Title

Fault Tolerant Lateral Control for Transit Buses and Trucks

Permalink

Authors

Suryanarayanan, Shashikanth
Hsiao, Tesheng
Tomizuka, Masayoshi

Publication Date

2004-04-01

CALIFORNIA PATH PROGRAM
INSTITUTE OF TRANSPORTATION STUDIES
UNIVERSITY OF CALIFORNIA, BERKELEY

Fault Tolerant Lateral Control for Transit Buses and Trucks

Shashikanth Suryanarayanan
Tesheng Hsiao
Masayoshi Tomizuka

California PATH Research Report
UCB-ITS-PRR-2004-6

This work was performed as part of the California PATH Program of the University of California, in cooperation with the State of California Business, Transportation, and Housing Agency, Department of Transportation; and the United States Department of Transportation, Federal Highway Administration.

The contents of this report reflect the views of the authors who are responsible for the facts and the accuracy of the data presented herein. The contents do not necessarily reflect the official views or policies of the State of California. This report does not constitute a standard, specification, or regulation.

Final Report for Task Order 4205

April 2004

ISSN 1055-1425

PROJECT TITLE:

Fault Tolerant Lateral Control for Transit Buses and Trucks

By

Shashikanth Suryanarayanan
Tesheng Hsiao
Masayoshi Tomizuka

Department of Mechanical Engineering
University of California at Berkeley
Berkeley, CA 94720

Final report for TO4205

February 2004

Executive Summary

This report documents the research results of Task Order 4205 (TO4205), *Fault Tolerant Lateral Control for Transient Buses and Trucks* performed during 2000-2003. In this task order, we studied the procedures for designing real-time lateral control systems for automated vehicles that are not sensitive to failures of the two key components: a set of magnetometers at the front bumper and another set at the rear bumpers. This problem is important because failures related to either front or rear magnetometers may have immediate effect on the stability of the closed loop control system.

We formulate the problem of designing fault tolerant controllers as a simultaneous stabilization problem. This formulation is based on the observation that the dynamics from the steering input to the sensor output depends on the location of the magnetometers. When both the front and rear sets of magnetometers are available, their outputs may be combined to synthesize a virtual sensor placed ahead of the vehicle; for convenience, let the dynamics from the input to the output of the virtual sensor be denoted by P_0. If the rear set of magnetometers fails, the vehicle must be controlled by the remaining front magnetometers only; let the dynamics from the steering input to the output of the front magnetometers be denoted by P_1. Likewise, the dynamics from the input to the output of the rear set of magnetometers in case of the failure of the front set of magnetometers is denoted by P_2. If a controller designed for the nominal dynamics P_0 simultaneously stabilizes the closed loop system with either P_1 or P_2, the closed loop system will remain stable under failure of either the front set of magnetometers or the rear set. In this report, two methods are developed for designing simultaneously stabilizing controllers. The first method applies to simultaneous stabilization of two plants, and the second three or more plants.

We also consider the problem of accommodating a specific type of failure in one of the two sets of magnetometers. The failure mode in this case is that in the event of a failure of any set of magnetometers, the associated output goes to a constant value.

A heuristic control architecture utilizing dedicated observers is proposed to solve this problem. The proposed observer-based fault tolerant control system is built on a Fault Detection and Identification (FDI) mechanism.

While the original goal was to evaluate the theoretical results on commuter buses, PATH test vehicles available for this study were passenger vehicles only. Thus, the report presents the evaluation of the fault tolerant and FDI based control methodologies on passenger vehicles. The merits and demerits of the simultaneously stabilizing controllers and the observer-based scheme are described.

Abstract

This report documents the research results of Task Order 4205 (TO4205), "*Fault Tolerant Lateral Control for Transit Buses and Trucks*" performed during 2000-2003. In this report, we develop procedures for the design of vehicle lateral control systems for automated vehicles that are insensitive to "hard" failures of magnetometers. The design methods may apply to various types of candidate vehicles for automated highway applications such as passenger vehicles, transit buses and trucks.

First, the problem of design of failure tolerant controllers is formulated as a simultaneous stability problem, i.e. given a finite number of LTI systems which respectively represent the vehicle under consideration operating in the normal and faulty conditions, design a controller such that the controller can stabilize all these given LTI systems while a performance criterion related to the normal operation is minimized. We reduce this problem to a standard H_∞ control problem with Linear Matrix Inequality (LMI). It however suffers from the limitation of being conservative because it is based on only sufficient conditions for simultaneous stability.

Next, we consider the problem of accommodating a specific type of failure in one of two sensors used for controlling a two-output system. We propose a *dedicated observer-based* fault tolerant control system which is built on a Fault Detection and Identification (FDI) mechanism. This control strategy is less conservative; however it is argued that the limitation of the dedicated observer based scheme is its heavy dependence on the model used to describe the system.

The strategies developed above are tested on the test vehicles used by the Partners for Advanced Transit on Highways (PATH). Experimental results demonstrating failure tolerant control action are documented.

Keywords

Vehicle lateral control, Simultaneously stabilizing controller, Fault tolerant control, Fault detection and identification, Dedicated Observer

Contents

1 Introduction

The focus of this project (TO 4205) is the development of procedures for the design of failure tolerant real-time control systems. In particular, this project deals with control systems described by the feedback topology. We define a **failure** (or a **fault**) as an anomaly that can have a significant detrimental effect on the performance of the system under consideration. A fault is classified as "hard" if its effect is immediate and as "soft" otherwise. As expected, hard faults are easy to detect and difficult to accommodate whereas soft faults are difficult to detect but provide leeway for their accommodation. In this report, we investigate the problem of design of control systems that are robust to hard faults.

Why are we interested in this study? The main reason is that in safety-critical, high-bandwidth real-time control systems, faults (especially hard faults) can potentially cause serious damage to life and property. Roughly speaking, high-bandwidth control systems respond "quickly" to external inputs. In the event of a hard failure, such systems (which often work under tight real-time deadlines) cannot tolerate prolonged delays in control reconfiguration (if at all possible) since delays can often render such systems unstable. This issue becomes serious in safety-critical systems such as nuclear power plants, hazardous chemical manufacturing plants, civilian aircrafts etc. Even in low-risk systems, hard failures can often result in significant down-times of infrastructures that include production houses and civilian services. Investing in failure management techniques to accommodate hard failures, therefore, can lead to significant savings.

In order to better illustrate the design procedures, this report focuses on a specific safety-critical system: The fully-automated Intelligent Vehicle Highway System (IVHS) under development at PATH (Partners for Advanced Transit on Highways). A typical highway system helps transport a large number of people at highway speeds. Therefore, safety and reliability are critical pre-required for full-scale operation of any highway, more so in the case of a fully-automated highway. We develop control schemes some of which are general while others are specific to the PATH IVHS system. In the case of the latter, we abstract important ideas which may be useful in other system design situations.

The PATH IVHS is based on the idea of platooning. A platoon is a group of vehicles moving with close inter-vehicle spacing. To realize the organization of the vehicles in platoons a multi-layered hierarchical control architecture has been adopted. The "lowest" layer of this hierarchy is called the *regulation layer*. This layer is responsible for administering the *longitudinal control* and *lateral control* operations for each vehicle in the IVHS. Longitudinal control deals with the control of the motion of the vehicle in a direction parallel to the direction of travel whereas lateral control deals with control of the vehicle normal to the direction of travel. In an automated highway, the longitudinal control system is responsible for maintaining appropriate highway speeds and spacing between vehicles whereas the lateral control system is used to realize the lane-keeping and lane-changing operations. The lane-keeping control operation is high-bandwidth in nature and cannot tolerate significant delays in the control loop. Therefore, accommodation of hard faults in the lane-keeping control system becomes an important issue. This report addresses the problem associates with the development of control schemes to accommodate hard faults in the sensors used in the lane-keeping control system deployed on test vehicles used by PATH.

1.1 Problem Addressed

As mentioned earlier, in this report we are interested in developing schemes for the design of failure insensitive controllers. We refer to such controllers as **fault tolerant controllers**. This report considers three problems:

1. Problem 1: Given two finite dimensional, linear-time invariant (FDLTI) system P_0 and P_1, design a single controller C (also FDLTI), such that each of the feedback interconnections $(P_i, C), i = 0, 1$ is internally stable.

2. Problem 2: Given a finite number of FDLIT plants $(P_i, i = 0, 1, \cdots, n)$,design a single controller C (also FDLTI) which ensure:
   - Internal Stability of each of the feedback systems $(P_i, C), i = 0, 1, \cdots, n$
   - Satisfactory performance of at least one of the feedback systems, say (P_0, C)

3. Problem 3: Give an LTI two-output system, design a control structure which guarantees stability in the event of failures described as one of the sensor outputs undergoing a step change from its correct reading to a constant value (at a time (say) t_0).

Remark:

1. Problem 1 is the simultaneous Stability problem for the two plant case. It should be noted that this problem has been solved completely ([9][10]) using a classical interpolation algorithm. In this report, we look at an alternate approach to this design problem. This problem has been motivated primarily by academic interest.

2. Problem 2 is an extended/modified version of the Simultaneous Stability problem. The plant P_0 can be interpreted as the non-faulty plant whereas plants $P_i (i \neq 0)$ can be constructed as the dynamics arising out of different failed situations. It is clear then that the solution of this problem, if it exists, yields a controller that is failure tolerant and one that guarantees satisfactory performance under the no-fault condition.

3. Problem 3 deals with the proposal of a fault tolerant controller structure for a specific scenario. This failure scenario is considered for two reasons:
   (a) Such a situation occurs in the lane-keeping control system on-board test vehicle used by PATH.

(b) Hard faults can be ”engineered” to behave in this fashion. In other words, since hard faults are usually easy to detect, a rule can be imposed to make the fault behave in a certain fashion that is suitable for control purposes.

4. In the statement of Problem 2 as well as Problem 3, real-time knowledge of failure is not assumed. However, in both these problems it is assumed that failure models are know *apriori*.

This report addresses these problems by answering them in parallel with questions pertaining specifically to the lane-keeping control system deployed on test vehicles at PATH.

2 Hardware Configuration and Failure

This section presents a brief summary of the lane-keeping control hardware setup on test vehicles used by PATH. This summary is followed by a description of the hard faults in the sensors used for lane-keeping control.

2.1 Hardware Configuration

The lane-keeping control system developed at PATH (Figure 1) utilizes a magnet-magnetometer based architecture. Magnets are installed along the center of lanes and act as the reference that vehicles track. The vehicles in turn are fitted with sensors (called **magnetometers**) which measure the magnetic field intensity of the locations of their installation. They are suitably calibrated to indicate how far they are displaced from the magnets they sense. This measurement is denoted as the *lateral error*.

The installation configuration of the lane-keeping hardware varies across the spectrum of test vehicles used by PATH. Figure 2 shows the installation configuration of the magnetometers and other components on the passenger test vehicles. As seen from

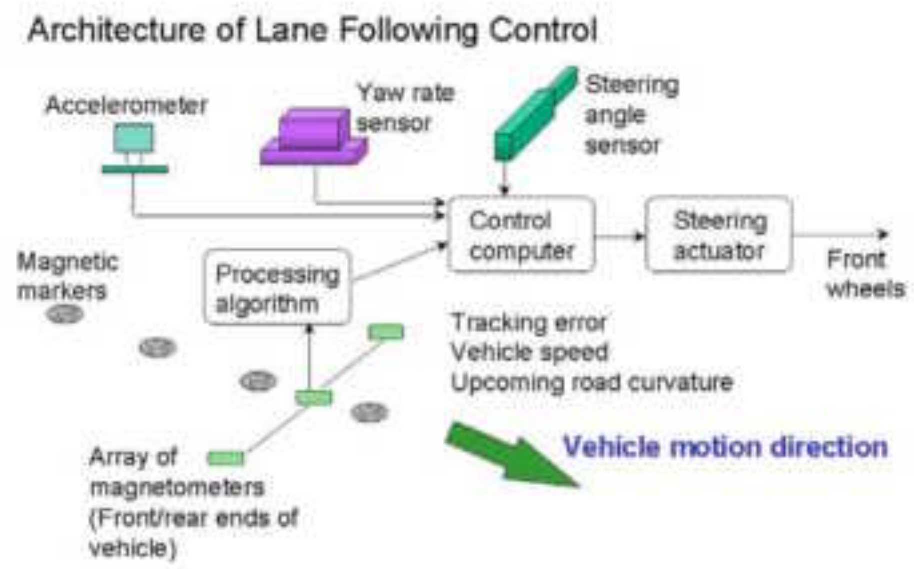


Figure 1: Scheme of lateral control system developed by PATH

this figure, two magnetometer banks are mounted on the front and rear bumpers of the vehicles. Each magnetometer bank is composed of multiple magnetometers which help in increasing the range of measurement.

A signal processing algorithm processes the information from the magnetometers that constitute each bank and returns the ”measured” lateral error. Roughly speaking, this algorithm returns the lateral error measured by the magnetometer with the largest detected magnetic field intensity as the ”measured” lateral error. The ”measured” lateral error is processed by a steering control routine which generates the desired steering angle that the tires are required to track. Both the signal processing and the steering control routines run on an on-board computer. The desired steering angle computed by the steering control routine is fed into an ”inner-loop” (Figure 2) which is designed to ensure that the actual steering angle of the tire follows the desired steering angle (computed by the steering control routine). The ”inner-loop” is comprised of a steering motor, an encoder (mounted on the steering column), the steering column itself (inclusive of the torsion bar and the hydraulic assist) and a

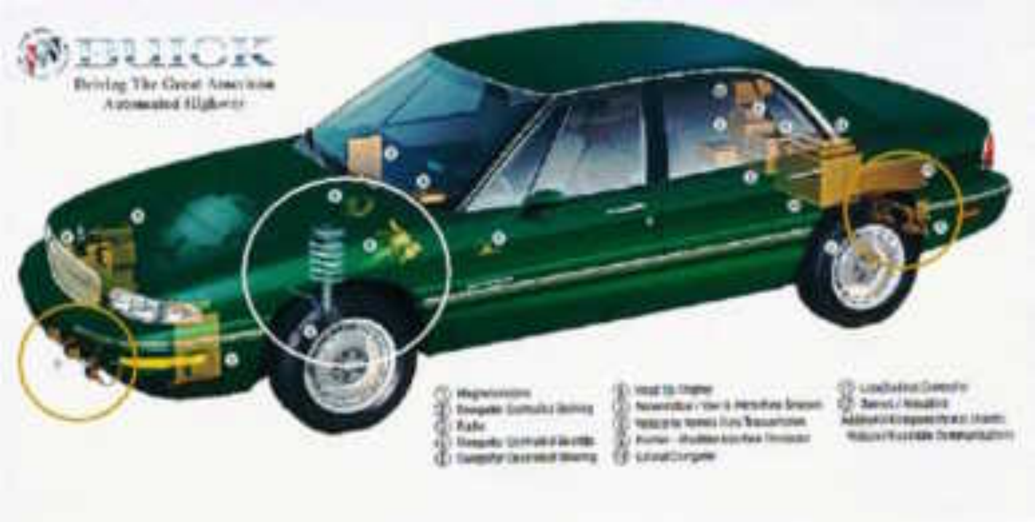


Figure 2: Hardware configuration on passenger vehicles. Smaller circles encircle magnetometer locations. Larger circle encircles the "inner-loop"

potentiometer (which measures the actual wheel angle of the tire).

The yaw rate gyro for lane-change operations whereas the accelerometers are used for sensor fusion/corroboration purposes. Since these sensors are not used for lane-keeping control, we will not describe them any further.

2.2 Magnetometer Failures

We define hard faults as faults that have a serious and immediate effect on system performance/stability. Even in simple systems such as the magnetometer banks and their associated communication links, many such failures can occur. For design purposes, however, it is useful to group failures based on how they can be modeled as affecting the system under investigation. As explained below, the groups into which these failures are split can, in fact, be "built-in" through physical redundancy measures.

The hard faults in the magnetometers are grouped into two groups. The first group relates to failures in the magnetometers themselves whereas the second category relates to failures in the communication link between the magnetometers and the computer that processes the information.

- Group 1: Failures caused due to magnetometer hardware malfunctioning.

  The magnetometers used on the test vehicles at PATH are equipped with a built-in hardware failure detection system. The circuitry in each magnetometer outputs a "health signal" to indicate if the magnetometer components are functioning well or not. In the event, that a failure is detected in the hardware components of the magnetometer, the magnetometer output is set to the maximum value of the output.

  For control purposes, these failures will be modeled as a step jump in the output of the magnetometer from the correct value to a value of 0.5m. This failure model will be referred to as Failure #1 in later sections.

- Group 2: Failure caused due to severance of the communication link.

  In order to maximize the signal to noise ratio, magnetometers need to be mounted so that they are as close as possible to the magnets on the road. However, this requirement also makes them more vulnerable to physical hazards that sever connections or in the worst case, knock magnetometers out. Such situations have been experienced in practice especially while operating the snow-plow and during testing under rainy conditions.

  For control purposes, these failures will be modeled as a step jump in the output of the magnetometer from the correct value to a value of 0m. This failure model will be referred to as Failure #2 in later sections.

Remarks:

1. The failure models are not precise. One can argue, for example, that almost never will a severance lead to a magnetometer output of precisely zero. In fact, in this system, it is observed that severance of communication links are usually manifestations of intermittent electrical connections. These failure models

have been chosen so that they are mathematically simple and convenient while acknowledging that it is almost impossible to construct precise mathematical descriptions of failures. Any failure management scheme utilizing such models has to incorporate the issue of robustness to uncertainties in them.

2. The failures listed are not all-encompassing. The failures and failure models described here are not meant to imply that these are the only hard failures that can occur in the lane-keeping control system. For example, a hardware failure in the magnetometer circuitry that is not detected by the built-in failure detection system is never accounted for in our description. However, we wish to mention that in all the testing thus far, hard failures in the magnetometers that do not fit into our description have not occurred.

3. The response to failures in Group 1 is "engineered". The failure response captured in the model is due to a built-in rule that responds to a certain signal in a chosen fashion. The choice for engineering such a rule into the failure management system has its pros and cons. The positive side being that it is much easier for the designer to characterize and accommodate failures since they are all bunched under one failure response. The negative side is the loss of freedom in tailoring the reconfiguration strategy to each of the individual failures. It is our opinion that more often than not, such rules enables easier and more tractable failure tolerant designs.

3 Bicycle Model for Lateral Control

Over the last three decades, the bicycle model has been used extensively in the analysis and design of lateral control systems for different vehicles. The primary reason for its popularity has been that it captures the most relevant lateral dynamics characteristics with a fairly simple structure. In this model, the lateral motion of the vehicles is modeled as that of a two-wheeled bicycle (Figure 3). The major assumptions made in the process are that: pitch and roll angles are small, steering angles are small, relative yaw angle (ϵ_r in Figure 3) are small and the lateral tire force model is linear.

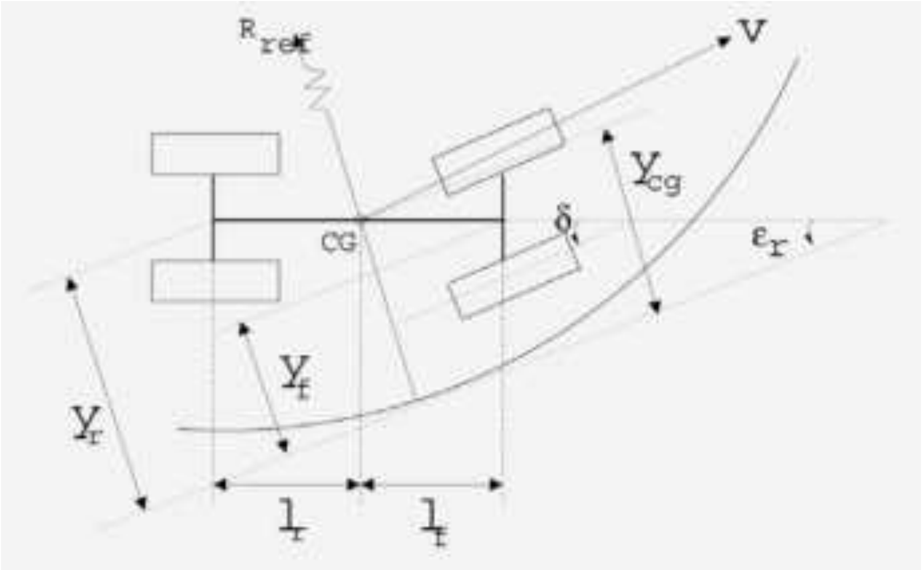


Figure 3: Vehicle moving along a reference path

The bicycle model for front wheel-steered, single-unit vehicles can be described using a four-state linear, time-varying model as follows:

$$\dot{x}(t) = A(\zeta)x(t) + B_1(\zeta)\delta(t) + B_2(\zeta)\dot{\epsilon}_d(t) \tag{1}$$

where $x = \begin{bmatrix} y_{cg}(t) & \dot{y}_{cg}(t) & \epsilon_r(t) & \dot{\epsilon}_r(t) \end{bmatrix}^T$. ζ is the vector of parameters shown in Table 1. $y_{cg}(t)$ is the deviation of the center-of-gravity(CG) from the road centerline and ϵ_r is the relative yaw angle (orientation of the vehicle with respect to the road). The model described above assumes that the road is either a straight line or a circle or, in other words, $\dot{\epsilon}_d(t)$ is assumed to be piece-wise constant. This is a good assumption for highways in the US.

The matrices and parameters that describe the model are:

$$A = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & -\frac{a_{11}}{\dot{x}} & a_{11} & \frac{a_{12}}{\dot{x}} \\ 0 & 0 & 0 & 1 \\ 0 & -\frac{a41}{\dot{x}} & a_{41} & \frac{a_{12}}{\dot{x}} \end{bmatrix} B_1 = \begin{bmatrix} 0 \\ b_{21} \\ 0 \\ b_{41} \end{bmatrix} B_2 = \begin{bmatrix} 0 \\ w_{21} \\ 0 \\ w_{41} \end{bmatrix}$$

$$a_{11} = (\phi_1 + \phi_2), a_{12} = \phi_1(d_s - l_f) + \phi_2(d_s + l_r), a_{41} = \frac{l_f C_f - l_r C_r}{I_z}$$

$$a_{42} = \frac{l_1 C_f (d_s - l_f) + l_2 C_r (d_s + l_r)}{I_z}, b_{21} = \phi_1, b_{41} = \frac{l_f C_f}{I_z}$$

$$w_{21} = -\frac{l_f^2 C_f + l_r^2 C_r}{I_z}, w_{41} = \phi_2 l_r - \phi_1 l_f - \dot{x}^2$$

$$\phi_1 = C_f \left(\frac{1}{m} + \frac{l_f d_s}{I_z} \right), \phi_2 = C_r \left(\frac{1}{m} - \frac{l_r d_s}{I_z} \right)$$

Table 1: Parameters used in the Bicycle Model

Param	Description	Values
m	Mass of the vehicle	1700-2100 Kg
I_z	Yaw moment of inertia	$\approx$ 2870Kgm^2
l_f	Distance between front axle and CG	0.9-1.2m
l_r	Distance between rear axle and CG	1.5-1.8m
C_f	Cornering Stiffness - Front tire system	$\approx$ 70000 N/rad
C_r	Cornering Stiffness - Rear tire system	$\approx$ 130000 N/rad
$\dot{x}, v$	Forward (longitudinal) velocity of vehicle	0-35 m/s
d_s	Distance between lateral error measuring sensor and CG	-3 to 10 m

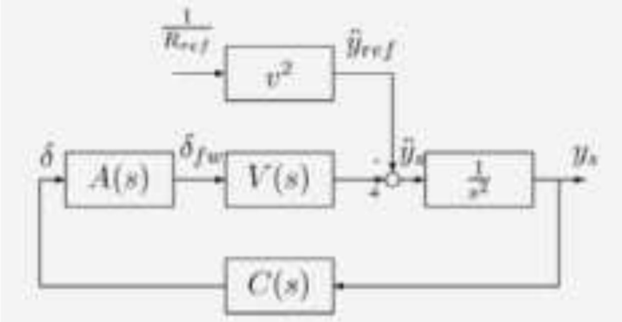
Table 1 describes the parameters used in the bicycle model and approximated values for the Buick LeSabre passenger vehicles.

Note that if the vehicle longitudinal velocity is treated as a varying parameter, then this model represents a linear parameter varying (LPV) system. For a fixed value of the longitudinal velocity, the above model represents a linear time invariant (LTI) system. Then for a fixed longitudinal velocity, the transfer function from the steering input (δ) to the lateral error ($\ddot{y}_s$) at the location of the sensor can be written as:

$$Y_s(s) = \frac{1}{s^2} V(s) \delta(s) \tag{2}$$

where $V(s)$ is of the from:

$$\begin{aligned} V(S) &= \frac{C_f v[(M l_f d_s + I_z) s^2 v + C_r l(v + (d_s + l_2) s]}{D(s)} \\ D(s) &= I_z(C_f + C_f) + M(C_f l_f^2 + C_r l_2^2) s + I_z M v_2 s_2 + (C_r l_2 - C_f l_1) + C_f C_f l_2 \end{aligned} \tag{3}$$



$A(s)$:Actuator Dynamics

$C(s)$:Controller

δ:steering angle at the steering wheel

δ_{fw}:Steering angle at the front wheel

R_{ref}:Radius of curvature of road

Figure 4: Block diagram used for vehicle lateral control

Note that $V(s)$ depends both on the vehicle longitudinal velocity and distance of the lateral error measuring sensors (magnetometers) and the vehicle CG. For control design, it is useful to think of the dynamics of the vehicle as composed of two coupled mechanisms (Figure 4). The first is the inertia of the vehicle represented by a double integrator in the frequency domain and the second, the force generation mechanism ($V(s)$) due to the tire road interaction. The acceleration produced by the force generating mechanism is combined with the road curvature input to produce the net acceleration of the vehicle.

The double integrator characteristics are well known (-40db/decade gain and 180 degree phase lag). Figure 5 and Figure 6 show the bode and pole-zero plots of the transfer function $V(s)$. From these plots we make the following observations.

1. The phase characteristics in Figure 5 indicate that the phase lag for a given position of the sensor (fix d_s) increases with increase in the vehicle longitudinal velocity. This makes the problem of lateral control design at higher speeds inherently difficult.

2. The input/output dynamics have smaller phase lags when the lateral error sensor for larger look-ahead distances (d_s). This nature was utilized in the design of the lateral controller for the 1997 NAHSC Demonstration by Patwardhan, Tan and the PATH lateral control team [7]

3. The open loop system has a pair of weakly damped zeros particularly at high longitudinal velocities and small values of d_s. If a high gain controller is applied to improve tracking performance, the closed loop poles are attracted to those zeros. Consequently, the closed loop system has a weakly damped oscillatory mode causing discomfort to the passengers.

4 Controller Design

4.1 Geometric Look-Ahead Scheme

The behavior of $V(s)$ indicates that the controller needs to provide lesser phase if d_s is large. However, due to physical limitations, it is impossible to realize d_s values larger than about 2m for passenger vehicles (since it is infeasible to place the front set of magnetometers any further the front bumper of the vehicle). Engineers at

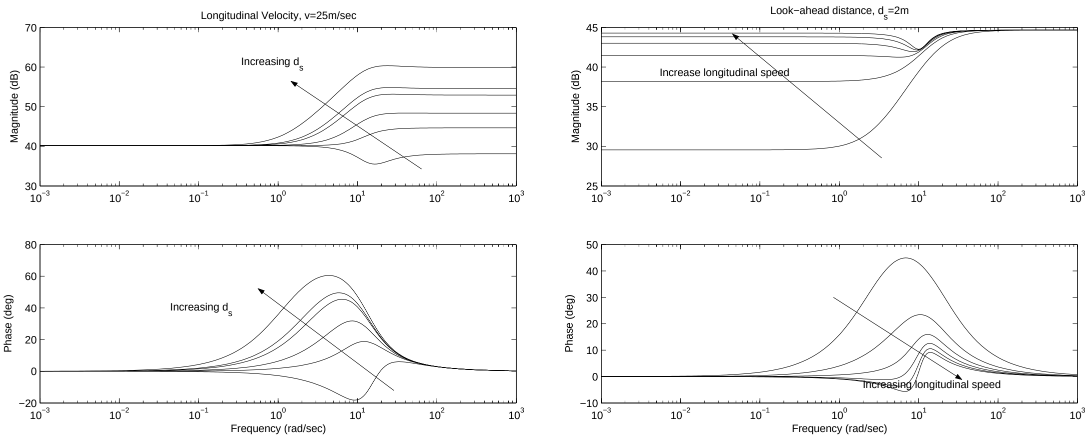


Figure 5: Bode plot of $V(s)$

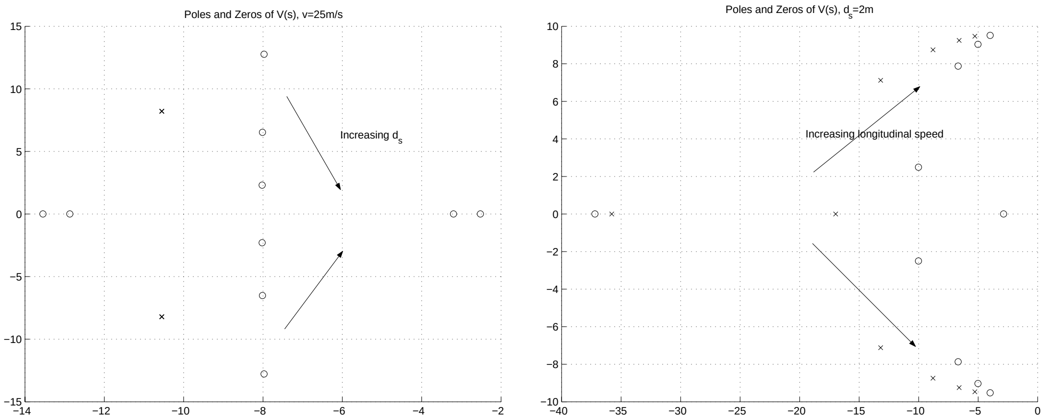


Figure 6: Poles and zeros of $V(s)$

PATH developed an ingenious way of working around this problem. They suggested a scheme that utilizes two independent lateral error measurements to geometrically construct the lateral error at any location ahead of the vehicle as though a virtual sensor was located at the point (Figure 7). (The second measurement is obtained from the magnetometers mounted under the rear bumper).

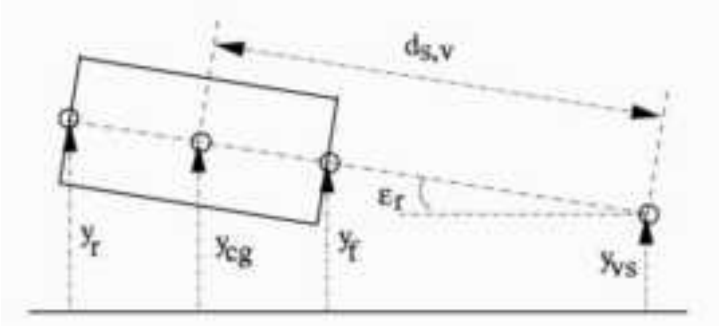


Figure 7: The Geometric Look-Ahead Scheme

In the geometric-look ahead scheme, the lateral error (y_{vs}) at the location of a virtual sensor may be approximated as

$$\begin{aligned} y_{vs}(t) &\approx y_{cg}(t) + d_{s,v}\epsilon_r(t) \\ &= \frac{d_r y_f(t) + d_f y_r(t)}{d_f + d_r} + d_{s,v}\frac{y_f(t) - y_r(t)}{d_f + d_r} \end{aligned} \tag{4}$$

where $d_{s,v}$, called the virtual look-ahead distance may be chosen arbitrarily. d_f and d_r are distance of the front and rear magnetometer bank from the vehicle CG. $y_{vs}(t)$ is used as the controlled output which acts as the input to the controller. The controller, now, acts as though it were working on a vehicle with a large d_s.

Remarks:

1. It is useful to interpret Equation (4) as a weighting scheme where $d_{s,v}$ acts as the ratio of the weighting on ϵ_r and y_{cg}, respectively. Larger values of $d_{s,v}$ imply higher penalties on ϵ_r and therefore guarantee smoother rides. However, the smoother rides are achieved at the expense of lane-tracking performance (since small y_{vs} does not imply small y_{cg}).

2. The look-ahead scheme defines a structure for the controller based on a specific linear combination of certain outputs. The reason why this structure has been adopted is its intuitively appealing nature. Similar or better performance can be obtained by using linear optimal control schemes with appropriate weighting on the outputs that are to be maintained small. However, deciding on such weights has not proven to be an easy exercise.

3. The control implemented in Demo'97 is a modified version of the scheme presented above where the look-ahead distance (d_{sv}) varies with time (or equivalently the Laplace variable in the s-domain). Varying d_{sv} is an ad-hoc way of accounting for the variation in the lateral dynamics at different longitudinal velocities. However, the salient features of this modified scheme remain the same.

4.2 Shortcomings of the Geometric Look-Ahead Scheme

Though the geometric look-ahead scheme provides a framework to achieve smooth control action, it does not work under hard failure in the magnetometers. Here, we provide some intuition to why this is so.

The geometric look-ahead scheme is based, as the name suggests, on constructing the lateral error at the location of a virtual sensor through geometric extrapolation. The success of this scheme, therefore, is critically dependent on whether it receives the correct value of the lateral error information or not, especially when higher values of $d_{s,v}$ are used. For example, consider the situation that the signal processing algorithm outputs a value of zero for the lateral error measured by the front bank of magnetometers (this condition can occur under the severance of the communication link between the magnetometer and the signal processing algorithm). Assume that the look-ahead distance, $d_{s,v}$ is chosen to be a large value. As suggested in Figure 8, in this situation, the value of $\tilde{y}_{vs}$ as calculated by the geometric look-ahead scheme will be significantly different from the "actual" lateral error (y_{vs}) at a distance ($d_{s,v}$)

in front of the vehicle CG. Figure 8 also suggests that there exist specific situations where the lateral error computed by the algorithm may indeed have a sign opposite to that of the lateral errors at the locations of both the front and rear magnetometers. Intuitively then, one can expect stability problems to result.

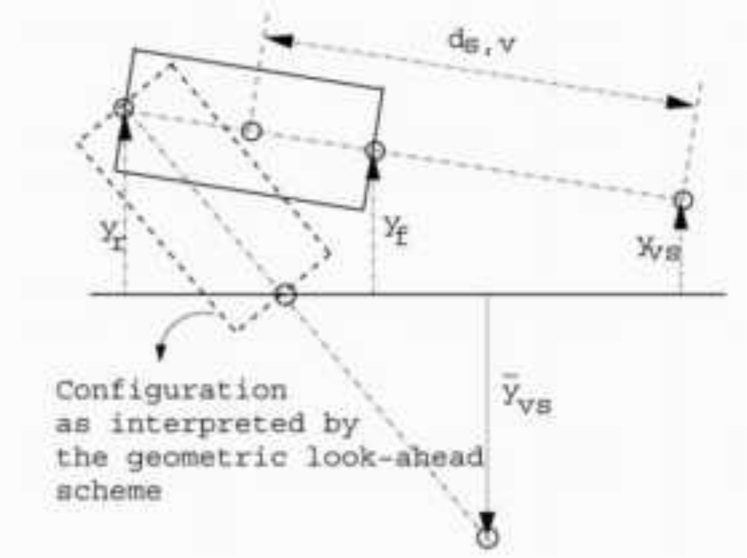


Figure 8: Look-ahead error under failure

It is useful to note that under the failure described above, the larger the value of $d_{s,v}$, the larger the discrepancy between the lateral error predicted by the geometric look-ahead scheme ($\tilde{y}_{vs}$) and the "actual" lateral error at a distance $d_{s,v}$ in front of the vehicle CG (y_{vs}). This suggests that if failure tolerance is required of the geometric look-ahead scheme, smaller look-ahead distances would work better. However, we also observed that smaller look-ahead distances imply jittery control action.

The above discussion suggests a fundamental trade-off between fault tolerance and control performance. Later we derive a strict limit on how large $d_{s,v}$ can be in order that the geometric look-ahead scheme may be modified to incorporate failure tolerance.

5 Simultaneous Stabilization

5.1 Generic Case

The simultaneous stabilization problem is:
Given a finite number finite dimensional linear-time invariant (FDLTI) systems $P_0, P_2, \cdots, P_n$, design a single controller (also FDLTI) that minimizes a certain performance specification for the feedback interconnection (P_0, C) subject to the constraint that each of the feedback interconnections (P_i, C) is internally stable for $i = 0, 1, \cdots, n$.

The simultaneous stabilization can be linked to the fault tolerant control problem in a natural way if it is interpreted as the problem of design of a controller that is insensitive to certain failures that may occur during system operation. The parallel becomes obvious if we interpret P_0 as the linearized dynamics describing non-faulty operation of a system and each of the $P_i^{'}s$ $(i \neq 0)$ as the dynamics representing a particular failed scenario (which we would like to make the control system insensitive to). The performance criterion is included to ensure that the failure tolerant controller performs satisfactorily under the no-fault scenario.

We define S as the set of all *proper, stable real rational* transfer functions. The following lemma has been proven in [8]

Lemma 5.1. *Let $P_0, P_1, \cdots, P_n$ be strictly proper SISO LTI systems. Then $\exists N_i, D_i X_i, Y_i \in \mathcal{S}$, (i=0,1,...,n) such that $P_i = \frac{N_i}{D_i}$ and $X_i N_i + Y_i D_i = 1$, (i=0,1,...,n). Define $V_{0j} := Y_0 D_j + X_0 N_j$ and $W_{0j} := -N_0 D_j + D_0 N_j$, (j=1,2,...,n) and $R_{0j} := W_{0j} V_{0j}^{-1}$. Assume that $R_{0j} \in \mathcal{S}$ for every $j \in \{1, 2, \cdots, n\}$. Then $P_0, P_1, \cdots, P_n$ are simultaneously stabilizable if there exists $Q \in \mathcal{S}$ such that $\|QR_{0j}\|_\infty < 1, j \in \{1, 2, \cdots, n\}$.*

With this lemma in mind, the design problem becomes
Design a controller C, which minimizes a weighted sensitivity function (for the feedback interconnection (P_0, C)) while guaranteeing simultaneous stability of LTI sys-

tems $P_0, P_1, \cdots, P_n$. More specifically, consider the problem:

$$\min_{Q \in \mathcal{S}} \|W_y(Y_0 - N_0 Q) D_0 G_0\|_\infty \tag{5}$$

subject to $\|QR_{0j}\| < 1, j = 1, 2, \cdots, n$.

Here R_{0j},j=1,2,...,n are defined in Lemma 5.1. It is assumed that $R_{0j} \in \mathcal{S}$ for every $j \in \{1, 2, \cdots, n\}$. The performance is chosen to represent a disturbance rejection problem where G_0 represents the disturbance dynamics and W_y is a frequency-shaped weight on the controlled output.

This problem can be treated as a standard $\mathcal{H}_\infty$ problem (Figure 9). The augmented plant acts as the "generalized plant" and Q as the "stabilizing controller" for the generalized plat. The cost function to be minimized may be interpreted as $\mathcal{H}_\infty$ norm from signal d to z_1 to z_2.

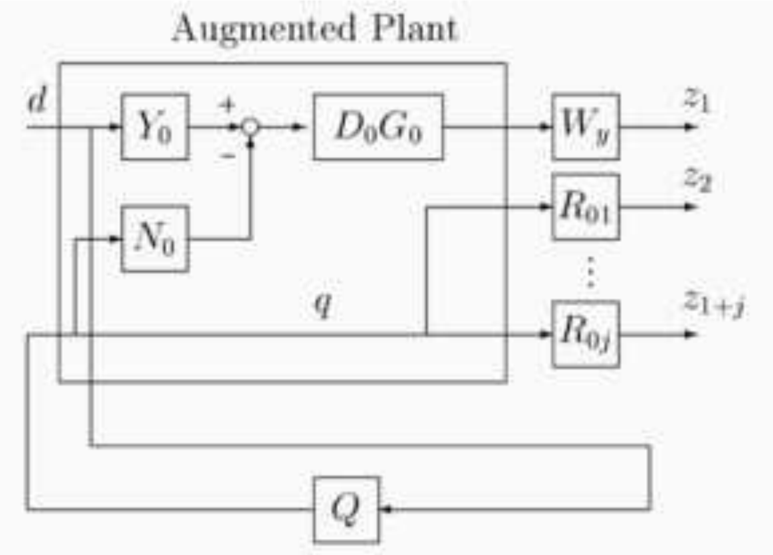


Figure 9: Augmented Plant for the design of Q

The summary of the design procedure is as follows:

- Step 1: Decide on coprime factorizations (ovser $\mathcal{S}$) of plants $P_0, P_1, \cdots, P_n$ such that they yield stable R_{0j},j=1,2,...,n.

- Step 2: Specify the weighting function W_y and a model of the disturbance dynamics G_0.

- Step 3: Find the solution Q for the above $\mathcal{H}_\infty$ control problem

- Step 4: If $\|QR\|_\infty \geq 1$ or if $Q \notin \mathcal{S}$, modify W_y (for example, reduce the gain and/or cutoff frequency) and go to step 3.

Remark: It should be noted that the above procedure does not guarantee a solution due to the following reasons:

1. In Step 1, it is assumed that we will be able to determine appropriate co-prime factorization representations to yield stable R_{0j}. This is possible only in select situations.

2. The $\mathcal{H}_\infty$ design procedure does not guarantee that the stabilizing controller is itself stable. Therefore, it may be the case that Step 3 returns an unstable Q.

5.2 Lane-Keeping Controller Design

In this subsection, we present the application of the procedure developed in subsection 5.1 to the problem of design of a fault tolerant lane-keeping controller which is insensitive to severance of either one of the communication links between the front and rear bank of magnetometers and the control computer. This failure will be modeled as the output of the faulty magnetometer bank being set to zero. We will assume that the controller utilizes a geometric look-ahead based structure. The reason for this choice of structure is to highlight the shortcomings of the geometric look-ahead scheme and modify it so that it can accommodate the failure scenarios described above.

Problem formulation: For a fixed longitudinal velocity, let P_{NF} denote the LTI system descirbed by the linearized lateral vehicle dynamics associated with the non-faulty operation of the system, and let P_f and P_r be the LTI systems associated with the situations corresponding to the failure of the rear and front magnetometer banks respectively. Assuming a geometric look-ahead based control structure with a look-ahead distance $d_{s,v}$, plants P_{NF}, P_F and P_r may be represented as:

$$
\begin{aligned}
P_{NF} &\sim \left[\begin{array}{c|cc} A & B_1 & B_2 \\ \hline C_0 & 0 & 0 \end{array}\right] \\
P_f &\sim \left[\begin{array}{c|cc} A & B_1 & B_2 \\ \hline C_f & 0 & 0 \end{array}\right] \\
P_r &\sim \left[\begin{array}{c|cc} A & B_1 & B_2 \\ \hline C_r & 0 & 0 \end{array}\right]
\end{aligned}
$$

where A, B_1, B_2 are as described in section 3 and C_0, C_f, C_r are:

$$
\begin{aligned}
C_0 &= \frac{\{(d_r + d_{s,v})C_{fs} + (d_f - d_{s,v})C_{rs}\}}{d_f + d_r} \\
C_f &= \frac{(d_r + d_{s,v})C_{fs}}{d_f + d_r} \\
C_r &= \frac{(d_f - d_{s,v})C_{rs}}{d_f + d_r}
\end{aligned}
\qquad (6)
$$

where $C_{fs} = [\ 1 \quad 0 \quad d_f \quad 0\ ], C_{rs} = [\ 1 \quad 0 \quad -d_r \quad 0\ ]$. d_f and d_r are the distance between the vehicle CG and the location of the front and rear magnetometer banks respectively. For the passenger cars used by PATH, $d_f \approx 2.06m$ and $d_r \approx 1.96m$.

Given coprime factorization representations $(N_0, D_0), (N_1, D_1)$ and (N_2, D_2) (over $\mathcal{S}$) of the transfer functions associated with P_{NF},P_f andP_r respectively, there exist X_i, Y_i such that $X_iN_i + Y_iD_i = 1,\ i = 0, 1, 2$. Let V_{0i}, W_{0i} and R_{0i} be defined as follows $V_{0i} = Y_0D_i + X_0N_i, W_{0i} = -N_0D_i + D_0N_i$ and $R_{0i} = W_{0i}V_{0i}^{-1}$. The design problem we are interested in solving is

$$\min_{Q \in \mathcal{S}} \|W_y(Y_0 - N_0Q)D_0G_0\|_\infty$$

subject to $\|QR_{01}\|_\infty < 1, \|QR_{02}\|_\infty < 1$. The cost in the optimization problem reflects the performance of the system under no-fault operation (system dynamics governed by P_{NF}). The constraints captures the requirement for simultaneous stability of the plant pairs P_{NF}, P_f and P_{NF}, P_r. It should be noted that in this formulation we have assumed that $R_{0i}, i = 1, 2$ are stable.

W_y represents a penalties on the effect of the disturbance on control performance (lateral error) and the disturbance (road curvature). W_y is modeled as a first order filter of the form:

$$W_y = \frac{1}{2}\frac{s + 0.2\pi}{s + 0.004\pi}$$

High frequency components of the lateral error measurement are attributed to noise. This is because the vehicle dynamics are slow and the road curvature is piecewise constant. Therefore, the penalty on lateral error is set high only at low frequencies.

G_0 represents disturbance dynamics. G_0 is modeled as:

$$G_0 = \frac{1}{400}\frac{s^2 + 2\zeta_1\omega_1 s + \omega_1^2\omega_2^2}{s^2 + 2\zeta_2\omega_2 s + \omega_1^2\omega_2^2}$$

where $\omega_1 = 20\pi, \zeta_1 = \zeta_2 = 0.7$ and $\omega_2 = 2\pi$.

The choice of the above model is motivated by the observation that lateral disturbances acting on the vehicle can be transformed to equivalent curvature disturbances. The maximum magnitude of curvature disturbances is assumed to be $\frac{1}{400}m$ (this is a harsh disturbance at highway speeds). Since the road curvature does not change frequently on highways, we choose a low pass filter disturbance model.

We make the following interesting observations.

1. The pair of plants P_{NF}, P_f is simultaneously stabilizable if and only if $d_{s,v} < d_f$
2. The pair of plants P_{NF}, P_r is simultaneously stabilizable if and only if $d_{s,v} > -d_r$

The first observation introduces a condition which represents a trade-off between fault tolerant action and non-faulty control performance. To see this, note that this observation implies that in order to realize failure tolerance, the look-ahead distance need to be restricted to $d_{s,v} < d_f$. In other words, the condition for failure tolerance implies that look-ahead distance should be restricted to within the physical limits of the vehicle. Small look-ahead distances imply jittery control action and therefore contribute to poor no-fault performance.

6 Dedicated Observers

6.1 Problem Formulation

Consider a two-output LTI system (say P_0) described as:

$$\begin{aligned} \dot{x}(t) &= Ax(t) + B_1 u(t) + B_2 d(t) \\ y(t) &= \begin{bmatrix} C_1 \\ C_2 \end{bmatrix} x(t) + \begin{bmatrix} D_{12} \\ D_{22} \end{bmatrix} d(t) \end{aligned}$$

where $A \in \mathbb{R}^{n \times n}, B \in \mathbb{R}^{n}, C_1 \in \mathbb{R}^{1 \times n}, C_2 \in \mathbb{R}^{1 \times n}$. As is customary, P_0 may be represented as:

$$P_0 \sim \left[\begin{array}{c|cc} A & B_1 & B_2 \\ \hline C_1 & 0 & D_{12} \\ C_2 & 0 & D_{22} \end{array} \right]$$

Now, define two other two-output LTI systems P_1 and P_2 as:

$$\begin{aligned} P_1 &\sim \left[\begin{array}{c|cc} A & B_1 & B_2 \\ \hline 0 & 0 & \tilde{D}_{12} \\ C_2 & 0 & D_{22} \end{array} \right] \\ P_2 &\sim \left[\begin{array}{c|cc} A & B_1 & B_2 \\ \hline C_1 & 0 & D_{12} \\ 0 & 0 & \tilde{D}_{22} \end{array} \right] \end{aligned}$$

The following problem is considered here: Design an LTI controller such that each of the feedback interconnections (P_i, K),i=0,1,2 is internally stable.

Note: P_1 and P_2 may be interpreted as LTI systems describing failed systems affecting only one of two outputs. The effect of the failures is modeled as the output of the faulty sensor going to a constant after the occurrence of the failure. In other words, effect of the failures are modeled as:

- Effect of failure in the first output $y_1(t)$:

$$y_1(t) = \begin{cases} C_1x(t) + D_{12}d(t) & \text{for } 0 \leq t < t_1 \\ \tilde{D}_{12}d(t) & \text{for } t \geq t_1 \end{cases}$$

- Effect of failure in second output $y_2(t)$

$$y_2(t) = \begin{cases} C_2x(t) + D_{22}d(t) & \text{for } 0 \leq t < t_2 \\ \tilde{D}_{22}d(t) & \text{for } t \geq t_2 \end{cases}$$

Equivalently, y_1 and y_2 may be written as: $y_i(t) = C_ix(t) + D_{i2}d(t) + f_i(t)$, i=1,2 where

$$\begin{aligned} f_1(t) &= \begin{cases} 0 & \text{for } 0 \leq t < t_1 \\ -C_1x(t) - D_{12}d(t) + \tilde{D}_{12}d(t) & \text{for } t \geq t_1 \end{cases} \\ f_2(t) &= \begin{cases} 0 & \text{for } 0 \leq t < t_2 \\ -C_2x(t) - D_{22}d(t) + \tilde{D}_{22}d(t) & \text{for } t \geq t_2 \end{cases} \end{aligned}$$

The constant signal (the output goes to) is subsumed by an appropriate choice of signals that comprise $d(t)$.

6.2 Dedicated Observer Based Control

In this subsection, we propose a Dedicated Observer based control structure to solve the problem described above. A description of this system follows.

First note that P_0,P_1 and P_2 represent linear maps form the inputs (u, d) to the outputs (y_1,y_2). In the control structure proposed here, we augment this map by including a Dedicated Observer system (DO) in cascade with P_0,P_1, or P_2 (Figure 10). The Dedicated Observer system (DO) represents a linear map from outputs(y_1,y_2) to independent estimates $(\hat{x}_1, \hat{x}_2)$ of the state x. More specifically, $\hat{x}_1$ and $\hat{x}_2$ are estimates generated using observers (with a Luenberger structure) each of which process only one of the two outputs.

$$
\begin{aligned}
DO1 \quad &: \quad \hat{x}_1 = A\hat{x}_1 + B_1 u(t) + L_1(y_1(t) - C_1\hat{x}_1) \\
DO2 \quad &: \quad \hat{x}_2 = A\hat{x}_2 + B_1 u(t) + L_2(y_2(t) - C_2\hat{x}_2)
\end{aligned}
$$

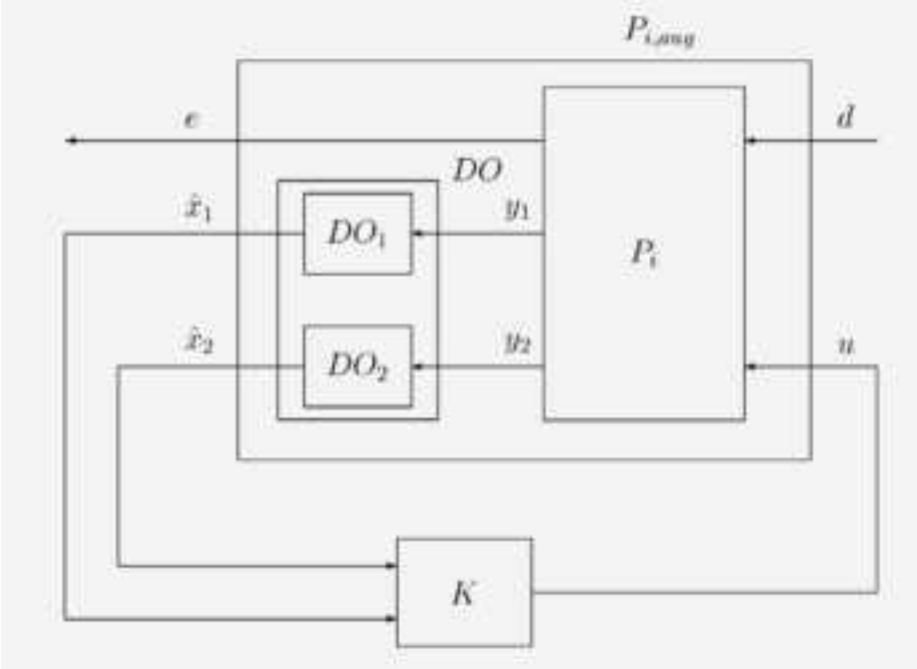


Figure 10: Dedicated Observer Based Control Structure

It is then easy to verify that the following are state-space realizations of LTI systems $P_{0,aug}$, $P_{1,aug}$, and $P_{2,aug}$

$$P_{0,aug} \sim \left[\begin{array}{ccc|cc} A & 0 & 0 & B_1 & B_2 \\ L_1C_1 & A - L_1C_1 & 0 & B_1 & 0 \\ L_2C_2 & 0 & A - L_2C_2 & B_1 & 0 \\ \hline 0 & I & 0 & 0 & L_1D_{12} \\ 0 & 0 & I & 0 & L_2D_{22} \end{array}\right]$$

$$P_{1,aug} \sim \left[\begin{array}{ccc|cc} A & 0 & 0 & B_1 & B_2 \\ 0 & A - L_1C_1 & 0 & B_1 & 0 \\ L_2C_2 & 0 & A - L_2C_2 & B_1 & 0 \\ \hline 0 & I & 0 & 0 & L_1\tilde{D}_{12} \\ 0 & 0 & I & 0 & L_2D_{22} \end{array}\right]$$

$$P_{2,aug} \sim \left[\begin{array}{ccc|cc} A & 0 & 0 & B_1 & B_2 \\ L_1C_1 & A - L_1C_1 & 0 & B_1 & 0 \\ 0 & 0 & A - L_2C_2 & B_1 & 0 \\ \hline 0 & I & 0 & 0 & L_1D_{12} \\ 0 & 0 & I & 0 & L_2\tilde{D}_{22} \end{array}\right]$$

Note that in the LTI systems, $P_{i,aug},\ i = 1,2$ the estimates $\hat{x}_i$ $(i = 1,2)$ are corrupted because of erroneous sensor readings provided to the corresponding dedicated observer.

The motivation for such an augmentation becomes clear if the observer gains L_1 and L_2 are chosen to be small. In this case, plants $P_{0,aug}$,$P_{1,aug}$ and $P_{2,aug}$ ”look” similar. In other words, for small L_1 and L_2, the difference between the estimates $\hat{x}_1,\ i = 1,2$ in the three LTI systems $P_{i,aug},\ i = 0,1,2$ is small. Therefore, if a controller K is chosen such that the feedback interconnection $(P_{0,aug}, K)$ is ”robustly” stable, then it is not unreasonable to expect that the feedback interconnection $(P_{1,aug}, K)$ and $(P_{2,aug}, K)$ will be stable as well.

In summary, for a two-output LTI system, $P_0 \sim \left[\begin{array}{c|c} A & B \\ \hline C & D \end{array}\right]$, a dedicated observer based control structure can be constructed as follows:

- Step 1: Design stable Luenberger observers with "small" observer gains L_1 and L_2. For example, a Kalman Filter design with a large fictitious sensor noise can be used to obtain low observer gains.

- Step 2: Design a controller K for the augmented plant $P_{0,aug}$ such that the controller guarantees good robust stability properties for the feedback interconnection $(P_{0,aug,}, K)$. The dedicated observer based controller is then give by : $C_{ded} = K \cdot DO$.

Remark: Philosophically, low values of observer gains imply low confidence level in the outputs (accounting for the possibility of failure in the sensors). Since this scheme uses low values for observer gains, practical application of his heuristic depends critically on the quality of the model P_0. In other words, if the model P_0 is a "close-enough" approximation of the physical system under control, then one can expect this scheme to be successful. On the other hand, if large values of observer gains are required to achieve faithful estimates of the states of the system, then the plants $P_{i,aug},\ i = 0, 1, 2$ can potentially be significantly different. Then it will be difficult to find a controller K that works stabilizes the all three feedback interconnection $(P_{i,aug}, K),\ i = 0, 1, 2$.

6.3 The observer Based Look-Ahead Scheme

In this subsection, a lane-keeping control scheme based on the concept of **Observer Based Look-Ahead** is introduced. This scheme (Figure 11) works as follows. Two observers, DO_f and DO_r, each processing only one lateral error output (DO_f processes y_f and DO_r processes y_r) are used to generate independent estimates of the states of the system. These states are combined (in a manner similar to that of the geometric look-ahead scheme) to generate independent estimates, $(\hat{y}_{vs})_f$ and $(\hat{y}_{vs})_r$, of the lateral error at the location of a virtual sensor. $(\hat{y}_{vs})_f$ and $(\hat{y}_{vs})_r$ are weighted depending on the confidence level in each of the outputs to generate an estimate, $\hat{y}_{vs}$, of the lateral error at the location of a virtual sensor. $\hat{y}_{vs}$ is then fed to a "controller" that computes the desired angle.

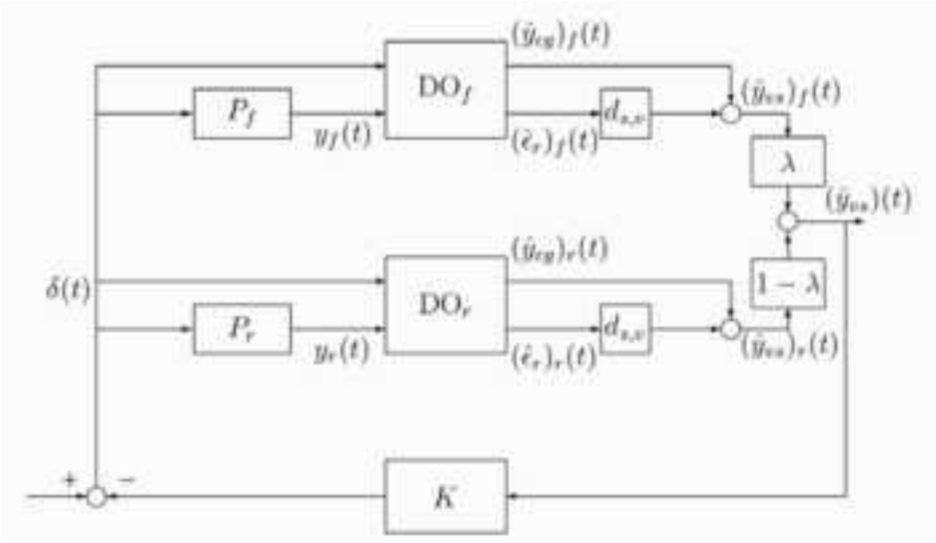


Figure 11: Observer Based Look-Ahead Scheme

The equation that govern the dynamics of the observers (DO_f and DO_r) are:

$$\begin{aligned} DO1 &: \dot{\hat{x}}_1 = A\hat{x}_1 + B_1u(t) + L_f(y_f(t) - C_f\hat{x}_1) \\ DO2 &: \dot{\hat{x}}_2 = A\hat{x}_2 + B_1u(t) + L_r(y_r(t) - C_r\hat{x}_2) \end{aligned}$$

The observer gains L_f and L_r are chosen based on a Kalman filter design methodology where a suitably low confidence level is placed on the sensor outputs. The lateral error at the location of a virtual sensor (at distance $d_{s,v}$ in front of the vehicle CG) is constructed as follows:

$$\begin{aligned} (\hat{y}_{vs})_f(t) &= (\hat{y}_{cg})_f(t) + d_{s,v}(\hat{\epsilon}_r)_f(t) \\ (\hat{y}_{vs})_r(t) &= (\hat{y}_{cg})_r(t) + d_{s,v}(\hat{\epsilon}_r)_r(t) \\ \hat{y}_{vs}(t) &= \lambda(t)(\hat{y}_{vs})_f(t) + (1-\lambda)(t)(\hat{y}_{vs})_f(t) \end{aligned} \tag{7}$$

where $\lambda \in [0, 1]$ is chosen based on the confidence level of the output of the magnetometers. The confidence level is set in real-time based on the result of a failure detection process. In the case of the hard failure in the magnetometers, detection of the failure is almost immediate the therefore λ can be modified quickly. For example, if the rear magnetometer fails, λ is changed from 0.5 to 1 indicating that the system trusts the estimate of the front sensor more.

The controller K is chosen to be identical with the controller used under the geometric look-ahead scheme.

The following notes highlight the salient features of this scheme.

1. Under no-fault operation performance similar to no-fault geometric look-ahead performance can be obtained. To see this, note that in the observer based scheme the "controller" K processes an estimate of the lateral error at the location of a virtual sensor which is constructed based on vehicle lateral dynamics (as opposed to a geometric construction used in the geometric look-ahead scheme). Therefore, if the observers generate reliable estimates of the states of the vehicle (as described in the Bicycle Model), then on can expect that the estimate of the lateral error as predicted by the observer based look-ahead scheme would math up with its geometric counterpart. As was noted in the previous section, for small observer gains, the quality of the estimates of the observers depend heavily on the quality of the model describing the dynamics.

2. This scheme is a replica of the dedicated observer based control architecture albeit with added structure (the additional structure is in the form of a specific linear combination of the independent estimates of the states of the system). Therefore, failure tolerance properties highlighted in the previous subsection translate directly to this application (provided L_f and L_r are maintained small).

3. In this scheme no restriction is placed on the look-ahead distance $d_{s,v}$. In other words, this scheme guarantees failure tolerance even if large look-ahead

distances are chosen. Recall from Section 4 that utilizing large look-ahead distances leads to favorable yaw damping characteristics and smoother steering especially under high-speed operation.

We conclude this presentation with a few remarks comparing the observer-based look ahead and the geometric look-ahead scheme. The geometric look-ahead scheme is based on a geometric extrapolation of the lateral errors sensed by the two magnetometers to construct the lateral error at the location of a virtual sensor. The quality of the estimate of the lateral error at the location of the virtual sensor is susceptible to severe degradation in the event of failure of either one of the magnetometers. In comparison, the observer-based scheme does not rely on sensor measurements alone. This scheme utilizes the system model to estimate the lateral error at the location of the virtual sensor and is therefore more robust to failure in the sensors. The flip-side is that the observer-based scheme relies on the accuracy of the system model. Therefore, it cannot accommodate model uncertainty efficiently and its performance, therefore, is likely to be sensitive to operating conditions.

7 Observer-based FDI

In this section, we present another observer-based fault tolerant control scheme, which explicitly exploits *fault detection and identification* (FDI) mechanism. Whenever faults took place, they are first detected and identified by FDI. The controller is then reconfigured according to the result of FDI. By sensor fault identification we mean to distinguish the healthy sensor from the faulty one. We are more concerned about the *source* (front or rear magnetometers) of faults than its *types* (bias, disconnection, etc.).

The essential step in FDI is *residual generation.* Residuals are small when there are no faults and significantly large when faults occur. Residuals must be sensitive to faults while robust to disturbances as well as model uncertainties. Meanwhile, residuals should exhibit unique patterns (called *fault signatures*) for different faults. Faults can then be identified by recognizing these signatures. In this report, we concentrate on generating recognizable fault signatures. Hence we assume the vehicle runs along a straight line.

Fault detection is relatively easy because the discrepancy between the information contained in both magnetometers indicates the occurrence of faults. Fault identification is difficult if only two sensors are available. How do we distinguish the healthy sensor from the faulty one when their measurements are inconsistent? Insufficient redundancy can be made up by exploiting dynamic relations between sensor outputs, i.e. observers should be involved in FDI. Once the faulty sensor is detected and identified, its output is replaced and synthesized by the healthy sensor; hence the same controller can be applied to the both normal and sensor failure cases.

7.1 Observer-based FDI structure

Overall Structure

Figure 12 is the flowchart of the proposed fault tolerant control system with observer-based FDI. The failure is *detected* first, and then the faulty sensor is *identified.* After that, the output of the faulty sensor is *reconstructed* from the output of the healthy sensor. The lateral control system enters the degraded mode that guarantees stability and an acceptable level of performance.

Figure 13 is the block diagram of the proposed observer-based FDI. The observability properties of the bicycle model imply that we can build two observers each of which is driven by a single sensor output. In order to avoid the state estimated by either observer totally becoming wrong under sensor failures, we fuse the sensor output and the estimated output from the other observer before they enter the observer. Fusion blocks in Figure 13 play the role of switches which select the healthy signal. The post-filters are designed such that the transfer functions from fault signals to residuals r_i's have consistent behavior and facilitate fault identification. The weight

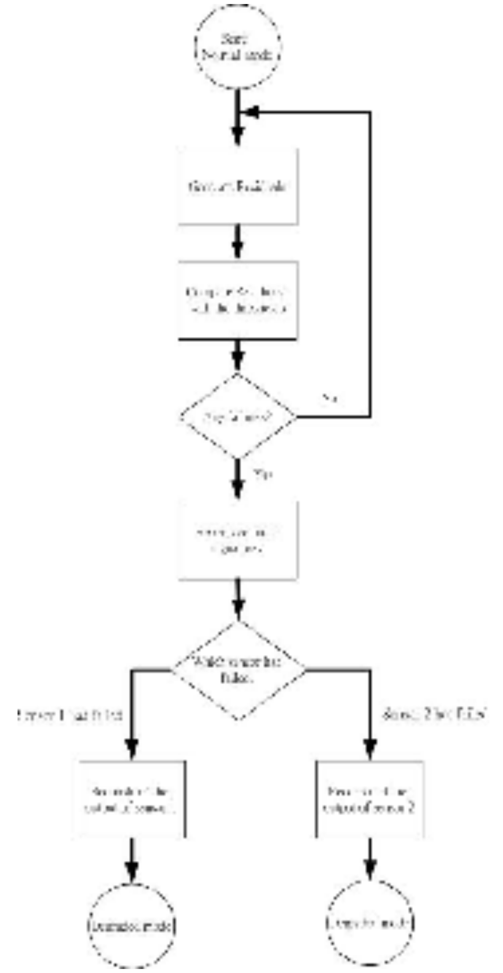


Figure 12: Flowchart of the proposed fault tolerant control system with observer-based FDI

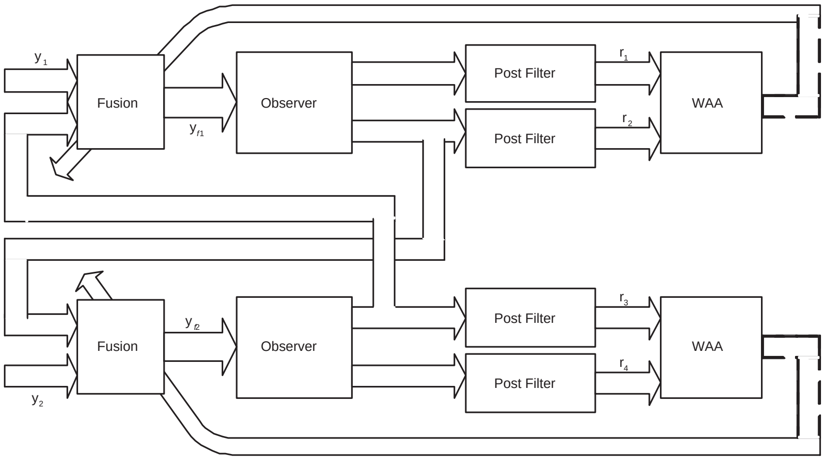


Figure 13: Block diagram of the observer-based FDI

adjustment algorithm (WAA) adjusts the weighting factors in the fusion block. The details of each block are described in the following subsections.

Plant Model

The bicycle model in Section 3 is adopted here. For easy reference, we rewrite the state equation below. Readers are encouraged to review Section 3 for detailed discussion of the bicycle model.

$$\dot{\mathbf{x}}(t) = \mathbf{A}\mathbf{x}(t) + \mathbf{B_1}\delta(t)$$

We assume the vehicle runs along a straight line and hence assume the disturbance caused by the road curvature is zero.

The output equation is

$$\mathbf{y} = \begin{bmatrix} y_1 \\ y_2 \end{bmatrix} = \mathbf{C}\mathbf{x} + \mathbf{D}_f f = \begin{bmatrix} \mathbf{C}_1 \\ \mathbf{C}_2 \end{bmatrix} \mathbf{x} + \mathbf{D}_f f$$

,where y_1 and y_2 are outputs of the front and rear magnetometers respectively. f

is the additive sensor fault signal and

$$\mathbf{D}_f = \begin{cases} [1\ 0]^T & \text{for failure of the front sensor} \\ [0\ 1]^T & \text{for failure of the rear sensor} \end{cases}$$

The particular choice of $\mathbf{D}_f$ implies that at any time at most one sensor fails. But it does not exclude the possibility that both sensors fail intermittently or two sensors fail taking turns. The additive fault signal f can be used to model all sensor faults that we are interested in. For example, if the communication link between the front magnetometer and the controller is severed, we model this situation as $y_1 \equiv 0$, i.e. $f = -\mathbf{C}_1\mathbf{x}$. Another example is when the vehicle's on-board sensing module for y_1 has detected faults, y_1 is set to its maximum value (≈ 0.5), i.e. $f = -\mathbf{C}_1\mathbf{x} + 0.5$.

Output Fusion

Output fusion is a convex combination of the sensor output and the estimated output from the other observer:

$$y_{fi} = (1 - \lambda_i)y_i + \lambda_i \hat{y}_i^j \qquad \text{i,j=1,2} \tag{8}$$

where $\hat{y}_i^j$ is the estimate of the i-th output from the j-th observer. The *weights* $\lambda_i \in [0, 1]$ are adjusted on-line. When there is no fault, $\lambda_i = 0$, i=1,2. The fused output y_{fi} is identical to the sensor output y_i. When faults occur, the corresponding λ_i increases towards 1. $\lambda_i = 1$ indicates the sensor output is incorrect and is not taken into account at all.

Observers

The observers switch between two configurations according to the relative size of weights λ_i:

If $\lambda_1 < \lambda_2$, then

$$\begin{aligned} \dot{\hat{\mathbf{x}}}_1 &= \mathbf{A}\hat{\mathbf{x}}_1 + \mathbf{B}_1\delta + \mathbf{L}_1(y_{f1} - \hat{y}_1^1) + \lambda_1\mathbf{L}_1\mathbf{C}_1(\hat{\mathbf{x}}_1 - \hat{\mathbf{x}}_2) & (9) \\ \dot{\hat{\mathbf{x}}}_2 &= \mathbf{A}\hat{\mathbf{x}}_2 + \mathbf{B}_1\delta + \mathbf{L}_2(y_{f2} - \hat{y}_2^2) & (10) \end{aligned}$$

else

$$\dot{\hat{\mathbf{x}}}_1 = \mathbf{A}\hat{\mathbf{x}}_1 + \mathbf{B}_1\delta + \mathbf{L}_1(y_{f1} - \hat{y}_1^1) \tag{11}$$

$$\dot{\hat{\mathbf{x}}}_2 = \mathbf{A}\hat{\mathbf{x}}_2 + \mathbf{B}_1\delta + \mathbf{L}_2(y_{f2} - \hat{y}_2^2) + \lambda_2\mathbf{L}_2\mathbf{C}_2(\hat{\mathbf{x}}_2 - \hat{\mathbf{x}}_1) \tag{12}$$

Observers (9)-(12) are variations of Luenberger observers with the fused outputs y_{fi} replacing sensor outputs y_i. Observability of the bicycle model does not guarantee $\hat{\mathbf{x}}_i$'s converge to $\mathbf{x}$, i=1,2, because two observers are coupled via fusion blocks. However, we can prove the stability of the observers under the *slowly-varying* conditions [6].

Post-Filters

Let $\mathbf{e}_y^T = [e_{y1}, e_{y2}, e_{y3}, e_{y4}] = [y_1 - \hat{y}_1^1, y_1 - \hat{y}_1^2, y_2 - \hat{y}_2^1, y_2 - \hat{y}_2^2]$ be the output estimation error. Residuals are generated by filtering $\mathbf{e}_y$ through post-filters $\mathrm{M}_i(s)$, i.e. $r_i = \mathrm{M}_i e_{yi}$, i=1,2,3,4. $\mathrm{M}_i(s)$ shapes the transfer functions from the fault signal f to residuals such that residuals from two observers are comparable in magnitude. Note that r_1 and r_2 are related to the front sensor and r_3 and r_4 are related to the rear sensor. Faults are detected according to the following rule:

Detection: If $\max(\|[r_1, r_2]\|, \|[r_3, r_4]\|) > T$ for some prescribed threshold T, then the fault has occurred.

Here $\| \bullet \|$ denotes Euclidean norm at each time instant. Since model uncertainty and sensor noise also contribute to nonzero residuals under the normal operation, the threshold T must be large enough to alleviate false alarms while small enough to avoid missed alarms. It is usually determined by observing the experimental data. We do not pursue theoretical analysis of the selection the of threshold T in this report.

Fault identification is more elaborate. Notice that observers (9)-(12) are coupled, i.e. failures of either sensor affect all residuals. The effects caused by the failures on the residuals are magnified or attenuated by the observers and post-filters. Therefore

$\|[r_1, r_2]\| > \|[r_3, r_4]\|$ does not necessarily conclude the failure of the front sensor. However this problem can be solved by properly-designed post-filters. We explain the post-filter design issues below.

Let the transfer functions from fault signal f to $\mathbf{e}_y$ be

$$\mathbf{V}(s) = \mathbf{C}_e \left(s\mathbf{I} - \mathbf{A}_e\right)^{-1} \mathbf{B}_e + \mathbf{D}_e \tag{13}$$

$$\text{where } \mathbf{A}_e = \begin{cases} \mathbf{A}_{e1} = \begin{bmatrix} \mathbf{A} - (1-\lambda_1)\mathbf{L}_1\mathbf{C}_1 & \mathbf{0} \\ \lambda_2\mathbf{L}_2\mathbf{C}_2 & \mathbf{A} - \mathbf{L}_2\mathbf{C}_2 \end{bmatrix} & \lambda_1 < \lambda_2 \\ \mathbf{A}_{e2} = \begin{bmatrix} \mathbf{A} - \mathbf{L}_1\mathbf{C}_1 & \lambda_1\mathbf{L}_1\mathbf{C}_1 \\ \mathbf{0} & \mathbf{A} - (1-\lambda_2)\mathbf{L}_2\mathbf{C}_2 \end{bmatrix} & \text{otherwise} \end{cases}$$

$$\mathbf{B}_e = \begin{cases} \begin{bmatrix} -(1-\lambda_1)\mathbf{L}_1 \\ 0 \end{bmatrix} & \text{for failure of the front sensor} \\ \begin{bmatrix} 0 \\ -(1-\lambda_2)\mathbf{L}_2 \end{bmatrix} & \text{for failure of the rear sensor} \end{cases}$$

$$\mathbf{C}_e = \begin{bmatrix} \mathbf{C}_1 & \mathbf{0} \\ \mathbf{0} & \mathbf{C1} \\ \mathbf{C}_2 & \mathbf{0} \\ \mathbf{0} & \mathbf{C}_2 \end{bmatrix}, \quad \mathbf{D}_e = \begin{cases} [1,1,0,0]^T & \text{for failure of the front sensor} \\ [0,0,1,1]^T & \text{for failure of the rear sensor} \end{cases},$$

Note that $\mathbf{A}_e$ and $\mathbf{B}_e$ change their values as weights are adapted and as failures take place at different sensors. It is not difficult to check that if $\lambda_1 > \lambda_2$ and the front sensor has failed, then $V_2(s) \equiv 1$ and $V_4(s) \equiv 0$. On the other hand, if $\lambda_1 < \lambda_2$ and the rear sensor has failed, then $V_1(s) \equiv 0$ and $V_3(s) \equiv 1$. However, we have to find out which sensor has failed.

If we choose post-filter M_i's such that $a_1\mathrm{M}_1\mathrm{V}_1 = \mathrm{M}_3\mathrm{V}_3$ and $a_2\mathrm{M}_4\mathrm{V}_4 = \mathrm{M}_2\mathrm{V}_2$ for some real numbers $0 < a_1, a_2 < 1$, we may claim the following identification rules:

Identification: If $\lambda_1 < \lambda_2$, and a fault has been detected, $|r_1| > |r_3|$ implies that the front sensor has failed while $|r_1| < |r_3|$ implies that the rear sensor has failed. Similarly, If $\lambda_1 > \lambda_2$ and a fault has been detected, $|r_2| > |r_4|$ implies that the front sensor has failed while $|r_2| < |r_4|$ implies that the rear sensor has failed. These rules are summarized in Table 2.

Table 2: Fault identification rules

$\lambda_1 > \lambda_2$	$\lambda_1 < \lambda_2$	
$\|r_2\| > \|r_4\|$	$\|r_1\| > \|r_3\|$	the front sensor has failed
$\|r_2\| < \|r_4\|$	$\|r_1\| < \|r_3\|$	the rear sensor has failed

To verify the identification rules, suppose we have detected any failure but do not know where it comes from. Suppose $\lambda_1 < \lambda_2$. Under these circumstances, if the front sensor has failed, then $|r_1| = |\mathrm{M}_1\mathrm{V}_1 f| > |r_3| = |\mathrm{M}_3\mathrm{V}_3 f|$ because of our choice of M_1 and M_3. If the rear sensor has failed, then $r_1 = \mathrm{M}_1\mathrm{V}_1 f \equiv 0$ and $r_3 = \mathrm{M}_3\mathrm{V}_3 f = \mathrm{M}_3 f$ due to the properties of V_1 and V_3. Therefore $|r_1| < |r_3|$. This illustrates the second column of Table 2. Similar arguments can be applied to the first column of Table 2.

Let us take a closer look at the post filter design problem. If the front sensor has failed and $\lambda_1 < \lambda_2$, from (13) we have:

$$\begin{aligned}
\mathrm{V}_1(s) &= -(1-\lambda_1)\mathbf{C}_1\Big(s\mathbf{I} - \mathbf{A} + (1-\lambda_1)\mathbf{L}_1\mathbf{C}_1\Big)^{-1}\mathbf{L}_1 + 1 = \frac{n_1(s)}{d(s)} \\
\mathrm{V}_3(s) &= -(1-\lambda_1)\mathbf{C}_2\Big(s\mathbf{I} - \mathbf{A} + (1-\lambda_1)\mathbf{L}_1\mathbf{C}_1\Big)^{-1}\mathbf{L}_1 = \frac{(1-\lambda_1)n_3(s)}{d(s)}
\end{aligned}$$

where $(n_1(s), d(s))$ and $(n_3(s), d(s))$ are coprime pairs of polynomials. Since $n_1(s) = \det\begin{bmatrix} s\mathbf{I} - \mathbf{A} + (1-\lambda_1)\mathbf{L}_1\mathbf{C}_1 & \mathbf{L}_1 \\ (1-\lambda_1)\mathbf{C}_1 & 1 \end{bmatrix}$ [1] we have

$n_1(s) = \det\left(\begin{bmatrix} s\mathbf{I} - \mathbf{A} & \mathbf{L}_1 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} \mathbf{I} & 0 \\ (1-\lambda_1)\mathbf{C}_1 & 1 \end{bmatrix}\right) = \det(s\mathbf{I} - \mathbf{A})$ which is independent of λ_1. Similarly, $n_3(s)$ is also independent of λ_1. Now factorize $n_1(s) = n_1^+(s)n_1^-(s)$ and $n_3(s) = n_3^+(s)n_3^-(s)$, where $n_i^+(s)$ and $n_i^-(s)$, i=1,3, have their roots in the closed right half plane and open left plane respectively. Choose $\mathrm{M}_1(s) = \frac{n_3^+(s)}{n_1^-(s)k(s)}$ and $\mathrm{M}_3(s) = \frac{n_1^+(s)}{n_3^-(s)k(s)}$. $k(s)$ is a Hurwitz polynomial such that $\mathrm{M}_1(s)$ and $\mathrm{M}_3(s)$ are proper and stable. Then $(1-\lambda_1)\mathrm{M}_1(s)\mathrm{V}_1(s) = \mathrm{M}_3(s)\mathrm{V}_3(s)$. Notice that $0 < 1-\lambda_1 < 1$ as required.

Similarly, we can choose M_2 and M_4 such that $a_2\mathrm{M}_4\mathrm{V}_4 = \mathrm{M}_2\mathrm{V}_2$ for some $0 < a_2 < 1$, then the identification rule can be applied.

Weight Adjustment Algorithm (WAA)

If any fault has been detected and identified, weights λ_i, i=1,2, in fusion blocks will be adjusted on-line. Suppose the front sensor has failed, then we adjust the weights according the following 1st order differential equations:

$$\begin{aligned} \dot{\lambda}_1 &= -\alpha\left(\lambda_1 - g(\|[r_1, r_2]\|)\right) && (14) \\ \dot{\lambda}_2 &= -\alpha\lambda_2 && (15) \end{aligned}$$

If the rear sensor has failed, the adapting rule becomes

$$\begin{aligned} \dot{\lambda}_1 &= -\alpha\lambda_1 && (16) \\ \dot{\lambda}_2 &= -\alpha\left(\lambda_2 - g(\|[r_3, r_4]\|)\right) && (17) \end{aligned}$$

where $\alpha > 0$ and $g : \mathbb{R} \to [0,1]$ is the *logistic function.*

$$g(x) = \frac{1}{1+\exp^{-ax+b}} \qquad a, b > 0 \qquad (18)$$

The sufficient conditions for convergence of the estimated state are $|\dot{\lambda}_i| < \alpha$ and $\lambda_1 + \lambda_2 \leq 1$ [6]. $|\dot{\lambda}_i| < \alpha$ may be concluded immediately from (14)-(17). $\lambda_1 + \lambda_2 \leq 1$ is also satisfied [6]. The parameter α is a trade-off between stability and FDI performance. Large α makes FDI respond quickly to faults while small α is required to satisfy the slowly-varying conditions such that stability can be guaranteed.

Fault Accommodation

In order to accommodate faults, we feed the lateral controller with fused outputs y_{f1} and y_{f2} rather than sensor outputs y_1 and y_2. As we mentioned above, $y_{fi} = y_i$

when there is no fault. If fault occurs, the faulty sensor output is replaced by the observer output. The same controller can be applied to both the normal case and the sensor failure cases.

7.2 Simulation Results

In the following simulations, we set the longitudinal speed to be 10 m/sec $\approx$ 22 mph. Measurement noise is added to each magnetometer output. The measurement noise is modeled as a zero-mean, Gaussian, white noise with standard deviation 0.0075, i.e. 99% of the noise is within the rang (-0.02, 0.02).

Case I: The front sensor is disconnected for $t > 10$ sec (Figure 14). In normal operation, $y_1 \approx y_2 \approx 0$ in steady state; hence the effect of disconnected sensor is nearly unobservable at the beginning. The fault is detected at t$\approx$13 sec when its effect is accumulated such that the corresponding residual exceeds the threshold. The lateral error remains small ($<$ 15cm). Also notice that both observers can estimate states correctly after the fault took place.

Case II: The rear sensor is set to its maximum (0.5) for $t > 10$ sec (Figure 15). The fault is detected immediately and the lateral error remains small. Both observers can estimate state correctly after the fault took place.

8 Experiments: Lane-keeping Control

In this section, we document experimental results pertaining to the fault tolerant and degraded mode design problems considered in sections 5 and 6. The purpose of this exposition is to highlight experimental corroboration of analytical predictions of failure tolerant action.

The test platform for the experiments is the lane-keeping control system deployed on test vehicles[1] used by PATH.

[1] All experiments documented here were performed on Buick Le Sabre passenger cars.

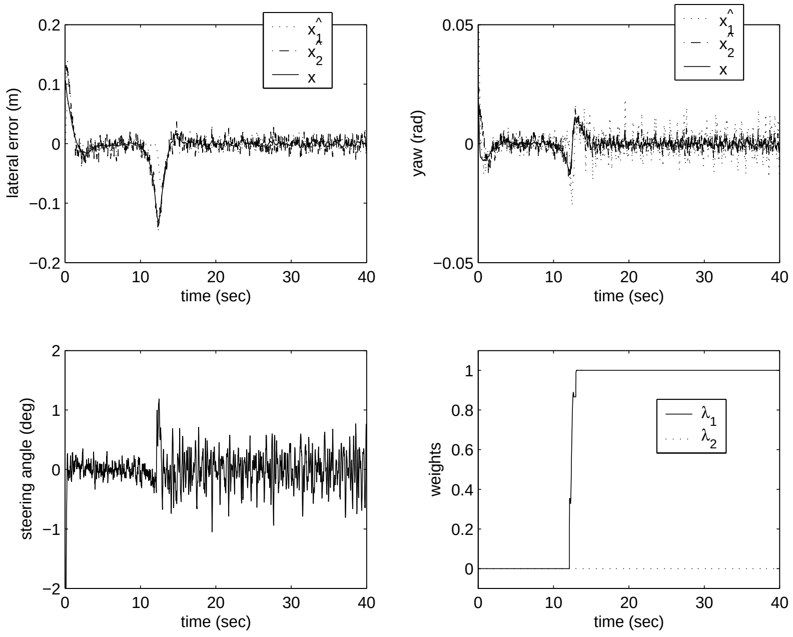


Figure 14: The front sensor is disconnect for $t > 10$

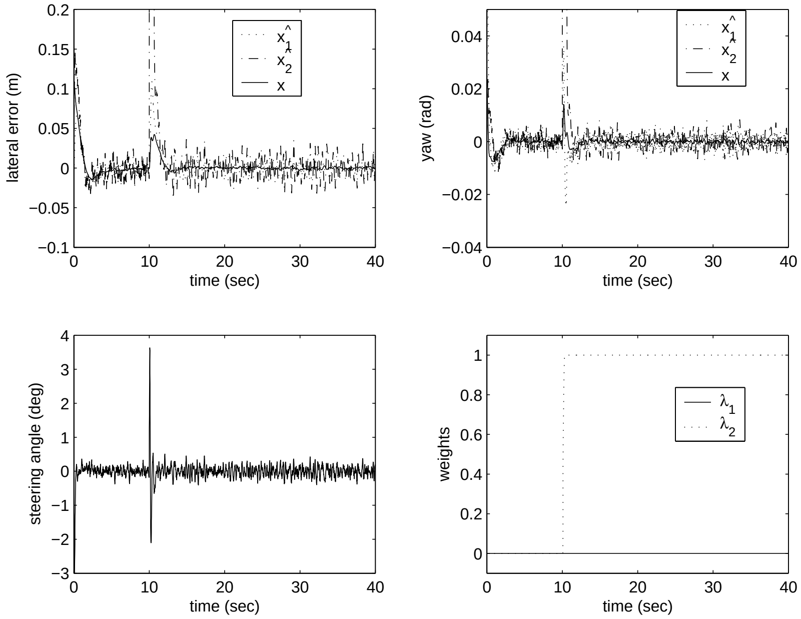


Figure 15: $y_2(t) = 0.5$ for $t > 10$

8.1 Preliminaries

This section provides background information to enable the reader to better appreciate/interpret the experimental results discussed in the next section.

The Experiments

In this section, sample results of the following experiments are documented.

1. Lane-keeping control using a controller that is designed based on simultaneous stability theory:
   - (a) High-speed test under **failure#2**[2] in **rear** magnetometer bank
   - (b) High-speed test under **failure#2** in **front** magnetometer bank
2. Lane-keeping control using controller that is designed using the observer based look-ahead scheme:
   - (a) High-speed test under **failure#1**[3] in **rear** magnetometer bank
   - (b) High-speed test under **failure#2** in **rear** magnetometer bank

Remarks:

1. In each of these experiments, the longitudinal velocity of the vehicle was controlled by a human operator.
2. Whenever necessary, failures were introduced manually by striking a key on the key board attached to the control computer. This strike was designed to prompt failure-like behavior. For example, to introduce failure#2 in the rear magnetometer bank, the key strike was used to set the value of the error sensed by the rear magnetometer bank to zero. The key strike mimics, albeit

[2] Magnetometer bank output goes to zero.

[3] Magnetometer bank output goes to maximum.

approximately, the condition of severance of the communication link between the faulty magnetometer bank and the control computer.

Implementation of Lane-keeping Controllers

The lateral dynamics of vehicles vary significantly across the spectrum of longitudinal velocities experienced by vehicles on highways. A framework to explicitly incorporate this variation into the design of lane-keeping controllers is provided in [5].

Most lane-keeping control design schemes, however, are designed for fixed longitudinal velocities, as is the case for control schemes in this report as well. In these designs, accommodation of variation in the lateral dynamics is handled in an ad-hoc, though effective, manner. Multiple lane-keeping controllers are designed at different fixed longitudinal velocities. A suitable interpolation scheme is then used to determine the controller dynamics for intermediate velocities. The choice of the interpolation methodology varies depending on the designer's preference. In the control schemes developed in this report, the controllers (designed for different fixed longitudinal velocities) were designed to have the same structure. A linear interpolation routine is used to interpolate between different values of parameters that define the controllers. In other words, suppose $C(\zeta_1, v_1)$ and $C(\zeta_2, v_2)$ represent two controllers with the same structure (here ζ_1 and ζ_2 represent parameter vectors and v_1, v_2 with $v_1 < v_2$ represent velocities), then the controller dynamics at a velocity v where $v_1 < v < v_2$ is computed as $C(\lambda\zeta_1 + (1-\lambda)\zeta_2, v)$ where $\lambda = \frac{v-v_1}{v_2-v_1}$. It should be noted that such methods, usually, cannot provide theoretical guarantees of stability. However, they have proven to be popular because of reduced design complexity.

Test Tracks

PATH primarily uses three test tracks for performing experiments related to IVHS development. Each of these tracks consists of magnets installed on the road surface (with an inter-magnet spacing of about 1.2m). This series of magnets acts as the reference that vehicles track. A description of these test tracks follows.

1. Richmond Field Station, CA: This is a low-speed test track used for testing control algorithms on passenger cars. On this track, longitudinal speeds are restricted to about 30mph. The track consists of short straight sections interspersed with sharp curves. Figure 16 shows a "bird's-eye" view of the track.

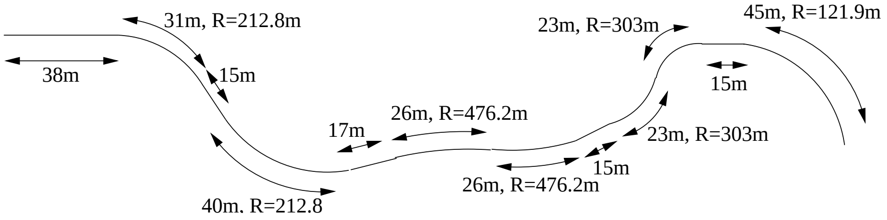


Figure 16: Richmond Field Station test track

2. Crows Landing, CA: This is a high-speed test track used for most of the development related to control of heavy vehicles and also for high speed testing of control algorithms designed for passenger cars. The track consists of straight and curved sections constituting a total length of about 2km (Figure 17). It is useful to note that the sharpest curves on highways in the US have a radius of curvature of about 1000m.

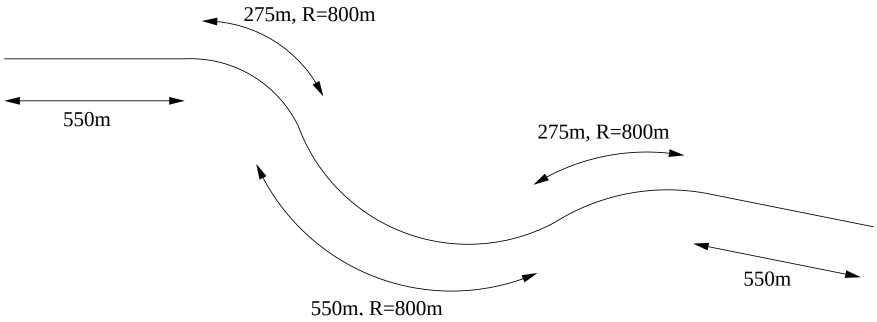


Figure 17: Crows Landing test track

3. I-15 Lanes, San Diego, CA: This track has been laid out on the "Fast-Track"

lanes on Interstate 15 (between Los Angeles and San Diego). The track is used primarily for automated highway demonstration purposes.

Low and high speed experiments documented in this chapter were performed at the Richmond Field Station and Crows Landing, respectively.

8.2 Discussion of Results

This subsection presents discussions on the results of the experiments. The primary variables of interest which are used to qualify performance of the lane-keeping control system are: (a) lateral errors at the location of the front and rear magnetometers (b) steering angle at the steering-wheel and (c) yaw rate. As mentioned earlier, a "good" controller is one that ensures that these variables are maintained small. For passenger cars, the following ranges of values are considered "small".

- -0.3m < lateral error < 0.3m
- -30 deg < steering angle at hand-wheel < 30 deg
- -8 deg/s < yaw rate < 8 deg/s

Fault Tolerant Control: Controller designed using simultaneous stability theory

The design of a fault tolerant lane-keeping controller based on results from simultaneous stability theory was discussed in Section 5. Recall that this controller was chosen to make the closed-loop system insensitive to failure#2 in either one of the two magnetometer banks. Figures 18 and 19 are sample high-speed experimental results for the cases where failure#2 is induced in the rear and front magnetometer banks respectively. From these results, we note the following.

1. Even though the occurrence of the failure leads to an increase in the values of the variables of interest, safe high-speed lane-keeping control action can be achieved for the occurrence of failure#2 in either one of the two magnetometers.

2. In the case of failure of the front magnetometer bank (Figure 19), oscillations become significantly larger after the failure. However, as long as longitudinal speeds are maintained high stability problems do not seem to arise.

Remarks:

1. The inclusion of a sample low-speed experimental result for the case of occurrence of failure#2 in the rear magnetometer bank has been omitted because the control performance does not exhibit characteristics which are not captured in the high-speed experiment.

2. For the case of occurrence of failure#2 in the **front** magnetometer bank it has been observed that under low-speed operation, stability problems arise (the vehicle goes out of the range of measurement of the magnetometers fairly rapidly). Up to now, we have not been able to demonstrate a **low-speed** experiment in which the vehicle (controller designed using simultaneous stability theory) remained stable in the event of failure#2 in the front magnetomter bank.

Fault Tolerant Control: The Observer Based Look-Ahead Scheme

The observer based look-ahead scheme was discussed in Section 6. In this scheme, two observers (one dedicated to each of the two lateral error outputs) are used to generate independent estimates $(y_{vs})_f$ and $(y_{vs})_r$ of the lateral error at the location of a virtual sensor. These estimates are then assigned weights, based on the level of confidence in a particular output, to generate a consolidated estimate y_{vs} of the lateral error at the location of the virtual sensor. In other words, y_{vs} is constructed as: $y_{vs} = \lambda(y_{vs})_f + (1 - \lambda)(y_{vs})_r, \lambda \in [0, 1]$. During no-fault operation, λ is chosen to be 0.5. The controlled output y_{vs} is fed to a "controller" which generates the desired steering angle.

Figures 20 and 22 show results of sample high-speed experiments where the controller used was designed based on the observer based look-ahead idea and failures#1

& #2 are, respectively, introduced in the rear magnetometer bank output. The variable y_v in the figures represents the consolidated estimate y_{vs} introduced above. In both experiments, real-time knowledge of the failure is assumed. The knowledge of the failure is then used to change the weights suitably so that the spurious estimate is discarded.

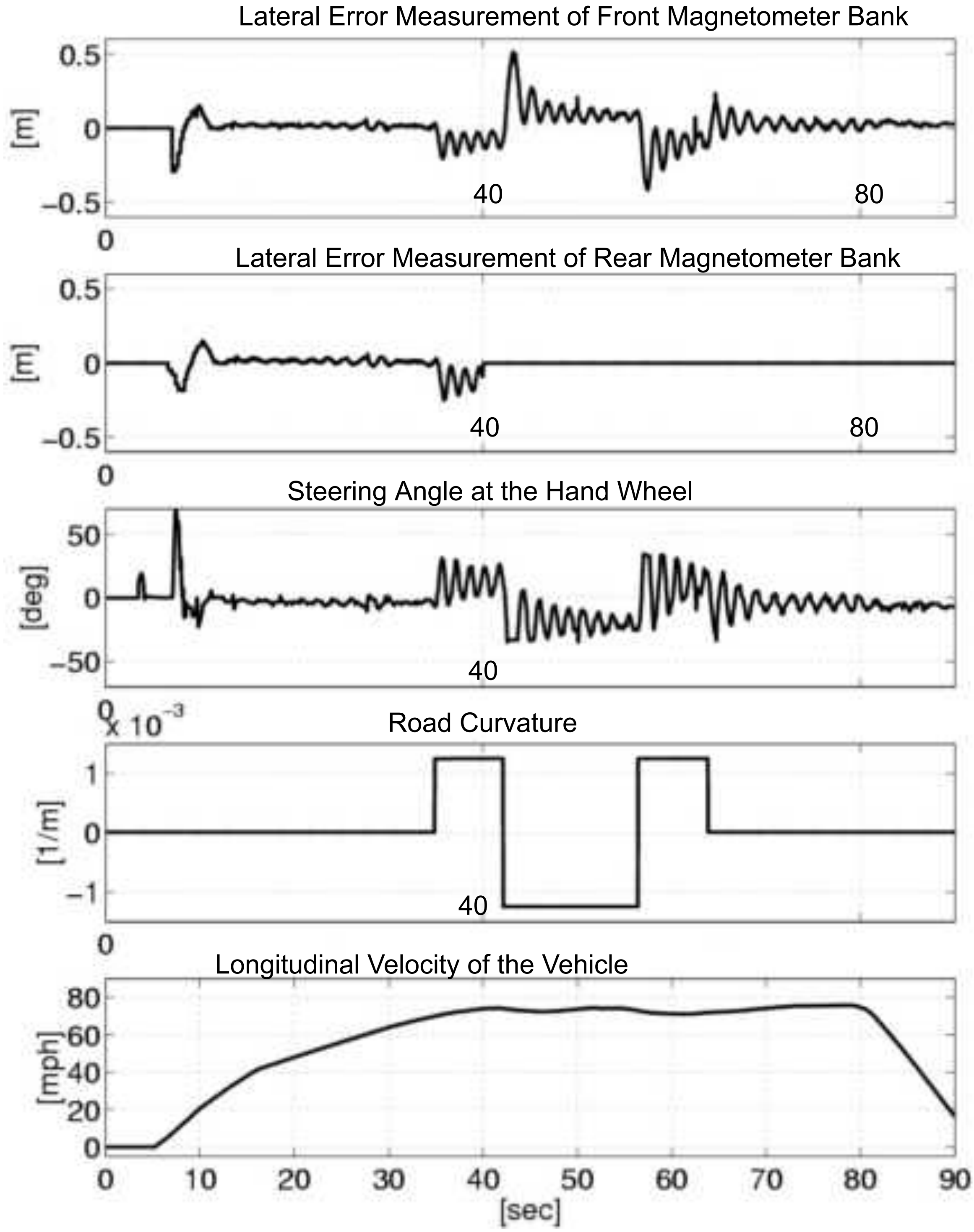
The following observations can be made:

1. The occurrence of failures leads to increased lateral errors, yaw rates and steering angles. However, the degradation in performance is within tolerable limits.

2. Even during the transition phase when λ changes from 0 to 1, the estimate of the lateral error at the location of the virtual sensor using the observer based scheme, though incorrect, is not altogether faulty. This property ensures that stability is maintained during the transition.

8.3 Summary

In this section, we discussed experimental results demonstrating fault tolerant lane-keeping control action in test vehicles used by PATH. Specifically, experiments pertaining to control with a simultaneously stabilizing controller and the *observer based look-ahead* scheme have been documented. The results demonstrate that reliable lane-keeping control can be achieved in the event of a failure of the rear magnetometer bank. However, failure of the front magnetometer bank can result in pathological situations.


Lateral Error Measurement of Front Magnetometer Bank

Lateral Error Measurement of Rear Magnetometer Bank

Steering Angle at the Hand Wheel

Road Curvature

Longitudinal Velocity of the Vehicle

Figure 18: High speed test: Simultaneous stability based design. Failure #2 in rear magnetometer bank around 40 sec

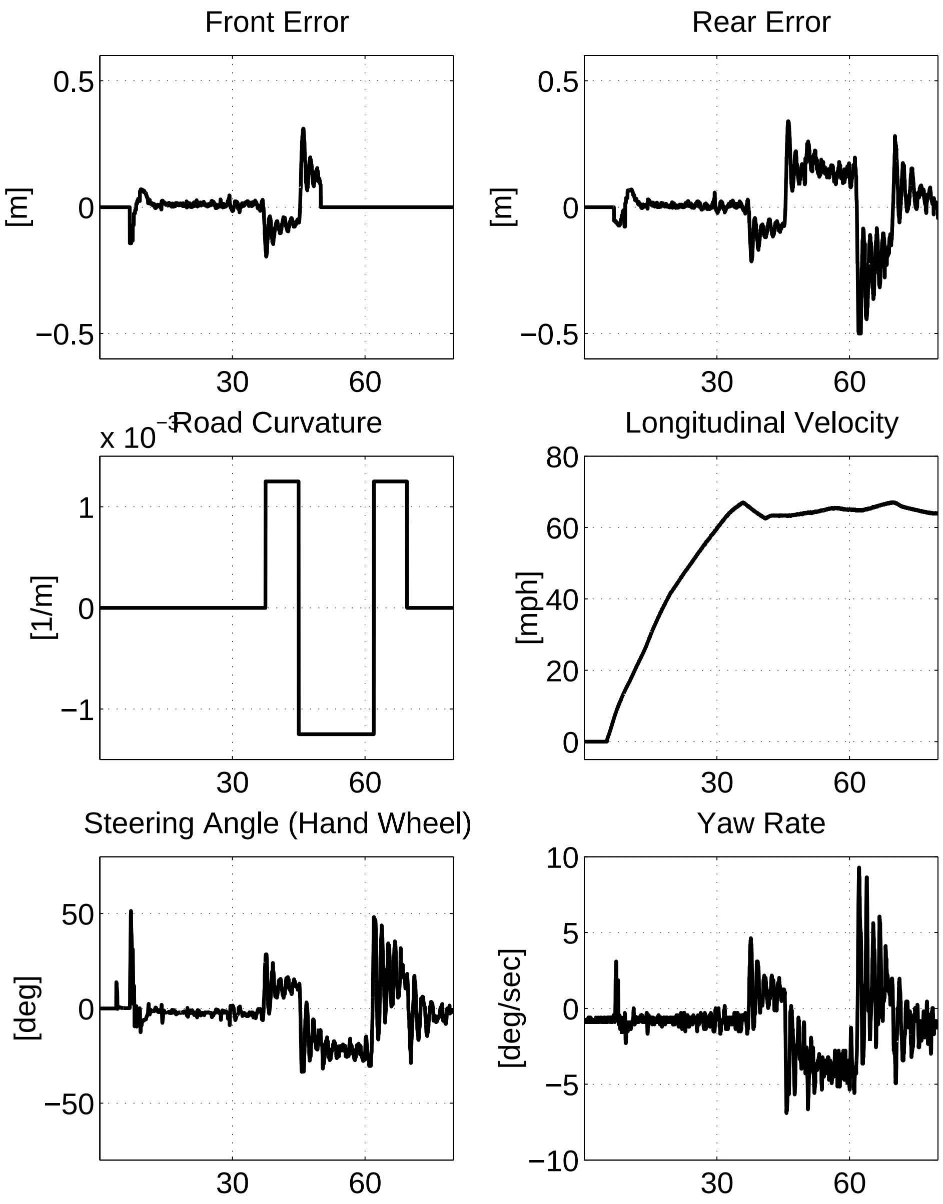


Figure 19: High speed test: Simultaneous stability based design. Failure #2 in the front magnetometer bank around 50 sec

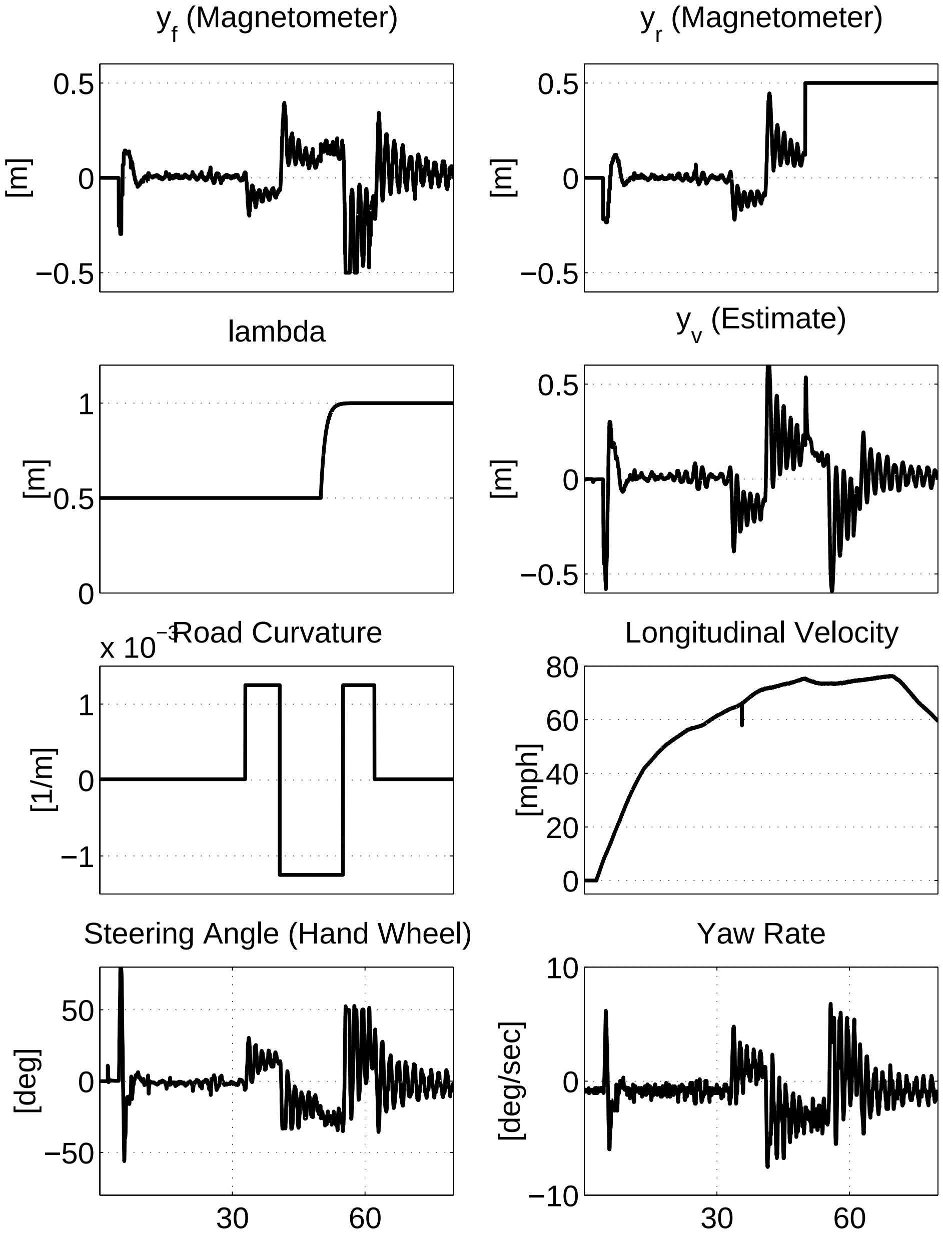


Figure 20: High speed test: Observer based look-ahead scheme. Failure #1 in rear magnetometer bank around 50 sec

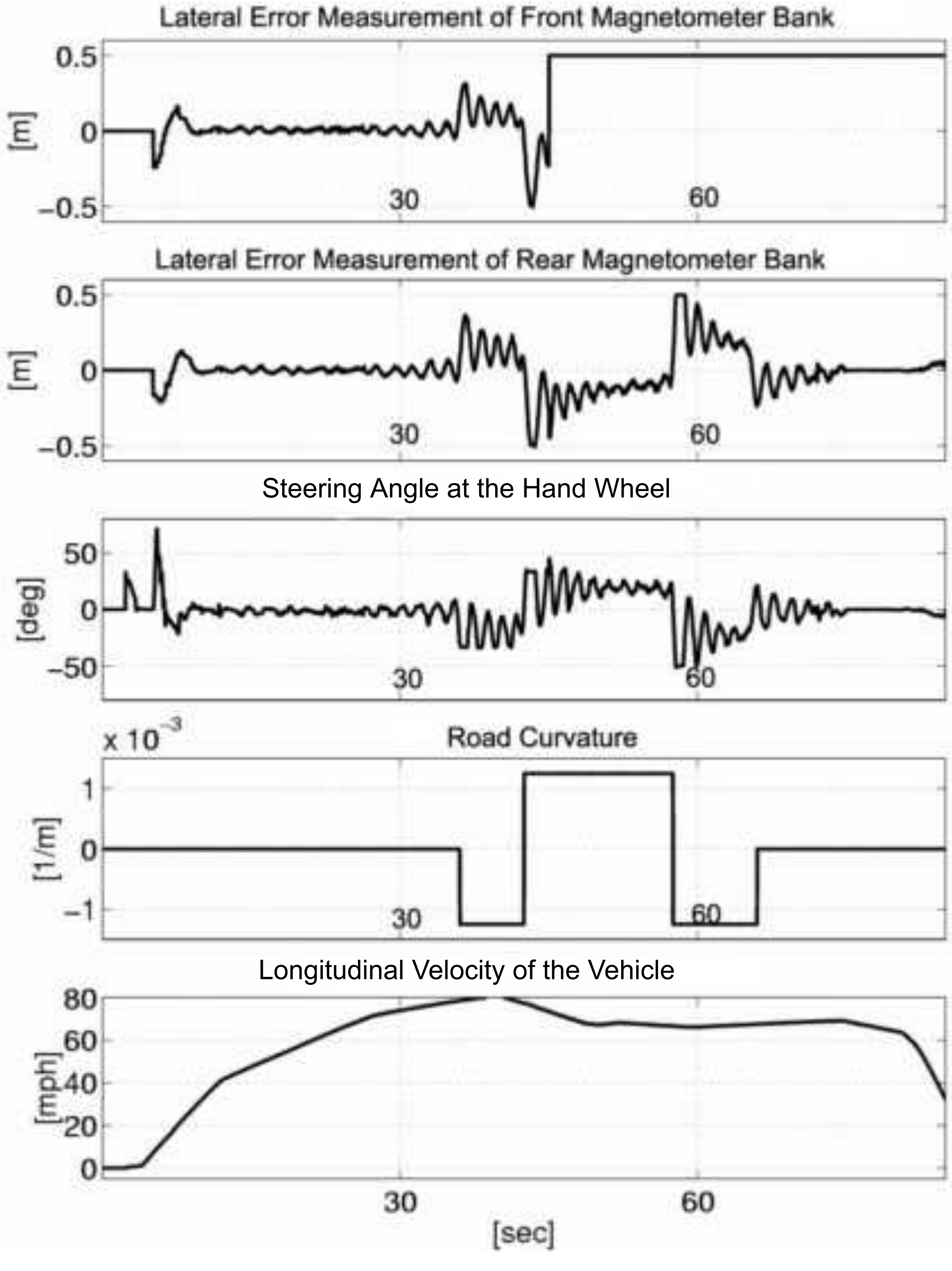


Figure 21: High speed test: Observer based look-ahead scheme. Failure #1 in front magnetometer bank around 45 sec

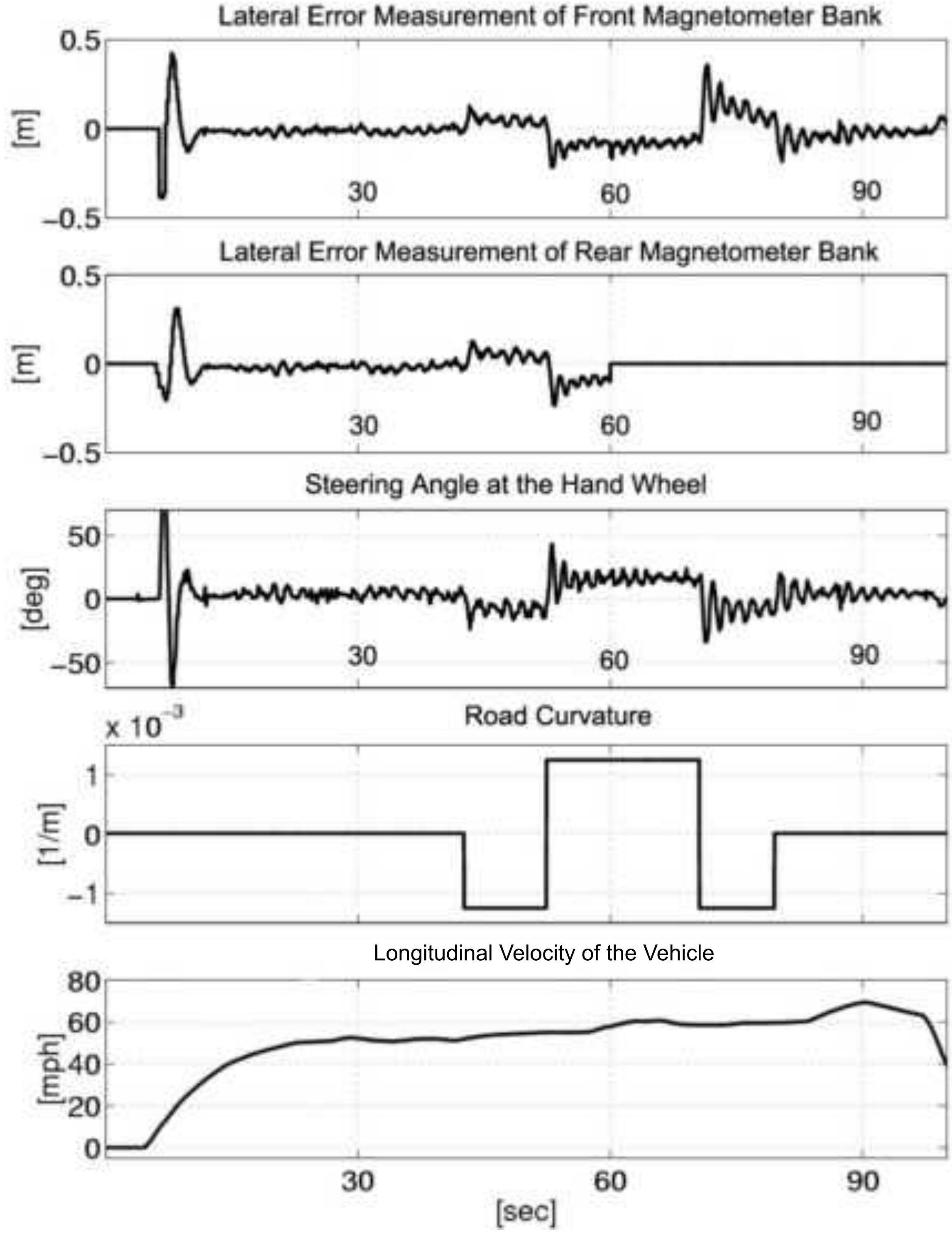


Figure 22: High speed test: Observer based look-ahead scheme. Failure #2 in rear magnetometer bank around 60sec

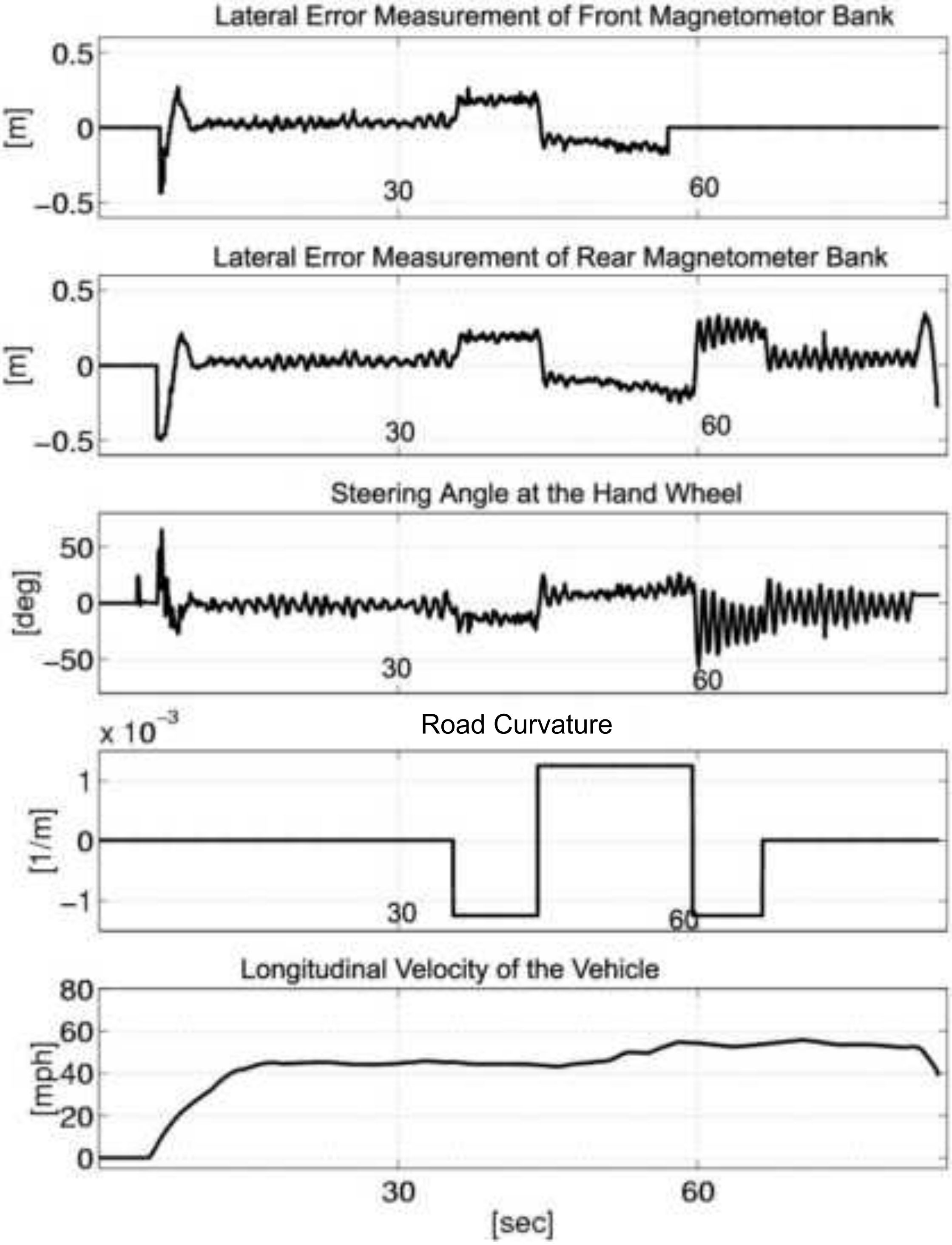


Figure 23: High speed test: Observer based look-ahead scheme. Failure #2 in front magnetometer bank around 57 sec

9 Conclusion

The focus of this report was the development of methodologies for the design of control systems that accommodate hard failures. To achieve this end, we focused on the development of robust controllers that were insensitive to hard failures. More specifically, the report focused on developing control strategies that preserved stability of the control system, for certain failed states of operation. This feature of control action implies that such control schemes are inherently conservative. In other words, stability is guaranteed (in the event of a failure) at the expense of performance in both non-faulty and faulty states.

The primary motivation for considering the problem mentioned above arose from a specific application , namely, the Intelligent Vehicle-Highway System (IVHS) under the Partners for Advanced Transit on Highway (PATH). Specifically, this report focused on the lane-keeping control system deployed on passenger cars used in the PATH IVHS. The primary components of the lane-keeping control system include a steering motor and two sensors (called magnetometers) that measure the lateral deviation from a series of magnets (representing the lane center-line). A lane-keeping control algorithm is used to process the outputs of the two magnetometers to generate a desired steering action (which is communicated to the steering motor). On the passenger cars, the magnetometers are mounted under the front and rear bumpers of the vehicle. Our efforts were geared towards design of lane-keeping controllers that were robust to certain, potentially catastrophic, failures in the magnetometers. These failure are described in Section 2.2.

We argued that the problem of design of failure insensitive controllers may be cast as a simultaneous stabilization problem. This argument directed the focus of Section 5 on the development of methodologies for the design of simultaneously stabilizing controllers (LTI case). More specifically, the section considered two problems. The first problem considered the design of a simultaneously stabilizing controller for two plants. It was shown that if a certain ”small-gain” condition is satisfied then this problem may be cast as an *output estimation problem* [2]. It was noted that the primary advantage of this scheme over the classical interpolation based scheme discussed in [9] [11] is that it guarantees that the order of the simultaneously stabilizing controller is kept small. The second problem dealt with the design of a simultaneously stabilizing controller that stabilized a finite number of plants while guaranteeing a chosen level of performance. The notion of performance used here was the ”size” of a certain weighted sensitivity function. Again, a ”small-gain” condition was used to cast this problem as a standard H_∞ control problem. It is useful to note that both techniques were based on **sufficient** conditions for simultaneous stability. Consequently, their application is limited only to certain select situations. Also, it was noted that sufficient conditions based on ”small-gain” conditions are overly conservative. Future work on the development of sufficient conditions for simultaneous stability with reduced levels of conservativeness may thus be justified.

The focus of Section 6 was the development of a control scheme which exploited redundancy in multi-sensor systems (described as LTI systems) to accommodate a hard failure situation where the output of one of the sensors goes to a constant value. To achieve this end, a *Dedicated Observer Based System* was proposed. In this system Luenberger observers are used, one for each sensor output, to generate redundant estimates of the states of the system. It was argued, heuristically, that if the observer gain are maintained small, one can achieve fault tolerant control action. On a philosophical note, this result can be interpreted as a re-affirming the tenet that small observer gains imply low confidence in the sensor outputs. Since small observer gains are used, we argued that the success of the application of this scheme to real-world situations depended critically on the quality of the mathematical model used to describe the system.

Lane-keeping controllers were designed based on results from the aforementioned work on design of simultaneously stabilizing controllers as well as the dedicated observer based architecture. The simultaneous stability based design scheme assumed the ”geometric” look-ahead [3] [4] structure. It was shown that the requirement for simultaneous stability imposed restrictions on the look-ahead distance. For the lane-keeping control problem, this limitation was interpreted as representing a trade-off between fault tolerant action versus non-faulty performance. The lane-keeping control design algorithm utilizing dedicated observers was called the *Observer Based Look-Ahead Scheme* since this algorithm uses observers to construct an estimate of the lateral error at the location of a virtual sensor in a manner similar to the ”geometric” look-ahead scheme. This scheme guarantees failure tolerance action even when large look-ahead distances are used. The primary concerns related to efficacy of this scheme were implementation related. These controllers were tested experimentally to determine the efficacy of the design methodologies. Results of these experiments (documented in Section 8) indicate that safe failure tolerant control action can indeed be achieved.

In Section 7, we explore further the idea of the observer-based fault tolerant control systems. In stead of using two independent observers, a more delicate structure including two coupled observers and fusing blocks was proposed. An on-line adapting law was applied to combining the estimates from both observers. This particular structure granted the fault tolerant control system under consideration the ability to *detect* and *identify* the faulty sensor. The faulty sensor output were then replaced by the signal synthesized from the healthy sensor output. The proposed methodology possesses the advantage over the simultaneously stabilizing controller that the performance is less conservative and can accommodate a variety of failures which may not be foreseen in the controller design phase. However, it suffers the same problem as the Dedicated Observers that the performance relies critically on the accuracy of the model and the stability is not guaranteed during the transition between normal and degraded mode operations.

The simultaneously stabilizing controllers and the observer-based scheme have their own merits and demerits. It is unclear as to how these schemes can be integrated synergistically in the process of design of real-time control systems. One plausible framework for integration could be a structure where domains in which these scheme work are separated. For example, simultaneously stabilizing controllers can be used to exploit redundancy to provide system stability in the event of failures. This stability guarantee could provide the cushion for employing reliable failure detection and identification (FDI) methodologies. These reliable FDI techniques can then be used to spawn appropriate reconfiguration in control action. A formalization of this preliminary notion may provide a good starting point for future work.

References

[1] F. Callier and C. Desoer, *Linear System Theory*, Springer-Verlag, 1991

[2] J. C. Doyle, K. Glover, P. P. Khargonekar, and B. A. Francis, *State-space solutions to standard H_2 and H_∞ control problems*, IEEE Transactions on Automatic Control, Vol. 45, No. 8, 1989, pp831-847.

[3] J. Guldner, H-S Tan, and S. Patwardhan, *Analysis of automatic steering control for vehicles with look-down lateral reference systems*, Vehicle Systems Technology, Vol 26, No. 4, 1996, pp243-269

[4] J. Guldner, H-S Tan, and S. Patwardhan, *Study of design directions for vehicle lateral control*, Proc. of the Conference on Decision and Control, 1996, p1732-1737

[5] P. Hingwe, A. Packard, and M. Tomizuka, *Linear parameter varying controller for automated lane guidance: Experimental study on tractor semi-trailer*, Proc. of the American Control Conference, 2000.

[6] T. Hsiao and M. Tomizuka, *Observer-based Sensor Fault Detection and Identification with Application to Vehicle Lateral Control*, Proc. of the American Control Conference, 2004

[7] S. Patwardhan, H-S. Tan, and J. Guldner, *A general framework for automatic steering control: System analysis.* Proc. of the American Control Conference, 1997, p1598-1602

[8] S. Suryanarayanan, *Fault Tolerant Control and its Application to Lane-keeping Control of Automated Vehicles*,Ph. D. thesis, 2002.

[9] M. Vidyasagar. *Control System Synthesis: A Factorization Approach.* MIT Press. Boston, 1985

[10] M. Vidyasagar and N. Viswanadham, *Algebraic design techniques for reliable stabilization.* IEEE Transactions on Automatic Control, Vol. 27,1982, pp1085-1095

[11] D. C. Youla, B. Bongiorno, and C. Lu, *Single loop feedback stabilization of multivariable plants*, Automatica, Vol 21, 1976, pp133-148