ECU is computed only after a command is generated by the Health monitor (after the transition period).
We simulate for different transition period values $T = [0.02, 0.04, 0.06, 0.10, 0.15, 0.22, 0.28]$ s, at fixed headway time $h = 0.3$ s, initial velocity $v_i = 80$ km/h and stand still distance $r = 3$ m.

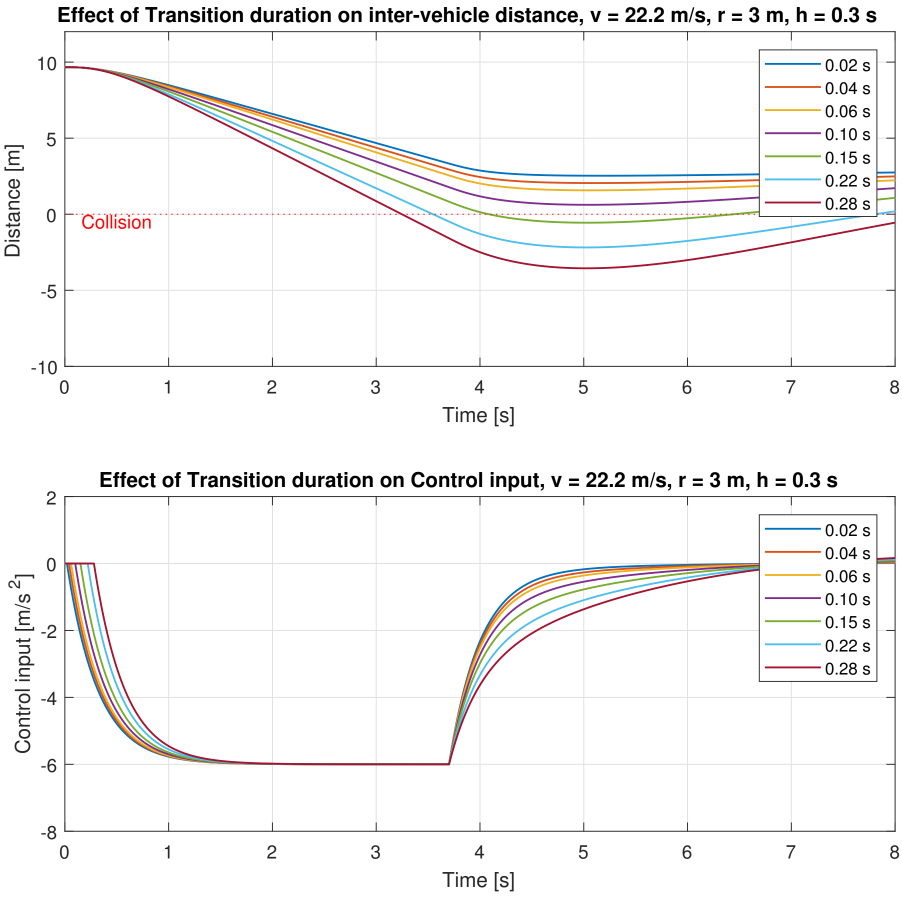


Figure 4-5: Warm standby, Top: inter-vehicle distance d_i in the presence of different transition durations. Bottom: control input that is generated for vehicle i after switching from faulty ECU to a healthy one incorporating the transition duration.

We can see from the Figure 4-5 that for certain transition durations (T = 0.15 s, 0.22 s, 0.28 s), the distance between the vehicles $i - 1$ and i is less than zero, which implies that the vehicle $i - 1$ and i have met with a collision. In Figure 4-5 we can also see how the control input evolves after the transition duration. This gives a very interesting result, because of the spacing policy filter, the control input u_i takes time to reach its maximum deceleration value. Larger transition duration means that the more time the vehicle i remains at its initial speed and gives less time for the control input u_i to act on the vehicle to reduce its speed. To further visualize the evolution of control input, we simulate for a fixed transition duration $T = 0.15$ s, headway time $h = 0.3$ s, standstill distance $r = 3$ m, initial velocity v_i,v_{i-1} = 80 km/h and lead vehicle deceleration u_{i-1} = -6 m/s^2. In Figure 4-6, it can be seen that the control input is generated after the transition period. Due to the inverse spacing policy $(1/H)$, the control input undergoes a delay to reach its maximum value which causes a slow reaction on the vehicle i acceleration and hence velocity. Next, it can be seen that the distance between the vehicle is crossing zero, this implies a collision which is not the case when T = 0 s.

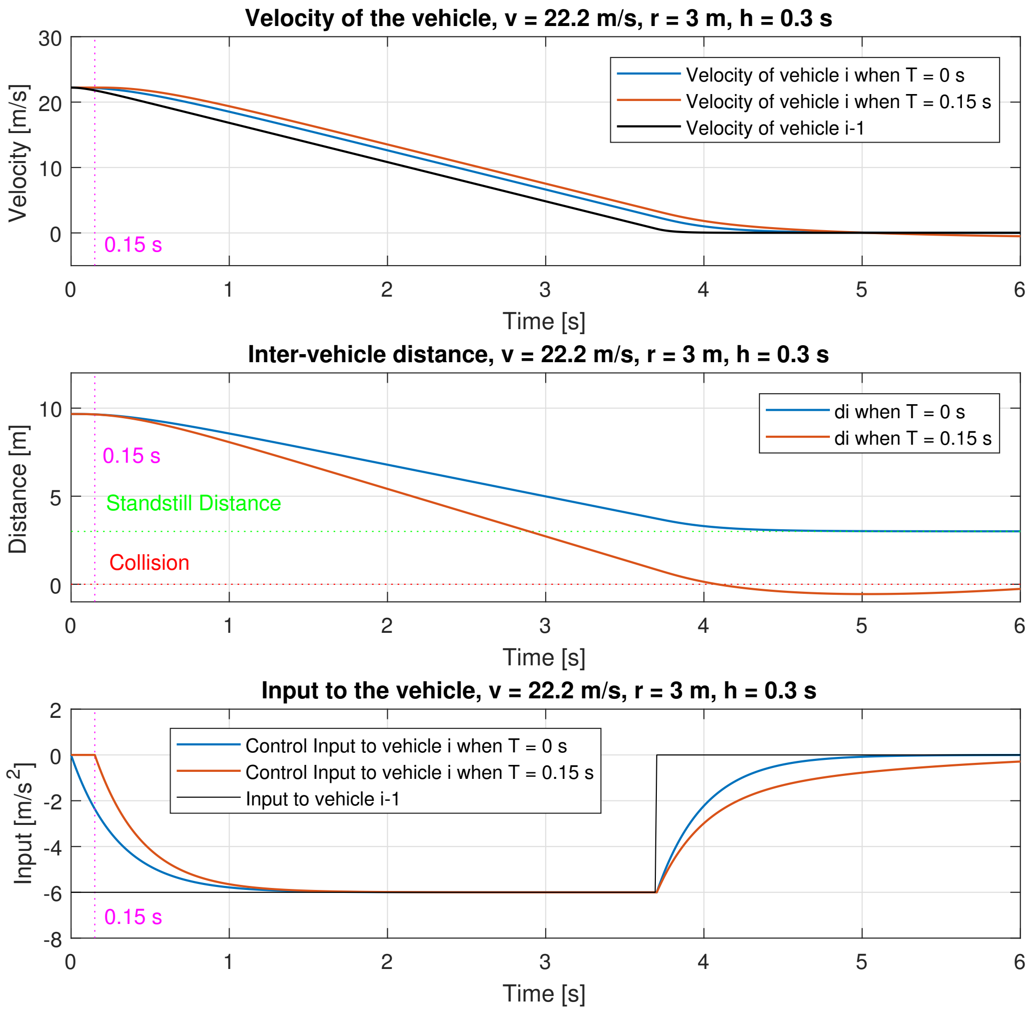


Figure 4-6: Top: Velocity of the vehicle $i-1$ and vehicle i with and without transition duration. Middle: The distance d_i between the vehicles $i-1$ and i with and without transition duration. Bottom: The input to the vehicle $i-1$ and the control input to the vehicle i with and without transition duration.

Figure 4-6 shows, that the value of transition period is critical to the safety of the vehicle i. As mentioned earlier, that the maximum transition duration in the TNO implemented system is 0.15 s, then under warm standby mode safety is compromised. Hence, simulations were carried out with operable parameters to find the range of transition period under which warm standby is safe.
In Table 4-1 to 4-6, time to collision in seconds has been presented for the different parameter. Here, nc means no collision, T is the transition period in seconds, v is the initial velocity in km/h, r is the standstill distance between the vehicles $i-1$ and i, h is the headway time in seconds and u_{i-1} is the lead vehicle deceleration value in m/s^2. A total of 200 combinations are presented in every table. Finally, collision percentage is calculated based on the number of appearances of time to collision out of the total number of combinations (200) present in the Tables.

$$Collision\% = \frac{Number \quad of \quad time \quad to \quad collisions}{Total \quad number \quad of \quad combinations(200)} \times 100 \tag{4-3}$$

Table Observations

Following observations were made from the Table 4-1 to 4-6:

- There are no collisions when the transition period is in the range (0-0.9) s.
- For transition duration 0.15s which is considered to be highest in the current hardware implementation, collisions are observed.

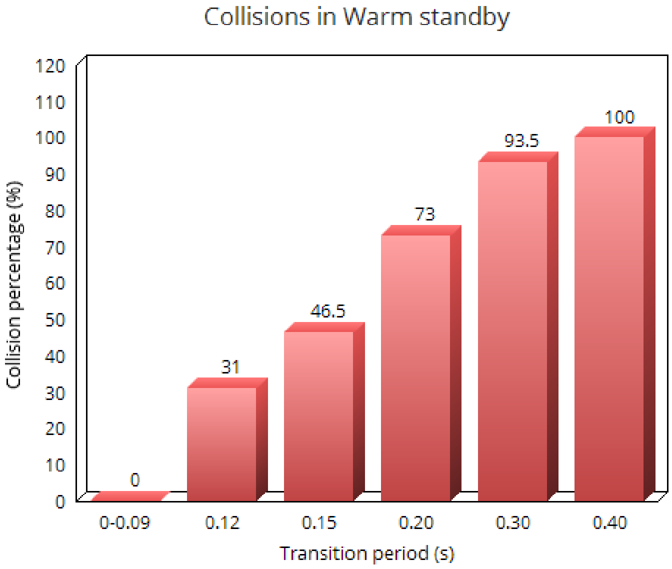


Figure 4-7: Chart representing collision percentage for different transition period in warm standby

Table 4-1: Time to collision when transition period is in the range [0, 0.09] s in warm standby mode

T	v (km/h)	h = 0.3 s															
		r = 2 m				r = 3 m				r = 4 m				r = 5 m			
0 - 0.09 s	50	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc
	60	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc
	70	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc
	80	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc
	90	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc
	100	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc
		h = 0.5 s															
0 - 0.09 s	50	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc
	60	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc
	70	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc
	80	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc
	90	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc
	100	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc
u_{i-1} (m/s^2)		-6	-7	-8	-9	-6	-7	-8	-9	-6	-7	-8	-9	-6	-7	-8	-9

Table 4-2: Time to collision when transition period is 0.12 s in warm standby mode

T	v (km/h)	h = 0.3															
		r = 2				r = 3				r = 4				r = 5			
0.12	50	nc	3.33	2.90	2.59	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc
	60	3.47	3.05	2.75	2.51	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc
	70	3.60	3.18	2.85	2.60	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc
	80	3.87	3.39	3.04	2.76	nc	nc	nc	3.67	nc	nc	nc	nc	nc	nc	nc	nc
	90	4.19	3.66	3.26	2.95	4.88	4.26	3.81	3.47	nc	nc	nc	nc	nc	nc	nc	nc
	100	4.52	3.94	3.50	3.16	5.00	4.37	3.89	3.54	nc	nc	nc	nc	nc	nc	nc	nc
		h = 0.5															
0.12	50	nc	nc	3.60	3.15	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc
	60	4.03	3.57	3.27	3.01	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc
	70	4.07	3.66	3.32	3.07	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc
	80	4.30	3.83	3.48	3.21	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc
	90	4.59	4.06	3.67	3.37	5.59	4.85	4.39	4.03	nc	nc	nc	nc	nc	nc	nc	nc
	100	4.92	4.33	3.89	3.56	5.49	4.87	4.38	4.03	nc	nc	nc	nc	nc	nc	nc	nc
u_{i-1} (m/s^2)		-6	-7	-8	-9	-6	-7	-8	-9	-6	-7	-8	-9	-6	-7	-8	-9

Table 4-3: Time to collision when transition period is 0.15 s in warm standby mode

T	v (km/h)	h = 0.3 s															
		r = 2 m				r = 3 m				r = 4 m				r = 5 m			
0.15 s	50	2.9	2.58	2.34	2.15	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc
	60	3.07	2.71	2.45	2.24	nc	nc	nc	3.09	nc	nc	nc	nc	nc	nc	nc	nc
	70	3.34	2.93	2.63	2.4	4.03	3.56	3.17	2.89	nc	nc	nc	nc	nc	nc	nc	nc
	80	3.65	3.19	2.85	2.58	4.1	3.6	3.23	2.94	nc	nc	nc	nc	nc	nc	nc	nc
	90	3.96	3.46	3.08	2.79	4.34	3.79	3.39	3.07	nc	4.69	4.13	3.72	nc	nc	nc	nc
	100	4.27	3.72	3.31	2.99	4.64	4.04	3.59	3.25	5.16	4.52	4.03	3.66	nc	nc	nc	nc
		h = 0.5 s															
0.15 s	50	3.38	3.05	2.8	2.6	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc
	60	3.5	3.14	2.88	2.67	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc
	70	3.73	3.34	3.03	2.8	4.62	4.12	3.68	3.38	nc	nc	nc	nc	nc	nc	nc	nc
	80	4.03	3.57	3.24	2.98	4.56	4.06	3.7	3.41	nc	nc	nc	nc	nc	nc	nc	nc
	90	4.36	3.84	3.46	3.17	4.75	4.21	3.81	3.5	nc	nc	nc	4.44	nc	nc	nc	nc
	100	4.71	4.13	3.7	3.38	5.02	4.43	3.99	3.65	5.7	5.04	4.52	4.16	nc	nc	nc	nc
u_{i-1} (m/s^2)		-6	-7	-8	-9	-6	-7	-8	-9	-6	-7	-8	-9	-6	-7	-8	-9

Table 4-4: Time to collision when transition period is 0.2 s in warm standby mode

T	v (km/h)	h = 0.3 s															
		r = 2 m				r = 3 m				r = 4 m				r = 5 m			
0.2 s	50	2.53	2.24	2.03	1.87	3.24	2.85	2.57	2.34	nc	nc	nc	nc	nc	nc	nc	nc
	60	2.79	2.46	2.21	2.02	3.21	2.84	2.56	2.35	nc	nc	nc	3.15	nc	nc	nc	nc
	70	3.07	2.69	2.41	2.2	3.41	3	2.69	2.45	4.04	3.56	3.18	2.89	nc	nc	nc	nc
	80	3.34	2.93	2.62	2.38	3.68	3.22	2.87	2.61	4.07	3.58	3.21	2.92	nc	nc	nc	3.77
	90	3.62	3.17	2.83	2.57	3.95	3.45	3.08	2.79	4.29	3.75	3.35	3.04	4.87	4.26	3.81	3.46
	100	3.9	3.41	3.04	2.75	4.23	3.69	3.29	2.97	4.57	3.98	3.54	3.2	4.94	4.32	3.85	3.5
		h = 0.5 s															
0.2 s	50	2.91	2.63	2.42	2.25	3.77	3.32	3.02	2.77	nc	nc	nc	nc	nc	nc	nc	nc
	60	3.15	2.82	2.58	2.39	3.64	3.25	2.98	2.76	nc	nc	nc	nc	nc	nc	nc	nc
	70	3.44	3.06	2.77	2.55	3.79	3.39	3.08	2.84	4.59	4.08	3.65	3.34	nc	nc	nc	nc
	80	3.77	3.32	3	2.75	4.04	3.58	3.25	2.99	4.49	4	3.64	3.35	nc	nc	nc	nc
	90	4.1	3.6	3.23	2.95	4.34	3.82	3.44	3.15	4.67	4.13	3.74	3.43	5.47	4.77	4.3	3.94
	100	4.43	3.89	3.48	3.17	4.66	4.09	3.67	3.34	4.93	4.35	3.91	3.57	5.37	4.75	4.27	3.92
u_{i-1} (m/s^2)		-6	-7	-8	-9	-6	-7	-8	-9	-6	-7	-8	-9	-6	-7	-8	-9

Table 4-5: Time to collision when transition period is 0.3 s in warm standby mode

T	v (km/h)	h = 0.3 s															
		r = 2 m				r = 3 m				r = 4 m				r = 5 m			
0.3 s	50	2.2	1.96	1.77	1.63	2.49	2.21	2.01	1.85	2.91	2.59	2.35	2.16	nc	nc	3.1	2.73
	60	2.43	2.16	1.95	1.78	2.71	2.39	2.16	1.97	3.01	2.66	2.4	2.2	3.49	3.07	2.78	2.54
	70	2.67	2.35	2.12	1.94	2.94	2.59	2.33	2.13	3.22	2.83	2.54	2.32	3.53	3.11	2.8	2.56
	80	2.9	2.55	2.3	2.09	3.18	2.79	2.5	2.28	3.45	3.03	2.71	2.47	3.73	3.27	2.93	2.66
	90	3.13	2.75	2.47	2.25	3.41	2.99	2.68	2.43	3.68	3.23	2.89	2.62	3.96	3.47	3.09	2.8
	100	3.36	2.95	2.64	2.4	3.64	3.19	2.85	2.59	3.92	3.43	3.06	2.77	4.19	3.66	3.27	2.96
		h = 0.5 s															
0.3 s	50	2.54	2.29	2.1	1.95	2.83	2.56	2.35	2.19	3.3	2.97	2.73	2.53	nc	nc	nc	3.2
	60	2.82	2.51	2.29	2.11	3.05	2.73	2.49	2.3	3.36	3.01	2.76	2.55	3.93	3.48	3.17	2.93
	70	3.11	2.76	2.5	2.29	3.32	2.95	2.67	2.46	3.56	3.17	2.88	2.65	3.89	3.48	3.16	2.92
	80	3.4	3.01	2.72	2.49	3.61	3.19	2.87	2.63	3.82	3.38	3.05	2.8	4.07	3.61	3.27	3.01
	90	3.69	3.26	2.93	2.68	3.9	3.44	3.09	2.82	4.11	3.62	3.25	2.97	4.32	3.81	3.43	3.14
	100	3.98	3.51	3.15	2.88	4.19	3.69	3.31	3.02	4.4	3.87	3.47	3.15	4.61	4.04	3.63	3.31
u_{i-1} (m/s^2)		-6	-7	-8	-9	-6	-7	-8	-9	-6	-7	-8	-9	-6	-7	-8	-9

Table 4-6: Time to collision when transition period is 0.4 s in warm standby mode

T	v (km/h)	h = 0.3 s															
		r = 2 m				r = 3 m				r = 4 m				r = 5 m			
0.4 s	50	2	1.79	1.63	1.5	2.24	1.99	1.81	1.67	2.48	2.21	2.01	1.85	2.8	2.5	2.27	2.1
	60	2.2	1.96	1.78	1.64	2.43	2.16	1.96	1.8	2.67	2.37	2.14	1.96	2.91	2.58	2.33	2.14
	70	2.39	2.13	1.93	1.77	2.63	2.33	2.11	1.93	2.87	2.54	2.28	2.09	3.11	2.74	2.46	2.25
	80	2.59	2.3	2.08	1.9	2.83	2.5	2.26	2.06	3.07	2.71	2.43	2.22	3.31	2.91	2.61	2.38
	90	2.79	2.47	2.23	2.04	3.03	2.67	2.4	2.2	3.27	2.88	2.58	2.35	3.51	3.08	2.76	2.51
	100	2.99	2.64	2.37	2.17	3.23	2.84	2.55	2.33	3.47	3.05	2.73	2.49	3.7	3.25	2.91	2.65
		h = 0.5 s															
0.4 s	50	2.35	2.11	1.94	1.8	2.55	2.3	2.11	1.97	2.8	2.53	2.33	2.17	3.15	2.84	2.62	2.43
	60	2.61	2.34	2.13	1.97	2.8	2.5	2.28	2.11	3	2.68	2.45	2.27	3.24	2.9	2.66	2.46
	70	2.87	2.56	2.32	2.14	3.06	2.72	2.47	2.27	3.24	2.88	2.61	2.4	3.44	3.06	2.78	2.56
	80	3.13	2.78	2.52	2.31	3.32	2.94	2.66	2.44	3.5	3.1	2.8	2.57	3.69	3.26	2.94	2.7
	90	3.39	3	2.71	2.49	3.57	3.16	2.85	2.61	3.76	3.32	2.99	2.74	3.94	3.48	3.13	2.86
	100	3.65	3.22	2.91	2.66	3.83	3.38	3.05	2.79	4.02	3.54	3.19	2.91	4.2	3.7	3.33	3.03
u_{i-1} (m/s^2)		-6	-7	-8	-9	-6	-7	-8	-9	-6	-7	-8	-9	-6	-7	-8	-9

4-3-2 Hot Standby

This subsection presents the simulations and results under hot standby mode. As mentioned earlier, the control input for vehicle i by the secondary ECU is computed in parallel with the primary ECU but is available for the lower-level controller only after only after a command is generated by the Health monitor after the transition period.
Figure 4-8 shows the inter-vehicle distance d_i plots for a different transition period. Comparing with Figure 4-5, it can be seen that the performance of hot standby is better than the warm standby as a collision can be seen only at higher transition periods.

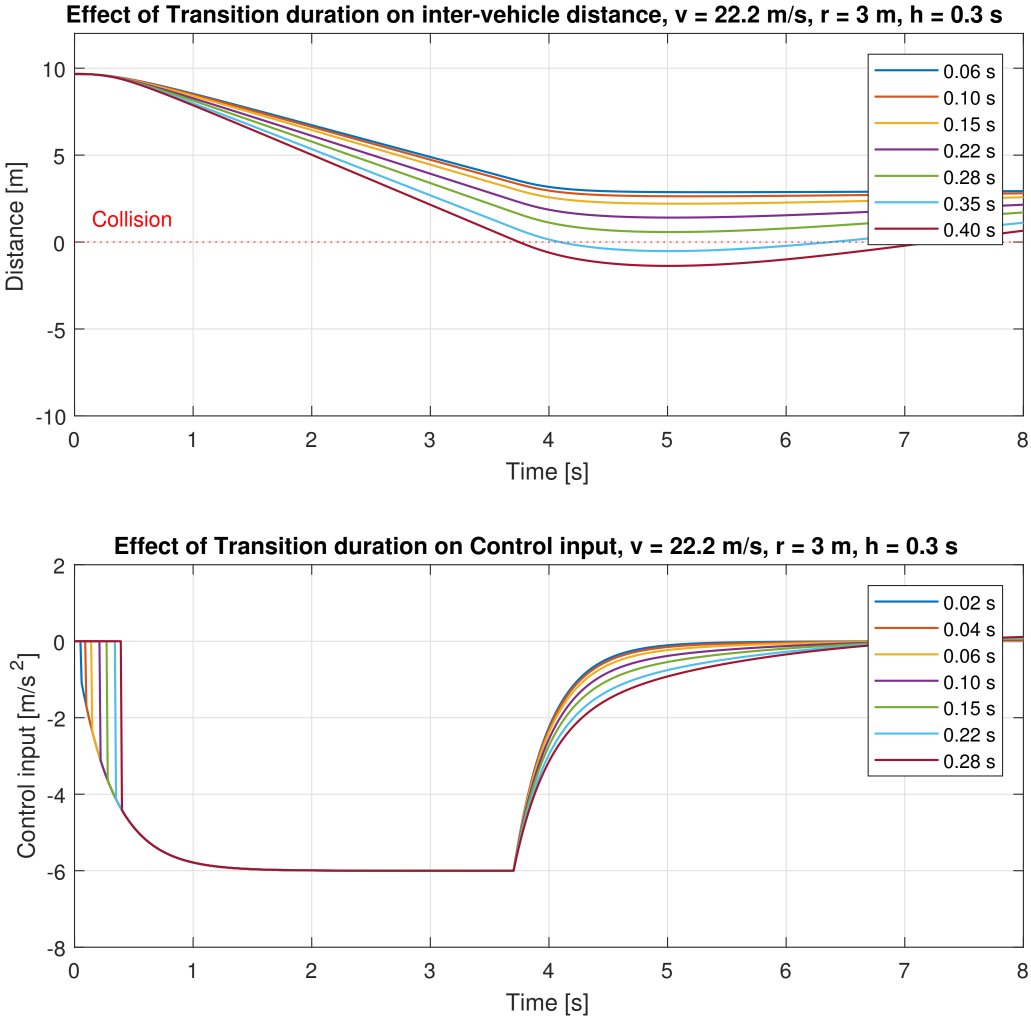


Figure 4-8: Hot standby, Top: inter-vehicle distance d_i in the presence of different transition durations. Bottom: control input that is generated for the vehicle i after switching from fault ECU to a healthy one incorporating the transition duration.

Next, it can be seen in Figure 4-9, that the control input u_i is available just after the transition period but in greater magnitude. This is because the secondary ECU computed the control input during the transition period. Hence the control input can change the velocity of vehicle i faster than in warm standby. It can also be seen that there is no collision between vehicle $i-1$ and i for transition period $T = 0.28s$ which is greater than the warm standby can handle.

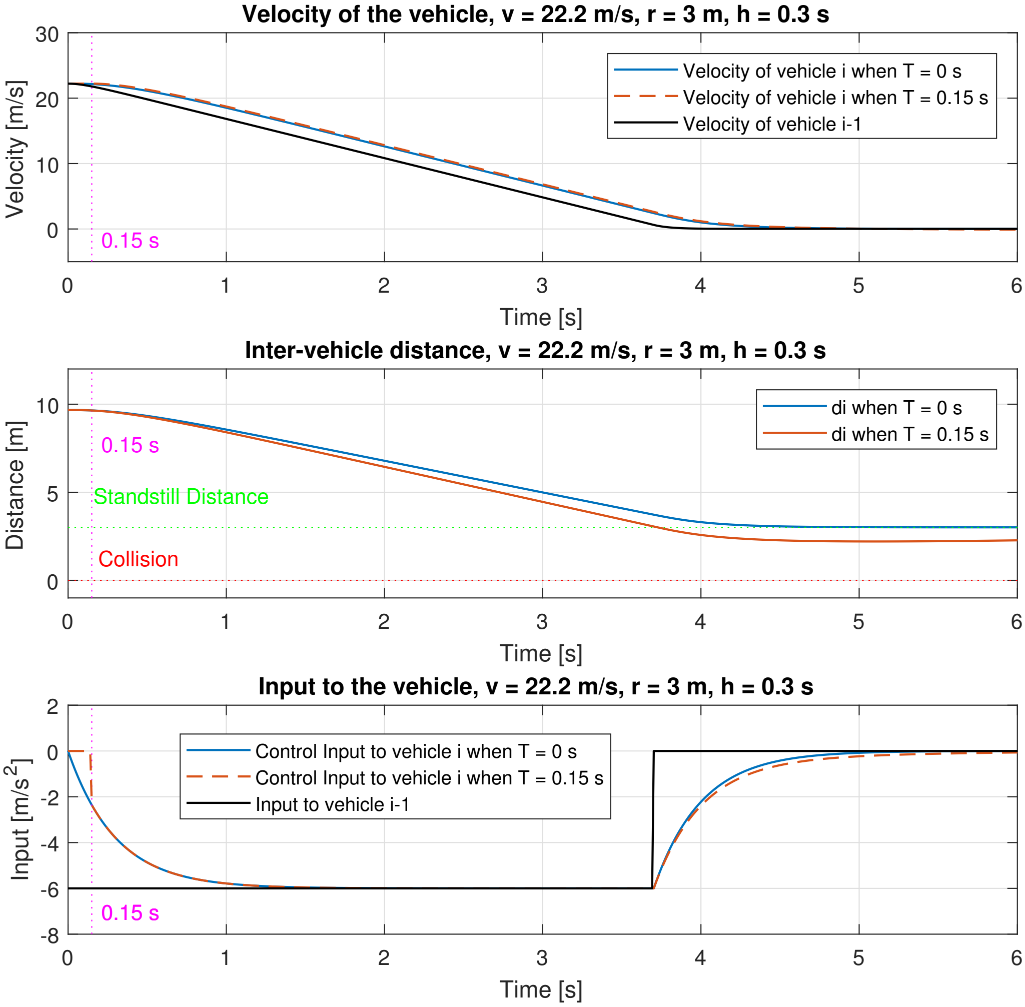


Figure 4-9: Hot standby when Transition period (T = 0.15 s) , Top: Velocity of the vehicle $i-1$ and vehicle i with and without transition duration. Middle: The inter-vehicle distance d_i with and without transition duration. Bottom: input to the vehicle $i-1$ and the control input to the vehicle i with and without transition period

As mentioned earlier, the maximum transition period considered in TNO implementation to be 0.15 s, then under hot standby mode there is no collision and the vehicles are safe.

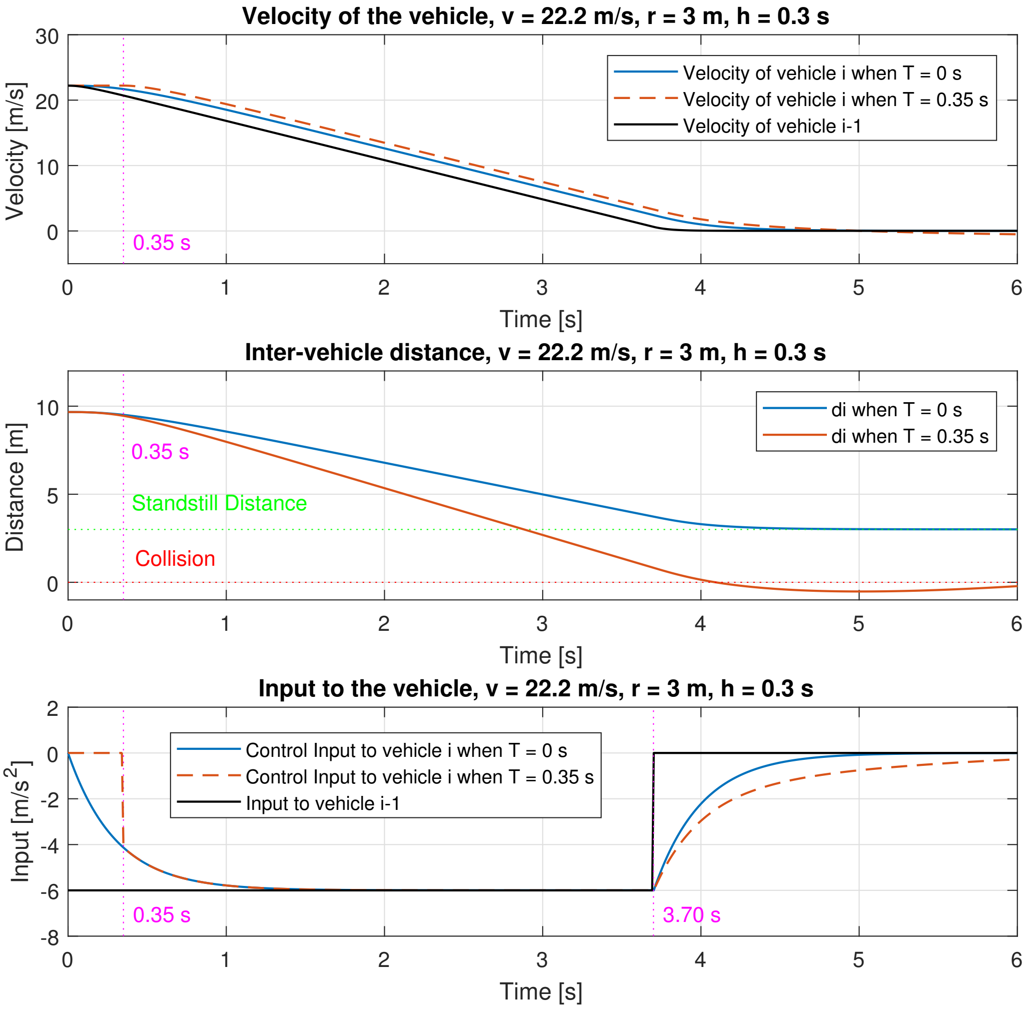


Figure 4-10: Hot standby when Transition period (T = 0.35 s) , Top: Velocity of the vehicle $i-1$ and vehicle i with and without transition duration. Middle: The inter-vehicle distance d_i with and without transition duration. Bottom: input to the vehicle $i-1$ and the control input to the vehicle i with and without transition period

Figure 4-10, presents an interesting result for a larger transition period T = 0.35 s, as there is a collision. Looking at the bottom plot explains that once the intended acceleration u_{i-1} becomes 0 at 3.70 s, the control law ξ_i after 3.70 s cannot generate the control input u_i at the maximum deceleration value. Due to this, the vehicle i could not be brought to a standstill before collision.

In Table 4-7 to 4-13, time to collision in seconds has been presented for the different parameter. Here, nc means no collision, T is the transition period in seconds, v is the initial velocity in km/h, r is the standstill distance between the vehicles $i-1$ and i, h is the headway time in seconds and u_{i-1} is the lead vehicle deceleration value in m/s^2. A total of 200 combinations are presented in every table. Finally, collision percentage is calculated based on the number of appearances of time to collision out of the total number of combinations (200) present in the Tables.

$$Collision\% = \frac{Number \quad of \quad time \quad to \quad collisions}{Total \quad number \quad of \quad combinations(200)} \times 100 \tag{4-4}$$

Table Observations

Following observations were made from the Table 4-7 to 4-13:

- There are no collisions when the transition period is in the range (0-0.21) s.
- For transition period 0.15 s which is considered to be highest in the current hardware implementation, no collisions are observed.

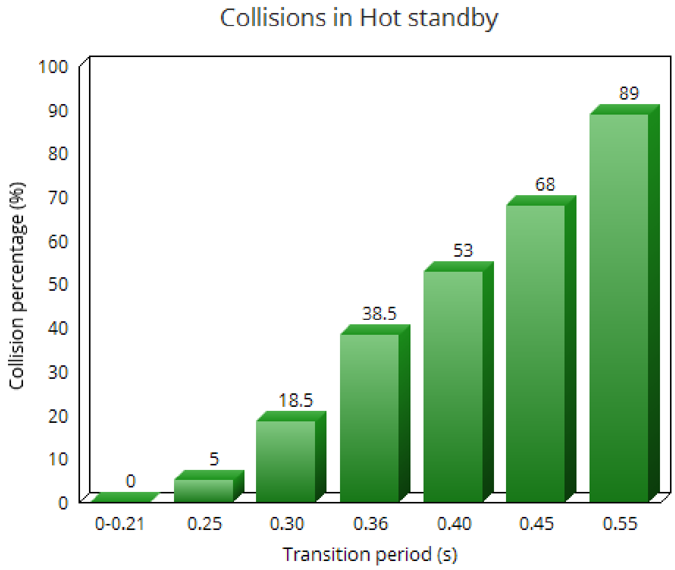


Figure 4-11: Chart representing collision percentage during transition periods in hot standby

Table 4-7: Time to collision when transition period is in the range (0-0.21 s) in hot standby mode

T	v (km/h)	h = 0.3 s															
		r = 2 m				r = 3 m				r = 4 m				r = 5 m			
0 - 0.21 s	50	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc
	60	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc
	70	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc
	80	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc
	90	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc
	100	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc
		h = 0.5 s															
0 - 0.21 s	50	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc
	60	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc
	70	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc
	80	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc
	90	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc
	100	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc
u_{i-1} (m/s^2)		-6	-7	-8	-9	-6	-7	-8	-9	-6	-7	-8	-9	-6	-7	-8	-9

Table 4-8: Time to collision when transition period is 0.25 s in hot standby mode

T	v (km/h)	h = 0.3 s															
		r = 2 m				r = 3 m				r = 4 m				r = 5 m			
0.25 s	50	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc
	60	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc
	70	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc
	80	nc	4.18	3.7	3.34	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc
	90	4.76	4.15	3.71	3.37	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc
	100	4.99	4.35	3.87	3.51	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc
		h = 0.5 s															
0.25 s	50	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc
	60	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc
	70	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc
	80	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc
	90	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc		nc	nc	nc	nc
	100	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc
u_{i-1} (m/s^2)		-6	-7	-8	-9	-6	-7	-8	-9	-6	-7	-8	-9	-6	-7	-8	-9

Table 4-9: Time to collision when transition period is 0.30 s in hot standby mode

T	v (km/h)	h = 0.3 s															
		r = 2 m				r = 3 m				r = 4 m				r = 5 m			
0.30	50	nc	nc	2.97	2.59	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc
	60	3.56	3.10	2.78	2.59	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc
	70	3.65	3.21	2.87	2.61	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc
	80	3.92	3.42	3.06	2.77	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc
	90	4.24	3.69	3.28	2.96	5.36	4.46	3.95	3.56	nc	nc	nc	nc	nc	nc	nc	nc
	100	4.57	3.97	3.52	3.18	5.13	4.47	3.97	3.60	nc	nc	nc	nc	nc	nc	nc	nc
		h = 0.5 s															
0.30 s	50	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc
	60	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc
	70	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc
	80	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc
	90	nc	4.92	4.43	4.05	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc
	100	5.66	4.99	4.47	4.10	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc
u_{i-1} (m/s^2)		-6	-7	-8	-9	-6	-7	-8	-9	-6	-7	-8	-9	-6	-7	-8	-9

Table 4-10: Time to collision when transition period is 0.36 s in hot standby mode

T	v (km/h)	h = 0.3 s															
		r = 2 m				r = 3 m				r = 4 m				r = 5 m			
0.36 s	50	2.78	2.45	2.22	2.02	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc
	60	2.99	2.63	2.36	2.15	nc	3.59	3.11	2.77	nc	nc	nc	nc	nc	nc	nc	nc
	70	3.28	2.87	2.56	2.32	3.85	3.38	3.01	2.73	nc	nc	nc	nc	nc	nc	nc	nc
	80	3.59	3.13	2.79	2.52	4.00	3.50	3.13	2.84	nc	nc	nc	nc	nc	nc	nc	nc
	90	3.90	3.39	3.02	2.73	4.27	3.72	3.31	2.99	5.06	4.35	3.87	3.49	nc	nc	nc	nc
	100	4.21	3.66	3.25	2.93	4.58	3.98	3.53	3.18	5.04	4.39	3.90	3.53	nc	nc	nc	nc
		h = 0.5 s															
0.36 s	50	nc	nc	nc	3.20	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc
	60	4.44	3.71	3.34	3.04	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc
	70	4.20	3.75	3.38	3.10	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc
	80	4.41	3.91	3.54	3.25	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc
	90	4.69	4.13	3.73	3.42	nc	nc	nc	4.44	nc	nc	nc	nc	nc	nc	nc	nc
	100	5.01	4.41	3.95	3.61	5.99	5.18	4.60	4.20	nc	nc	nc	nc	nc	nc	nc	nc
u_{i-1} (m/s^2)		-6	-7	-8	-9	-6	-7	-8	-9	-6	-7	-8	-9	-6	-7	-8	-9

Table 4-11: Time to collision when transition period is 0.4 s in hot standby mode

T	v (km/h)	h = 0.3 s															
		r = 2 m				r = 3 m				r = 4 m				r = 5 m			
0.4 s	50	2.57	2.27	2.05	1.88	3.7	3.05	2.69	2.42	nc	nc	nc	nc	nc	nc	nc	nc
	60	2.83	2.49	2.23	2.03	3.34	2.93	2.63	2.4	nc	nc	nc	nc	nc	nc	nc	nc
	70	3.12	2.73	2.44	2.21	3.5	3.07	2.74	2.49	nc	4.02	3.42	3.06	nc	nc	nc	nc
	80	3.41	2.98	2.66	2.41	3.76	3.28	2.93	2.65	4.27	3.74	3.34	3.03	nc	nc	nc	nc
	90	3.7	3.23	2.88	2.6	4.05	3.53	3.14	2.83	4.43	3.86	3.44	3.12	nc	nc	4.22	3.75
	100	3.99	3.48	3.09	2.79	4.34	3.78	3.35	3.03	4.69	4.08	3.62	3.27	5.22	4.55	4.04	3.65
		h = 0.5 s															
0.4 s	50	3.62	3.19	2.89	2.64	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc
	60	3.65	3.24	2.95	2.72	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc
	70	3.85	3.43	3.1	2.85	nc	nc	nc	3.71	nc	nc	nc	nc	nc	nc	nc	nc
	80	4.14	3.66	3.31	3.04	5.06	4.4	3.95	3.61	nc	nc	nc	nc	nc	nc	nc	nc
	90	4.47	3.93	3.53	3.23	5.02	4.42	3.99	3.65	nc	nc	nc	nc	nc	nc	nc	nc
	100	4.82	4.22	3.78	3.44	5.23	4.61	4.14	3.78	nc	nc	nc	nc	nc	nc	nc	nc
u_{i-1} (m/s^2)		-6	-7	-8	-9	-6	-7	-8	-9	-6	-7	-8	-9	-6	-7	-8	-9

Table 4-12: Time to collision when transition period is 0.45 s in hot standby mode

T	v (km/h)	h = 0.3 s															
		r = 2 m				r = 3 m				r = 4 m				r = 5 m			
0.45 s	50	2.4	2.12	1.91	1.75	2.86	2.52	2.28	2.08	nc	nc	nc	2.87	nc	nc	nc	nc
	60	2.66	2.34	2.1	1.91	3.01	2.64	2.38	2.17	3.73	3.22	2.87	2.6	nc	nc	nc	nc
	70	2.93	2.57	2.3	2.09	3.26	2.85	2.55	2.31	3.65	3.21	2.87	2.61	nc	nc	3.8	3.26
	80	3.2	2.8	2.5	2.27	3.52	3.08	2.75	2.49	3.85	3.37	3.01	2.73	4.42	3.85	3.44	3.12
	90	3.47	3.03	2.71	2.45	3.79	3.31	2.95	2.66	4.12	3.59	3.19	2.88	4.48	3.91	3.49	3.16
	100	3.74	3.26	2.91	2.63	4.06	3.54	3.15	2.84	4.38	3.82	3.39	3.06	4.71	4.1	3.64	3.29
		h = 0.5 s															
0.45 s	50	3.11	2.78	2.54	2.35	nc	nc	nc	3.37	nc	nc	nc	nc	nc	nc	nc	nc
	60	3.33	2.96	2.69	2.48	nc	3.75	3.35	3.04	nc	nc	nc	nc	nc	nc	nc	nc
	70	3.6	3.2	2.89	2.65	4.16	3.7	3.33	3.05	nc	nc	nc	nc	nc	nc	nc	nc
	80	3.92	3.46	3.11	2.85	4.33	3.83	3.46	3.18	nc	nc	nc	3.97	nc	nc	nc	nc
	90	4.27	3.74	3.35	3.06	4.59	4.04	3.64	3.33	5.33	4.64	4.17	3.8	nc	nc	nc	nc
	100	4.62	4.04	3.61	3.28	4.9	4.3	3.85	3.51	5.36	4.72	4.23	3.86	nc	nc	nc	nc
u_{i-1} (m/s^2)		-6	-7	-8	-9	-6	-7	-8	-9	-6	-7	-8	-9	-6	-7	-8	-9

Table 4-13: Time to collision when transition period is 0.55 s in hot standby mode

T	v (km/h)	h = 0.3 s															
		r = 2 m				r = 3 m				r = 4 m				r = 5 m			
0.55 s	50	2.15	1.91	1.72	1.58	2.44	2.16	1.95	1.79	2.82	2.5	2.26	2.06	nc	3.28	2.84	2.54
	60	2.39	2.11	1.9	1.74	2.67	2.35	2.11	1.92	2.95	2.6	2.34	2.14	3.38	2.97	2.67	2.44
	70	2.62	2.31	2.07	1.89	2.9	2.55	2.28	2.08	3.18	2.79	2.49	2.26	3.47	3.05	2.73	2.49
	80	2.85	2.51	2.25	2.05	3.13	2.75	2.46	2.23	3.41	2.98	2.67	2.42	3.69	3.22	2.88	2.61
	90	3.08	2.71	2.42	2.2	3.36	2.94	2.63	2.39	3.64	3.18	2.84	2.57	3.92	3.42	3.05	2.76
	100	3.32	2.9	2.6	2.36	3.59	3.14	2.81	2.54	3.87	3.38	3.01	2.73	4.15	3.62	3.22	2.91
		h = 0.5 s															
0.55 s	50	2.7	2.42	2.21	2.04	3.16	2.83	2.58	2.37	nc	nc	nc	3.05	nc	nc	nc	nc
	60	2.98	2.65	2.4	2.21	3.32	2.95	2.68	2.47	4.04	3.51	3.16	2.88	nc	nc	nc	nc
	70	3.3	2.91	2.62	2.4	3.56	3.16	2.85	2.61	3.97	3.53	3.18	2.92	nc	nc	4	3.52
	80	3.62	3.18	2.86	2.6	3.86	3.4	3.05	2.79	4.16	3.68	3.32	3.04	4.75	4.18	3.76	3.43
	90	3.94	3.46	3.1	2.82	4.18	3.66	3.28	2.98	4.43	3.89	3.5	3.19	4.8	4.23	3.81	3.48
	100	4.27	3.74	3.34	3.03	4.5	3.94	3.52	3.19	4.73	4.14	3.71	3.37	5.02	4.41	3.95	3.6
u_{i-1} (m/s^2)		-6	-7	-8	-9	-6	-7	-8	-9	-6	-7	-8	-9	-6	-7	-8	-9

4-3-3 Proposed CACC Implementation

This subsection presents the simulations and results for the proposed CACC strategy. As mentioned in Section 3-4, in this method the communicated intended acceleration u_{i-1} is available for the control input u_i for the lower-level controller during the transition period. This method has an advantage over the earlier mentioned warm and hot standby mode. Therefore, the control input is always available for vehicle i and there is no effect of the transition period on the vehicle i. From Figure 4-12, one could see that the control input u_i with and without transition period is the same. Hence, the velocity of vehicle i with the transition period gives the same plot as the vehicle i without any transition period. This confirms that not only feedforward signal can be used in CACC to enable short distance platooning but also for safety.

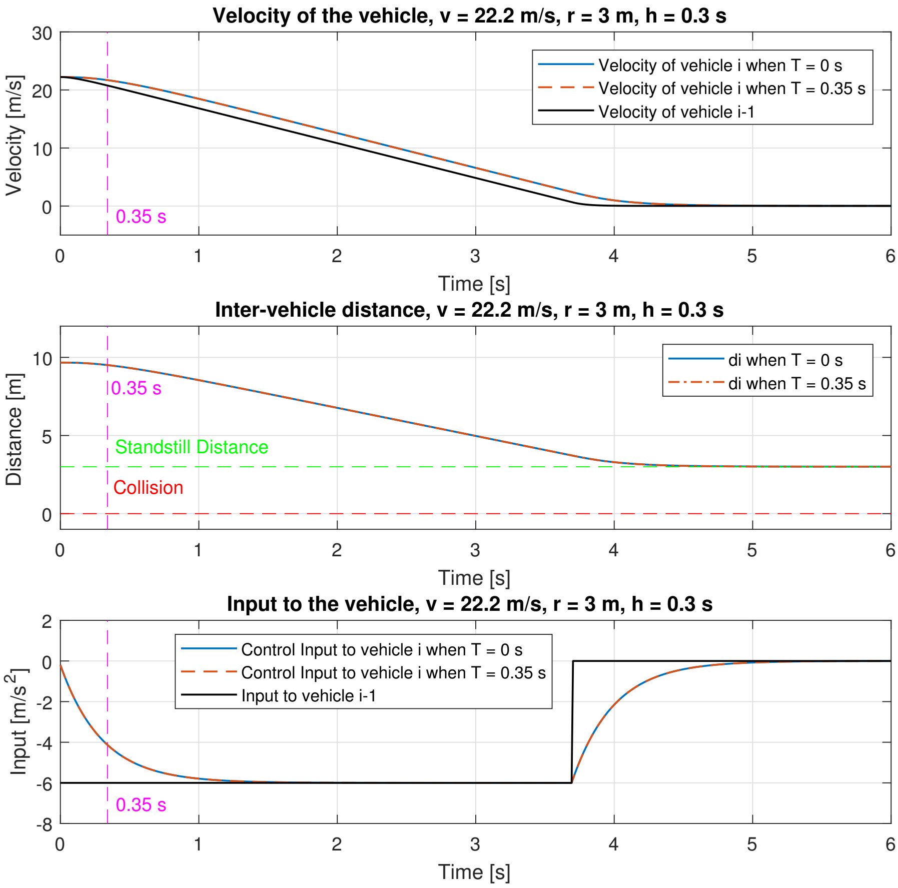


Figure 4-12: Top: Velocity of the vehicle $i-1$ and vehicle i with and without transition duration. Middle: The distance d_i between the vehicles $i-1$ and i with and without transition duration. Bottom: The input to the vehicle $i-1$ and the control input to the vehicle i with and without transition duration

In Table 4-14, time to collision in seconds has been presented for the different parameter.

Here, nc means no collision, T is the transition period in seconds, v is the initial velocity in km/h, r is the standstill distance between the vehicles $i-1$ and i, h is the headway time in seconds and u_{i-1} is the lead vehicle deceleration value in m/s^2. A total of 200 combinations are presented in every table. Finally, collision percentage is calculated based on the number of appearances of time to collision out of the total number of combinations (200) present in the Tables.

$$Collision\% = \frac{Number \quad of \quad time \quad to \quad collisions}{Total \quad number \quad of \quad combinations(200)} \times 100 \tag{4-5}$$

Table Observations

Following observations were made from the Table 4-14:

- There are no collisions when the transition period is in the range (0-0.60) s.
- For transition period 0.15 s which is considered to be highest in the current hardware implementation, no collisions are observed.

Table 4-14: Time to collision when transition period is in the range (0-0.60) s in the proposed CACC implementation.

T (s)	v (km/h)	h = 0.3 s															
		r = 2 m				r = 3 m				r = 4 m				r = 5 m			
0 - 0.60 s	50	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc
	60	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc
	70	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc
	80	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc
	90	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc
	100	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc
		h = 0.5 s															
0 - 0.60 s	50	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc
	60	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc
	70	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc
	80	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc
	90	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc
	100	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc	nc
u_{i-1} (m/s^2)		-6	-7	-8	-9	-6	-7	-8	-9	-6	-7	-8	-9	-6	-7	-8	-9

4-4 Conclusions

Using MATLAB simulations, behaviors of the vehicle in a CACC enabled platoon in the worst case scenario are presented. It is observed that in the current implementation by TNO, the vehicle i suffers from the transition period with a maximum value of 0.15 s. And under warm standby mode, vehicle i collides with vehicle $i-1$. TNO has implemented hot standby in the vehicle which does not lead to collision when transition period is 0.15 s. However, this hot standby mode is not safe when the transition period is greater than 0.21 s. On the other hand, the proposed improved method shows far better performance as there are no collisions even when transition period is 0.60 s.

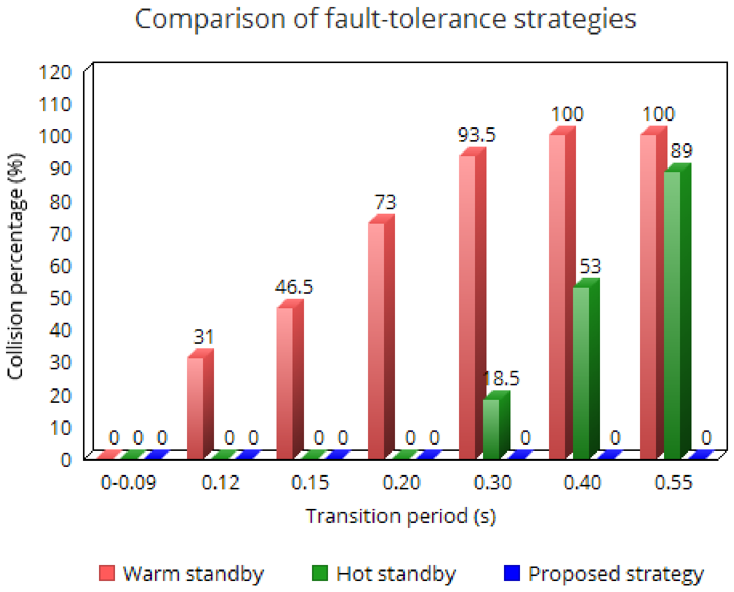


Figure 4-13: Comparison of fault-tolerance strategies

Figure 4-11 shows a column chart comparing the fault-tolerant strategies *viz.* warm standby, hot standby, and the proposed method. The simulation studies demonstrate that the feedforward signal, used to enable CACC for short distance platooning, can also be used to improve safety under ECU failure.

Chapter 5

Conclusions and Recommendations

5-1 Conclusions

Vehicle platooning is the grouping of vehicles, where individual vehicles automatically adjust their own speed as to maintain a desired inter-vehicle distance. Using on-board sensors and wireless communicated data, a platoon of CACC equipped vehicles is able to achieve the desired inter-vehicle time gap lower than 1 second which would facilitate a higher road throughput while maintaining string stability.

CACC enabled vehicles to communicate wirelessly to share their information which enables the vehicles to maintain a shorter distance between each other. However, these systems are hugely dependent on proper functioning of several mechatronic devices. Failure of those devices could jeopardize the safety of the platoon. TNO has identified ECU as one of the most safety-critical devices and has therefore implemented a redundant ECU mechanism to mitigate an ECU failure. However, in the implemented redundancy, there exists a transition period in which no control input u_i is present for the lower-level controller which provides signal to the vehicle actuator. The maximum considered transition period in TNO implemented system is 0.15 s which could possibly lead to inter-vehicle collisions under hard braking conditions.

The main contribution of this thesis is the evaluation of the states of the platoon and the control input u_i during the worst case emergency situation: simultaneous maximum emergency braking by the platoon leader with ECU failure in one of the following vehicles. This helps in capturing the effect of fault tolerant system on the platoon and evaluating the platoon safety. In the platoon's CACC system, three strategies for making CACC resilient to ECU failures were evaluated, namely, warm standby, hot standby and the proposed method. ECU hot standby has shown better performance than the ECU warm standby but still it is not able to mitigate collisions when the transition duration is comparatively larger, $T > 0.21$ s. Therefore, a new method to implement ECU redundancy in a CACC system is proposed under the same hardware structure which uses the communicated data to act as the control input during the transition period. Matlab-based simulations were used to compare the performance of all three strategies in terms of their ability of avoiding collisions under the worst-case emergency braking scenario. These simulations show that the proposed method is resilient to the larger transition period and can reject the disturbance caused by the preceding vehicle due to emergency braking scenario. However, the delay in wireless communication can affect the performance of the proposed strategy. Also, due to the distribution of control structure in multiple ECUs, synchronization of ECUs has to be perfect.

5-2 Recommendations

In this thesis, results are obtained using the linear time-invariant longitudinal vehicle model. However, this will not be the case in reality. In realistic platooning applications, vehicles in a platoon should be able to adjust longitudinal and lateral vehicle motion while maintaining a string stable behavior. The effect of loss of ECU would also affect the lateral motion of the vehicle. Therefore extending the vehicle model to include lateral motion is recommended.

Furthermore, the linear time-invariant vehicle model does not take into account of nonlinearities such as tire behavior, gear dynamics, weather conditions and aerodynamic resistance. Even though tires might behave linearly at constant velocities, their behavior becomes highly non-linear during extreme decelerations. Therefore, it is recommended to extend the analysis considering the model nonlinearities.

In this thesis, communication delays have not been considered. But in reality delays in wireless communication and other internal communications are present. Therefore, it is recommended to extend the analysis considering all the delays in the system.

Multiple ECUs are involved in the system and a state of perfect synchronization is assumed between them, however, a thorough analysis has to be made to check the system on the hardware level.

Finally, in this thesis, the results are obtained based on simulation studies. Hence, real-time experiments are needed to validate the results and the proposed method.

Appendix A

Condition for string stability for a homogeneous platoon

In this chapter, we summarize the condition for the controller values for string stability [8].

A-1 Condition for string stability of a CACC enabled platoon

For a CACC enabled platoon, the control parameter of vehicle i i.e. $K = [k_p \quad k_d \quad k_{dd}]$ the spacing policy h need to satisfy following conditions:

$$k_p, \quad k_d, \quad 1 + k_{dd} > 0, \quad h > 0, \tag{A-1}$$

$$(1 + k_{dd})k_d - k_p\tau > 0 \tag{A-2}$$

Bibliography

[1] T. Robinson, E. Chan, and E. Coelingh, “Operating platoons on public motorways: An introduction to the sartre platooning programme,” in *17th world congress on intelligent transport systems*, vol. 1, p. 12, 2010.

[2] J. Ploeg, “Vehicular platooning.” Internal Report, 2016.

[3] G. Dimitrakopoulos and P. Demestichas, “Intelligent transportation systems,” *IEEE Vehicular Technology Magazine*, vol. 5, no. 1, pp. 77–84, 2010.

[4] C. Bergenhem, S. Shladover, E. Coelingh, C. Englund, and S. Tsugawa, “Overview of platooning systems,” in *Proceedings of the 19th ITS World Congress, Oct 22-26, Vienna, Austria (2012)*, 2012.

[5] “What are the benefits of truck platooning?,” 2016.

[6] R. Rajamani, “Adaptive cruise control,” *Encyclopedia of Systems and Control*, pp. 13–19, 2015.

[7] M. Hoedemaeker and K. A. Brookhuis, “Behavioural adaptation to driving with an adaptive cruise control (acc),” *Transportation Research Part F: Traffic Psychology and Behaviour*, vol. 1, no. 2, pp. 95–106, 1998.

[8] J. Ploeg, “Analysis and design of controllers for cooperative and automated driving,” *Eindhoven University of Technology*, 2014.

[9] F. Bu, H.-S. Tan, and J. Huang, “Design and field testing of a cooperative adaptive cruise control system,” in *American Control Conference (ACC), 2010*, pp. 4616–4621, IEEE, 2010.

[10] J. Piao and M. McDonald, “Advanced driver assistance systems from autonomous to cooperative approach,” *Transport Reviews*, vol. 28, no. 5, pp. 659–684, 2008.

[11] G. J. Naus, R. P. Vugts, J. Ploeg, M. J. van de Molengraft, and M. Steinbuch, “String-stable cacc design and experimental validation: A frequency-domain approach,” *IEEE Transactions on vehicular technology*, vol. 59, no. 9, pp. 4268–4279, 2010.

[12] R. Isermann, R. Schwarz, and S. Stolzl, "Fault-tolerant drive-by-wire systems," *IEEE Control Systems*, vol. 22, no. 5, pp. 64–81, 2002.

[13] "Details revealed of ricardo contribution to 'ecotwin' truck platooning project," 2016.

[14] R. Isermann, *Fault-diagnosis systems: an introduction from fault detection to fault tolerance.* Springer Science & Business Media, 2006.

[15] E. van Nunen, J. Ploeg, A. M. Medina, and H. Nijmeijer, "Fault tolerancy in cooperative adaptive cruise control," in *Intelligent Transportation Systems-(ITSC), 2013 16th International IEEE Conference on*, pp. 1184–1189, IEEE, 2013.

[16] B. Wang, D. Zhao, C. Li, and Y. Dai, "Design and implementation of an adaptive cruise control system based on supervised actor-critic learning," in *Information Science and Technology (ICIST), 2015 5th International Conference on*, pp. 243–248, IEEE, 2015.

[17] R. Rajamani, *Vehicle dynamics and control.* Springer Science & Business Media, 2011.

[18] D. Swaroop, J. Hedrick, C. Chien, and P. Ioannou, "A comparision of spacing and headway control laws for automatically controlled vehicles1," *Vehicle System Dynamics*, vol. 23, no. 1, pp. 597–625, 1994.

[19] J. Ploeg, N. Van De Wouw, and H. Nijmeijer, "Lp string stability of cascaded systems: Application to vehicle platooning," *IEEE Transactions on Control Systems Technology*, vol. 22, no. 2, pp. 786–793, 2014.

[20] S. Sheikholeslam and C. A. Desoer, "Longitudinal control of a platoon of vehicles with no communication of lead vehicle information: A system level study," *IEEE Transactions on vehicular technology*, vol. 42, no. 4, pp. 546–554, 1993.

[21] T. Bronkhorst, "Hardware design of a cooperative adaptive cruise control system using a functional programming language," Master's thesis, University of Twente, 2014.

[22] S. Öncü, N. Van De Wouw, and H. Nijmeijer, "Cooperative adaptive cruise control: Tradeoffs between control and network specifications," in *Intelligent Transportation Systems (ITSC), 2011 14th International IEEE Conference on*, pp. 2051–2056, IEEE, 2011.

[23] R. Rajamani, A. S. Howell, C. Chen, J. K. Hedrick, and M. Tomizuka, "A complete fault diagnostic system for automated vehicles operating in a platoon," *IEEE transactions on control systems technology*, vol. 9, no. 4, pp. 553–564, 2001.

[24] K. Reif, *Automotive Mechatronics.* Springer, 2014.

[25] T. Bijlsma and T. Hendriks, "A fail-operational truck platooning architecture," in *Intelligent Vehicles Symposium (IV), 2017 IEEE*, pp. 1819–1826, IEEE, 2017.

[26] C. Gold, D. Damböck, L. Lorenz, and K. Bengler, "âĂIJtake over!âĂİ how long does it take to get the driver back into the loop?," in *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, vol. 57, pp. 1938–1942, SAGE Publications Sage CA: Los Angeles, CA, 2013.

[27] A. Kunnappillil Madhusudhanan, M. Corno, and E. Holweg, “Sliding mode-based lateral vehicle dynamics control using tyre force measurements,” *Vehicle System Dynamics*, vol. 53, no. 11, pp. 1599–1619, 2015.

[28] A. K. Madhusudhanan, M. Corno, and E. Holweg, “Vehicle sideslip estimator using load sensing bearings,” *Control Engineering Practice*, vol. 54, pp. 46–57, 2016.

[29] A. K. Madhusudhanan, M. Corno, M. A. Arat, and E. Holweg, “Load sensing bearing based road-tyre friction estimation considering combined tyre slip,” *Mechatronics*, vol. 39, pp. 136–146, 2016.

[30] E. Kreyszig, *Advanced engineering mathematics*. John Wiley & Sons, 2010.

[31] S. V. Amari and G. Dill, “A new method for reliability analysis of standby systems,” in *Reliability and Maintainability Symposium, 2009. RAMS 2009. Annual*, pp. 417–422, IEEE, 2009.

[32] O. Tannous, L. Xing, P. Rui, M. Xie, and S. H. Ng, “Redundancy allocation for series-parallel warm-standby systems,” in *Industrial Engineering and Engineering Management (IEEM), 2011 IEEE International Conference on*, pp. 1261–1265, IEEE, 2011.

[33] J. Ploeg, B. T. Scheepers, E. Van Nunen, N. Van de Wouw, and H. Nijmeijer, “Design and experimental evaluation of cooperative adaptive cruise control,” in *Intelligent Transportation Systems (ITSC), 2011 14th International IEEE Conference on*, pp. 260–265, IEEE, 2011.