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

Issues in Fault Tolerant Control of Vehicle Follower Systems

J.K. Hedrick
V. Garg

California PATH Research Paper

UCB-ITS-PRR-94-11

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.

April 1994

ISSN 1055-1425

Issues in Fault Tolerant Control of Vehicle Follower Systems

J.K. Hedrick, P.I.
V. Garg

Department of Mechanical Engineering
University of California, Berkeley
April 1994

Contents

1 Introduction **3**

2 Review of Fault Tolerant Control Techniques **4**
2.1 Design Considerations 4
2.2 General structure of model-based methods 5
2.3 Residual Generation 5
2.4 Alternative Approaches to Failure Detection 6
2.4.1 Failure sensitive filters 6
2.4.2 Voting Systems 8
2.4.3 Multiple Hypothesis Filter Detectors 8
2.5 Robustness Issues in Failure Detection 9
2.6 Some FDI Applications in the literature 9
2.7 Fault Tolerant Control 10
2.8 Conclusion 11

3 Potential fault modes & reconstruction schemes in vehicle follower systems **12**
3.1 4-Vehicle Simulations 12
3.1.1 Simplified Vehicle Model 13
3.1.2 Simulations 15
3.2 Considerations in Fault Analysis 17

4 Fault Detection **24**
4.1 Detection Filters for nonlinear systems 25

5 Conclusions and Future Work : **26**

List of Figures

3.1 Lead Vehicle Maneuvre 18
3.2 Fault in Spacing Measurement in Vehicle #1 19
3.3 Radar fault mode in Vehicle #1 20
3.4 Engine Speed sensor fault mode in Vehicle #1 21
3.5 Accelerometer Fault Mode 22
3.6 Reconstruction of sensor measurements 23

Chapter 1

Introduction

Physical systems are often subjected to unexpected changes, such as component failures and variations in operating conditions, that tend to degrade overall system performance. In order to maintain a high level of performance, it is important that failures be promptly detected and identified so that appropriate remedies can be applied. The aim of this report is to *study issues concerning fault detection and identification in vehicle follower control.*

Since the reliability of the overall system will be a product of the reliabilities of its **individual components, it is imperative that every individual car along with its control system should have a high level of reliability. Faults in a single car could have severe effects on the overall flow on the highways.** With the decrease in human factors involved, high dependability of car controllers, sensors,roadside computers, inter-car communication links etc. become crucial factors.

Over the past two decades numerous approaches to the problem of failure detection and identification (FDI) in dynamical systems have been studied and some of these techniques are delineated in **Chapter 2**.

Chapter 3 discusses various potential fault modes among sensors, and actuators used in the vehicle following experiments in cars. The emphasis is on the need to investigate all possible modes of sensor, actuator and process faults and thereafter reconstruct the information lost. This would help in decentralizing the control tasks involved. Simulations of various fault modes without and without lost information reconstruction were done to show effectiveness of simple reconstruction techniques.

Chapter 4 deals with issues of *fault detection* of sensors and actuators for vehicle following applications. Fault detection methodologies center around book-keeping. A new method of fault detection in nonlinear systems is being investigated.

A summary of results and proposed future work is presented in **Chapter 5**.

Chapter 2

Review of Fault Tolerant Control Techniques

Numerous approaches to the problem of failure detection and identification (FDI) in dynamical systems have been developed in the last two decades as surveyed in papers by Willsky [2], and Gertler [4] and the next few sections will discuss some of the frequently applied methods. Another good reference on FDI theory and applications is [6].

Fault analysis consists of three substages :

- Fault Detection: To detect that a fault has occured and that system performance is deteriorating.
- Fault Identification : To implement some form of voting scheme to identify which component has had a fault.
- Fault Reconfiguration : To reconstruct the information lost due to the fault and thereby, continue with the normal control schedule.

2.1 Design Considerations

The design of failure detection systems involves the considerations of several issues. One is usually interested in designing a system that will respond rapidly when a failure occurs; however, in high performance systems one often cannot tolerate significant degradation in performance during normal system operation. These two considerations are usually in conflict. That is, a system that is designed to respond quickly to abrupt changes must necessarily be sensitive to high frequency effects, and this in turn will tend to increase the sensitivity of the system to noise, via the occurence of false alarms signaled by the failure detection system. In general, one would like to design a failure detection system that takes system redundancy into account. In a system containing several backup subsystems we may be able to devise a simple detection algorithm that is easily implemented but yields only moderate false alarm rates. On the other hand, by implementing a more complex failure detection algorithm that takes careful account of system dynamics, one may be able to reduce requirements for costly hardware redundancy. Analytical redundancy based FDI (failure detection and isolation) uses a model of the dynamic system to generate the redundancy required for failure detection. In many systems, all of the states cannot be measured because of cost, weight and size considerations, therefore, FDI schemes for such systems must extract the redundant information from dissimilar sensors, using the differential equations that relate their outputs. In addition to taking hardware issues into consideration the designer should consider the issue of computational complexity.

2.2 General structure of model-based methods

Most model-based FDI methods rely on analytical redundancy. In contrast to physical redundancy,when measurements from different sensors are compared, now sensory measurements are compared to analytically obtained values of the respective variable and the resulting differences are called residuals. The deviation of residuals from the ideal value of zero is the combined result of noise, modeling errors and faults. A logical pattern is generated showing which residuals can be considered normal and which ones indicate a fault. Such a pattern is called the signature of the failure. The final step of the procedure is the analysis of the logical patterns obtained from the residuals, with the aim of isolating the failures that cause them. Such analysis may be performed by comparison to a set of patterns known to belong to sample failures or by the use of some more complex logical procedure.

2.3 Residual Generation

The residual generation techniques in the literature can be categorized in two broad groups. Open loop schemes form one group (see Chow and Willsky [8]). These schemes involve the construction of a set of parity equations which represent all of the analytical redundancies of a system. These parity relations are simply all of the input-output relationships of a given linear system. A generalized parity space (see Chow and Willsky [8]) can be formed from the parity equations, and in the presence of a failure the resulting parity errors combine to provide a failure signature with directional characteristics in addition to the usual residual magnitude information. Theoretically, these directional signatures should facilitate the failure detection and identification process. However, the open loop characteristics are of a highly temporal nature and, therefore, the directional signature is not generally

constrained.
The second category of residual formation techniques is that of closed loop schemes. Although any linear filter residual could be processed, one particular type of filter produces residuals with directional characteristics that can readily be associated with a known failure mode. These filters are known as detection filters, but are actually a particular class of observers. Unlike the directional failure signatures of the open loop parity space method, detection filters act in a closed loop fashion to fix the output direction associated with plant and actuator failures while restricting sensor failure output directions to lie in a plane.
If state variables are directly measureable or if they are computable from output measurements then the residuals can be expressed directly in terms of the state variables. The nominal state can be computed by Kalman filtering or by an observer. We consider the discrete time state space model as follows :

$$x(t+1) = Ax(t) + Bu(t); y = Cx(t);$$

If, as is usually the case , direct comparison of the state is not possible, then the residual can be defined as the difference between the measured output $\tilde{y}(t)$ and the estimate obtained by Kalman filtering, and is called the innovation :

$$e(t) = \tilde{y}(t) - C\hat{x}(t|t-1)$$

Here $\hat{x}(t|t-1)$ is the Kalman estimate of the state. If the model is perfectly accurate and the noise is white with zero mean, then the innovation sequence of a fault-free system is also white with zero mean. This property can be utilized to construct a number of statistical tests for failure detection (see Gertler[4]).

2.4 Alternative Approaches to Failure Detection

In this section we discuss several failure detection methods and comment on their characteristics.

2.4.1 Failure sensitive filters

This class of filters is aimed at overcoming the problem of an 'oblivious filter'. Optimal filters as defined in Beard [3] perform well if there are no modeling errors. It is possible for the filter estimate to diverge if there are substantial unmodeled phenomena. This problem occurs because the filter relies on old measurements and becomes oblivious to new measurements. Thus if an abrupt change occurs the system will respond sluggishly. As noted earlier as we increase sensitivity to new data, by effectively increasing the bandwidth of the Kalman filter, our system becomes more sensitive to sensor noise and the performance of the filter under no-failure conditions degrades. One might consider a two-filter system : with an optimal filter as a normal mode primary filter, with the failure sensitive filter as an auxiliary monitor, used to detect abrupt changes. One method to design failure sensitive filters for specific failures is to include several failure states in the dynamic model. If the estimates of these variables vary markedly from their nominal values, a failure is declared.

An alternative to the addition of failure states to the dynamic model is the class of detector filters developed by Beard [3] and Jones [14]. They considered a linear time-invariant, continuous-time, deterministic system model

$$\dot{x}(t) = Ax(t) + Bu(t); z(t) = Cx(t); \tag{2.1}$$

and designed a filter of the form

$$\dot{\hat{x}}(t) = A\hat{x}(t) + D(z(t) - C\hat{x}(t)) + Bu(t); \tag{2.2}$$

The primary criterion in the choice of the gain matrix D is not that in Eq. 2.2 it provides a good estimate of x, as it is with observers or optimal estimators, but rather that the effects of certain failures are accentuated in the filter residual

$$\gamma(t) = z(t) - C\hat{x}(t) \tag{2.3}$$

The basic idea is to choose D so that particular failure modes manifest themselves as residuals which remain in a fixed direction or in a fixed plane.

To illustrate the Beard-Jones approach, we consider the following simple example. Suppose we wish to detect a failure of the ith actuator, i.e. in the actuator driven by the ith component of the input u. If we assume the failure takes the form of a constant bias, our state equation becomes

$$\dot{x}(t) = Ax(t) + B(u(t) + ve_i) = Ax(t) + Bu(t) + vB_i, t \geq t_0 \tag{2.4}$$

where e_i is the ith standard basis vector, b_i is the ith column of B, and t_0 is the unknown time of failure. Suppose we consider the case of full state measurement-i.e. let $C = I$. In this case we obtain a differential equation for the residual

$$\dot{\gamma}(t) = (A - D)\gamma(t) + vb_i; \tag{2.5}$$

If we choose $D = \sigma I + A$, we obtain

$$\dot{\gamma}(t) = -\sigma y(t) + vb_i; \tag{2.6}$$

$$\gamma(t) = e^{-\sigma(t-t_0)}\gamma(t_0) + v(1 - e^{-\sigma t})b_i/\sigma; \tag{2.7}$$

Thus as the effect of the initial condition dies out,$\gamma(t)$ maintains a fixed direction (b_i) with magnitude proportional to failure size (v). Note that as we increase σ, thus increasing filter gain, the initial condition dies out faster, but the magnitude of the steady-state value of γ decreases. Thus, if there is any noise in the system, we cannot make γ arbitrarily large. White and Speyer [1] reformulated the detection filter theory as an eigensystem assignment problem. Their approach produced a straightforward derivation which yields a system of simultaneous linear equations to be solved for the detection filter gains and the closed loop eigenvectors, once the closed loop eigenvalues have been assigned. The only major restrictions on the system other than its linear time invariance are observability and output separability. The latter condition means that the output directions of different failure modes are distinct.

In summary, this design methodology is extremely useful conceptually, can be used to detect a wide variety of failures, and provides detailed failure isolation information. The major limitation of this approach is its applicability only to linear time invariant systems. Results in detection filter theory have perhaps led to the most thorough study of the basic concepts underlying failure detection.

2.4.2 Voting Systems

Voting systems are often useful in systems that possess a high degree of parallel hardware redundancy. In standard voting schemes, one has at least three identical instruments. Simple logic is then developed to detect failures and eliminate faulty instruments, for example, if one of the three redundant signals differs markedly from the other two, the differing signal is eliminated.

2.4.3 Multiple Hypothesis Filter Detectors

A rather large class of adaptive estimation and failure detection schemes involves the use of a 'bank' of linear filters based on different hypotheses concerning the underlying system behavior. In this scheme several different sets of system matrices are hypothesized and filters for each of the models are constructed, and the innovations from the various filters are used to compute the conditional probability that each system model is the correct one. In this manner, one can do a simultaneous sysytem identification and state estimation. In addition, an abrupt change in the probabilities can be used to detect changes in true system behavior. Montgomery and Caglayan [16] have used such a technique for digital flight control systems and have studied its robustness in the presence of nonlinearities via simulations.

2.5 Robustness Issues in Failure Detection

A major issue of concern in failure detection is robustness of the dynamic system i.e. minimizing the sensitivity of detection performance to model errors and uncertainties. An ideal simplistic approach to designing a robust FDI system is to include all uncertainties in the overall problem specification; then a robust design is obtained by optimizing the performance of the entire system with the uncertainties present. However, this generally leads to a complex mathematical problem. On the other hand, a simple approach is to ignore all model uncertainties in the performance optimization process and evaluate the resulting design in presence of model errors and accept the design if performance is tolerable. Chow and Willsky [8] developed a systematic approach to consider uncertainties directly. The basic idea is to identify the analytical redundancy relations of the system that are known well and those that contain substantial uncertainties. As model error directly affects residual generation, robustness can be achieved by designing a robust residual generation process. Residual generation is based on parity relations involving the particular component failing. Considerable work towards solving the problem of modeling errors has been done by Horak, [9], [10]. Given the input variables and uncertainty range of the parameters of the state space model, the reachable intervals of the output variables are explicitly computed. The technique is based on Pontryagin's optimum principle. The concept of reachable intervals is easily extended to plant and measurement noise. Once, the reachable intervals have been obtained, they serve as dynamic thresholds for the momentary measurements.
Robustness considerations in design of failure detection still remains an open problem and is currently a topic of extensive research.

2.6 Some FDI Applications in the literature

FDI has been applied to variety of engineering problems in the literature in the past two decades. Cho and Paolella [11], [12] are developing an FDI system for an automotive power train to detect faults in engine speed , torque converter turbine speed and wheel speed. They have used an experimentally validated nonlinear model for the automotive powertrain and and used a robust observer scheme to maximize robustness to parametric variations and unmodeled dynamics. Horak and Allison [9] have discussed the application of an FDI system to a hypothetical turbofan engine. Considerable emphasis is being given to the application of FDI in automotive systems. Rizzoni and Ribbens [15] are studying the application of detection filters to four wheel steering systems. Patwardhan and Tomizuka[5] are applying detection filter theory to lateral control of automobiles. Use of FDI theory is being proposed to detect failed sensors and actuators in automated highway systems and ensure safe vehicle follower operation until the affected vehicle has been separated from the platoon.

2.7 Fault Tolerant Control

Fault tolerant control is the means for determining the corrective action necessary when a fault has been detected and isolated in the system. Fault tolerant control structures generally operate by establishing a 'dual' control algorithm that can switch between modes when a failure has been detected. One can formulate a performance mode when the system is operating without failures and an 'emergency' mode when a serious failure has been detected. Fault tolerant control should be differentiated from robust control in that the latter aims to make the system insensitive to parametric variations caused by component failures whereas fault tolerant control has a two-fold purpose : identification of component failures and regulation of process outputs. The early detection of system anomalies allows the controller to take the appropriate action to avoid further complications. This requires that the potential component failures be taken into account in the design of the control system.

De Benito and Eckert [7] have developed a fault tolerant algorithm for on-board vehicle control systems. They considered a discrete time stochastic system described by a finite set of linear models in which the anticipated failure modes have been taken care of. They considered two fault tolerant algorithms : certainty-equivalence and dual control approximations to optimal control laws.

The optimal control law for the stochastic system should consider the parametric uncertainty as well as the randomness imposed by the plant and measurement disturbances. However, it is possible to ignore the dependence of the controller on the parametric uncertainty and derive a closed loop control law for the corresponding problem. The key to the derivation is replacing all of the random variables on which the states depend by their expected values. This 'passive' control strategy is called *certainty equivalence* approach. A conditional control law can be computed for each of the hypothesized modes of operation. The *CE* control law is computed as a weighted average of the conditional control laws.

The *dual control* algorithm uses the input to probe the system in an attempt to reduce the parametric uncertainty which conflicts with the regulatory nature of the control input and hence its name.

Scientists at NASA Lewis Research Center have developed an algorithm (ADIA algorithm) see [13] to improve overall demonstrated reliabilty of digital electronic control systems for turbine engines by detecting, isolating and accommodating sensor failures using analytical redundancy. In the normal mode of operation, the accommodation filter uses the full set of optimal estimates of the measurements. These estimates are used by the control law. When a sensor failure occurs, the detection logic determines that a failure has occurred, the isolation logic determines which sensor is faulty and the estimator removes the faulty measurement from further consideration. The estimator however continues to generate the full set of optimal estimates for the control. Thus, the control mode does not have to restructure for any sensor failure.

2.8 Conclusion

A literature review of work done so far in the field of fault detection and tolerance has been presented. Detection filter theory promises to be suitable for application to vehicle control problems in view of its simplicity, rigor and proven applicabilty. Literature available in fault tolerance is limited and this field seems to have immense reseach potential.

Chapter 3

Potential fault modes & reconstruction schemes in vehicle follower systems

Smooth operation of an automated vehicle control system is contingent on accurate and reliable sensor measurements and actuator performance. Therefore, an indepth study of all sensors, actuators and all communication accessories is in order.

A list of the sensors and actuators being used in the longitudinal control of the experimental vehicle is presented in Table 3.1. The information lost due to the faults in each sensor is also indicated and simple reconstruction schemes, wherever possible, are suggested. By simple reconstruction schemes we mean performing linear operations like addition and differentiation on outputs of functionally related sensors and reconstructing the information lost. For example, to reconstruct the lead car velocity and acceleration information lost in event of a radio failure, we can subtract the instantaneous closing rate obtained from the radar from the vehicle's own velocity obtained from the transmission speed sensor to estimate the lead car velocity . To estimate the lead car acceleration the estimated lead car velocity can be differentiated (subtract the value at previous sampling from current value and divide by sampling interval).

3.1 4-Vehicle Simulations

Simulation of failure scenarios in four vehicle platoons was done using a five state longitudinal model for each of the vehicles. The aim was to study sensitivity of the control

Sensor Fault	*Information lost*	*Alternatives*
Radio	Lead car acceleration, velocity	use radar & own speed sensor
radar	closing rate, spacing	use radio & own speed sensor
accelerometer of lead car	acceleration of lead car	use radar & own accelerometer.
accelerometer of own car	own acceleration	use radar and radio.
Transmission speed sensor	own speed	use radar, radio
throttle angle sensor	throttle angle	redundant sensor required.
mass flow rate sensor	mass air flow rate	use manifold pressure sensor
brake pressure sensor	brake pressure	redundant sensor needed.
maniford temperature sensor	temperature	use manifold pressure sensor
engine rpm sensor	engine speed	use radar, radio
manifold pressure sensor	pressure	use mass flow rate

Table 3.1: Sensor Fault Reconstruction

algorithm performance to sensor measurement accuracy. Simulations were done with erroneous data fedback to the controller and the performance was evaluated by looking at the resulting spacing error. Simulations were also done to evaluate the effectiveness of using state reconstructions in event of a particular sensor failure. The vehicle following maneuvre considered is shown in Figure 3.1 and the maximum accelerations and braking decelerations were 0.1g. The desired constant intervehicle spacing is 2m. The

3.1.1 Simplified Vehicle Model

The simplified 5-state vehicle powertrain model considered in simulations is described here . (See McMahon et al [17]). The states are :

- Mass of air in the manifold (m_a)
- Engine speed (ω_e)
- Brake torque (T_{br})
- Vehicle speed(v)

The following assumptions are made in deriving the governing equations for the model :

- Ideal gas law holds in the intake manifold.
- Temperature of the intake manifold does not change.
- Time delays in power generation in the engine are negligible.

- Torque converter is locked.
- The drive axle is rigid.

With these assumptions, the flow of air into and out of the intake manifold is governed by the continuity equations given by :

$$\dot{m}_a = \dot{m}_{ai} - \dot{m}_{ao} \tag{3.1}$$

where $\dot{m}_{ai}$ and $\dot{m}_{ao}$ are the mass flow rates through the throttle valve and into the cylinders, respectively.

The empirical relationship relating mass of air intake to the throttle angle is given by :

$$\dot{m}_{ai} = MAXTC(\alpha)PRI(m_a)$$

where MAX is a constant dependent on the size of the throttle body. TC(α) is the throttle characteristic, a nonlinear invertible function of the throttle angle (α). PRI is the pressure influence function which describes the choked flow relationship which often occurs through the throttle valve. Assumptions (1) and (2) help us relate pressure in the manifold and mass of the air in the manifold by a constant.

$$P_m = K_1 m_a$$

where

$$K_1 = R_m T_m / V_m$$

R_m, T_m and V_m are the gas constant for air, temperature of the intake manifold and volume of the intake manifold respectively. The rotational dynamics of the engine is given by :

$$I_e{}'\dot{\omega}_e = T_{net}(\omega_e, P_m) - T_{load} \tag{3.2}$$

where T_{net} is the net engine torque, a nonlinear function of engine speed and pressure in the manifold obtained from the steady state engine maps. I'_e is the effective inertia of the engine. The load torque T_{load} is given by :

$$T_{load} = R(T_{br} + hF_{tr})$$

where R is the effective gear ratio from the wheel to the engine and h is the effective tire radius. The tractive force F_{tr} is modelled by the following relation:

$$F_{tr} = K_r sat(i/0.15)$$

where K_r is the longitudinal tire stiffness and the longitudinal slip i is given by

$$i = 1 - v/(Rh\omega_e)$$

The longitudinal equation for the vehicle is given by :

$$M\dot{v} = F_{tr} - c_a v^2 - F_f \tag{3.3}$$

where c_a is the drag coefficient and F_f is the force due to rolling resistance. M is the effective mass of the vehicle. Finally, the brake torque T_{br} is modelled as a first order lag

$$\tau_b \dot{T}_{br} + T_{br} = T_{bc} \tag{3.4}$$

where T_{bc} is the commanded brake torque and τ_b is the time constant of the brake actuator.

3.1.2 Simulations

Analytical study of effect of faults can be done by feedback linearization and examining the transfer functions relating the error in a particular measurement to the spacing error. The following fault modes were simulated :

- Radar Fault Mode : The simulation of radar failure in Car #1 is shown in Figure 3.2. Accuracy of spacing measurement from the radar is essential for satisfactory performance of the platooning operation. If the spacing measurement is off by 20 percent, spacing errors become significant(0.6m). In this simulation only spacing error fed back was assumed to be faulty, whereas the closing rate measurement was accurate. The effect of a fault in the closing rate measurement is shown in Figure 3.3.

  Loss of Radar → Use comm. Link.

  Reconstruction of radar spacing measurement and closing rate can be done reliably by using previous vehicle information available through the communication link (Figure 3.6b). The issue in consideration then is whether information update occurs often enough. The communication link model considered here has an update rate of 60ms and for the maneuvres we are concerned with, this update rate is sufficient for reconstruction of the spacing error. Closing rate is obtained directly by subtracting the vehicle speed from the previous vehicle's speed. Spacing error is obtained just by integrating the spacing error.

- Engine Speed Sensor Fault : Engine speed sensor fault is simulated in Figure 3.3. The control algorithm is relatively tolerant to errors in engine speed, as 50error results in errors of the order of 0.7m. The engine speed reconstruction can be done using the wheel speed sensor or transmission speed sensor. Figure 3.6b shows effectiveness of replacing engine speed measurement by wheel speed divided by the transmission ratio.

- Accelerometer Fault : Accelerometer measurement of the lead vehicle is transmitted to other vehicles to avoid slinky effect in the platoon but the effect of the acclerometer fault of the lead vehicle is felt most on Vehicle #1 because acceleration of the lead vehicle is required by Vehicle #1 as feedforward information. If the lead vehicle acceleration is off by 50 percent the resulting maximum spacing errors are of the order of 0.7m from Figure 3.5a. Fault in any other vehicle is similar to as shown in Figure 3.5b for Vehicle #1. 50 percent error in that case gives rise to spacing errors of 0.5m.

  Acceleration reconstruction is not an easy task because it involves differentiating other sensor outputs like speed sensors and the noise in the sensors would amplify.

3.2 Considerations in Fault Analysis

- In the simulations it was assumed that there were no multiple sensor faults, therefore, we could exploit the considerable functional redundancy in the system.
- The relevance of the simulations is obviously heavily dependent on the validity of the model for the longitudinal control that was used. The model used was a simplified 4-state model, which has been experimentally validated in various vehicle follower tests done in the PATH program.
- Multi-Sensor Faults/Process Faults : System redundancy may not be sufficient to deal with simultaneous faults of different components. It would be helpful to construct a system observer, using some of the outputs, which will essentially be a copy of the system. Thereby, redundancy in system measurement increases and other faults like process failures i.e. faults in system dynamics can be detected. Detection filters are suitable for detecting multisensor faults.
- False Alarms : False alarms indicating faults could occur due to modeling errors, sensor noise, process noise etc. The fault detection scheme should avoid giving false alarms.
- It is clear that without reconstruction the results would be catastrophic and there would be a high possibilty of an accident as the vehicles would not be able to maintain the desired spacing between themselves. It is evident too, that the simple reconstruction schemes suggested are reasonably effective.

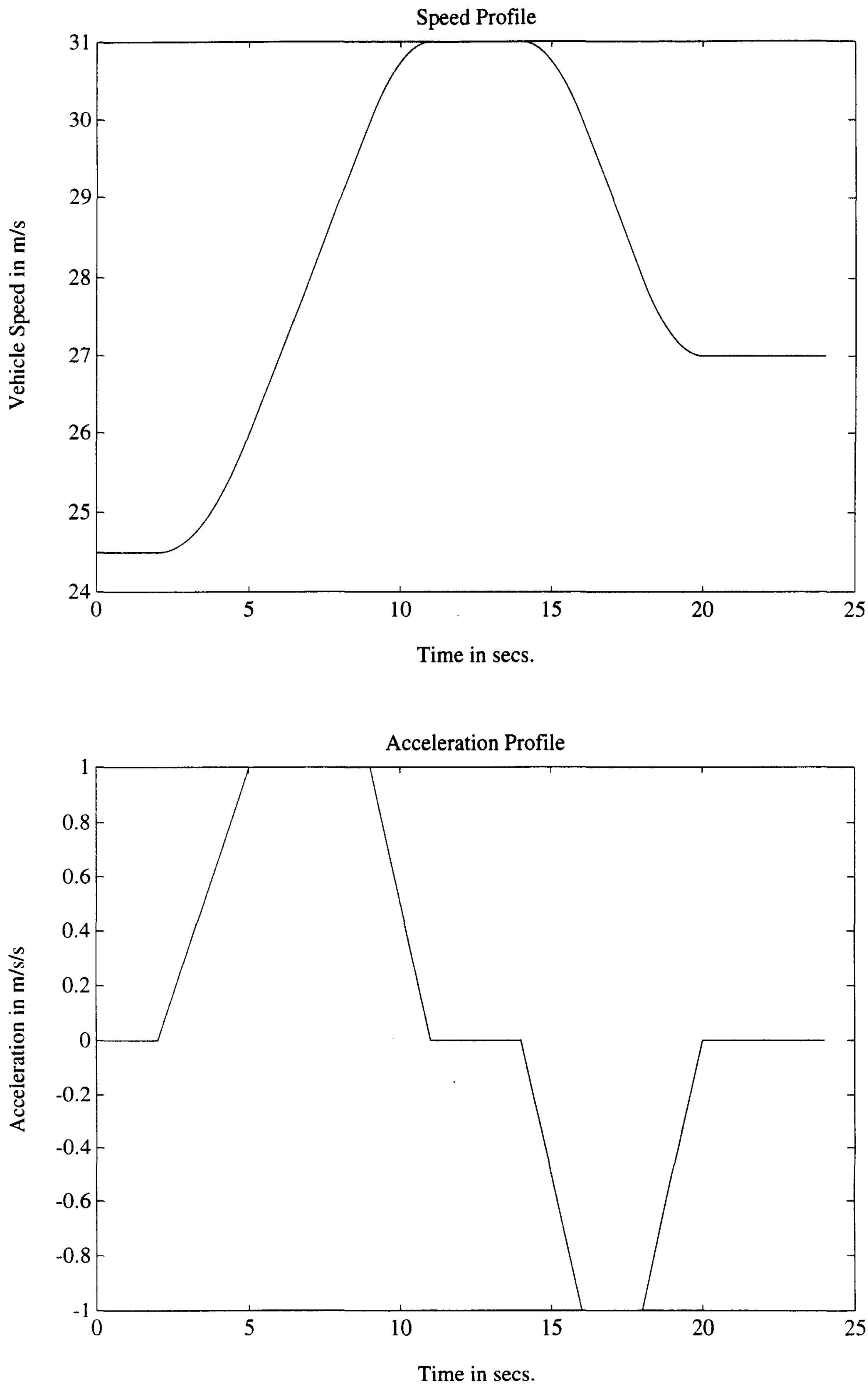
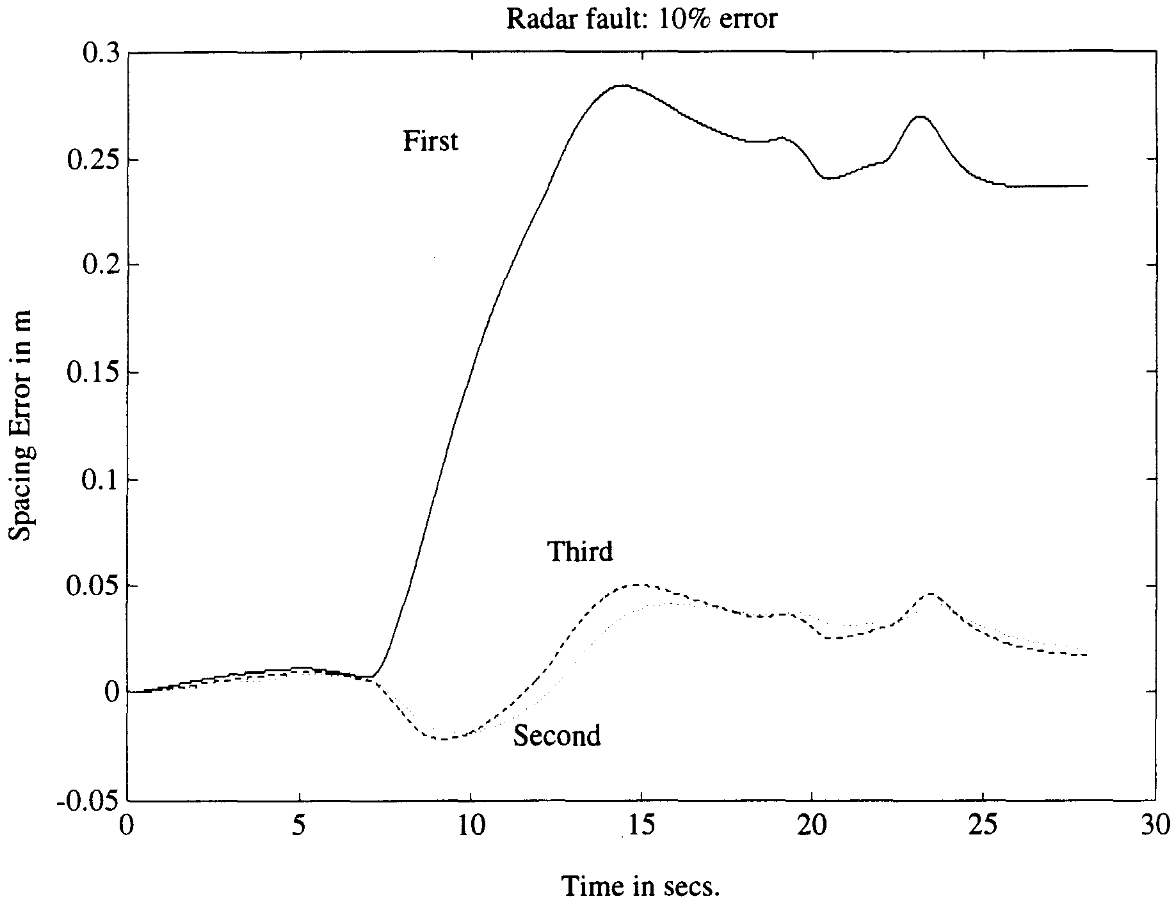


Figure 3.1: Lead Vehicle Maneuvre



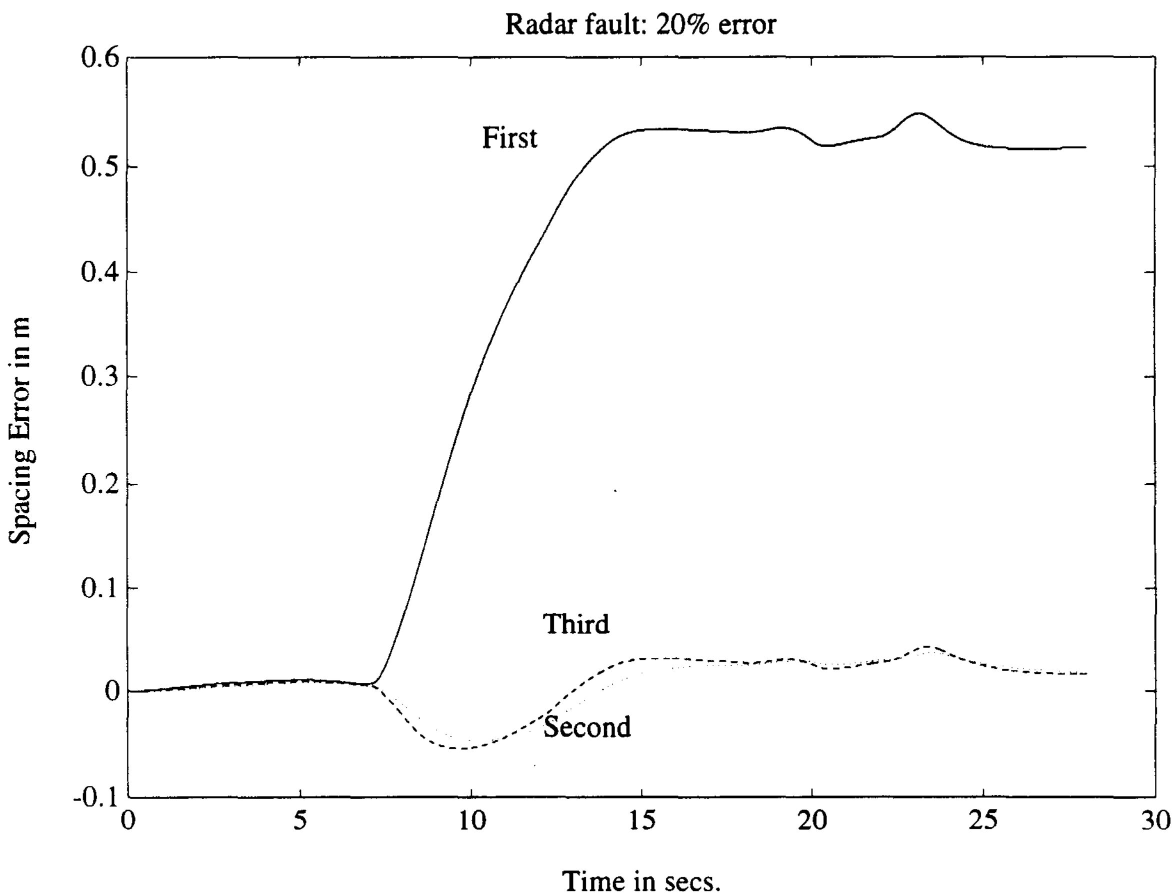


Figure 3.2: Fault in Spacing Measurement in Vehicle #1

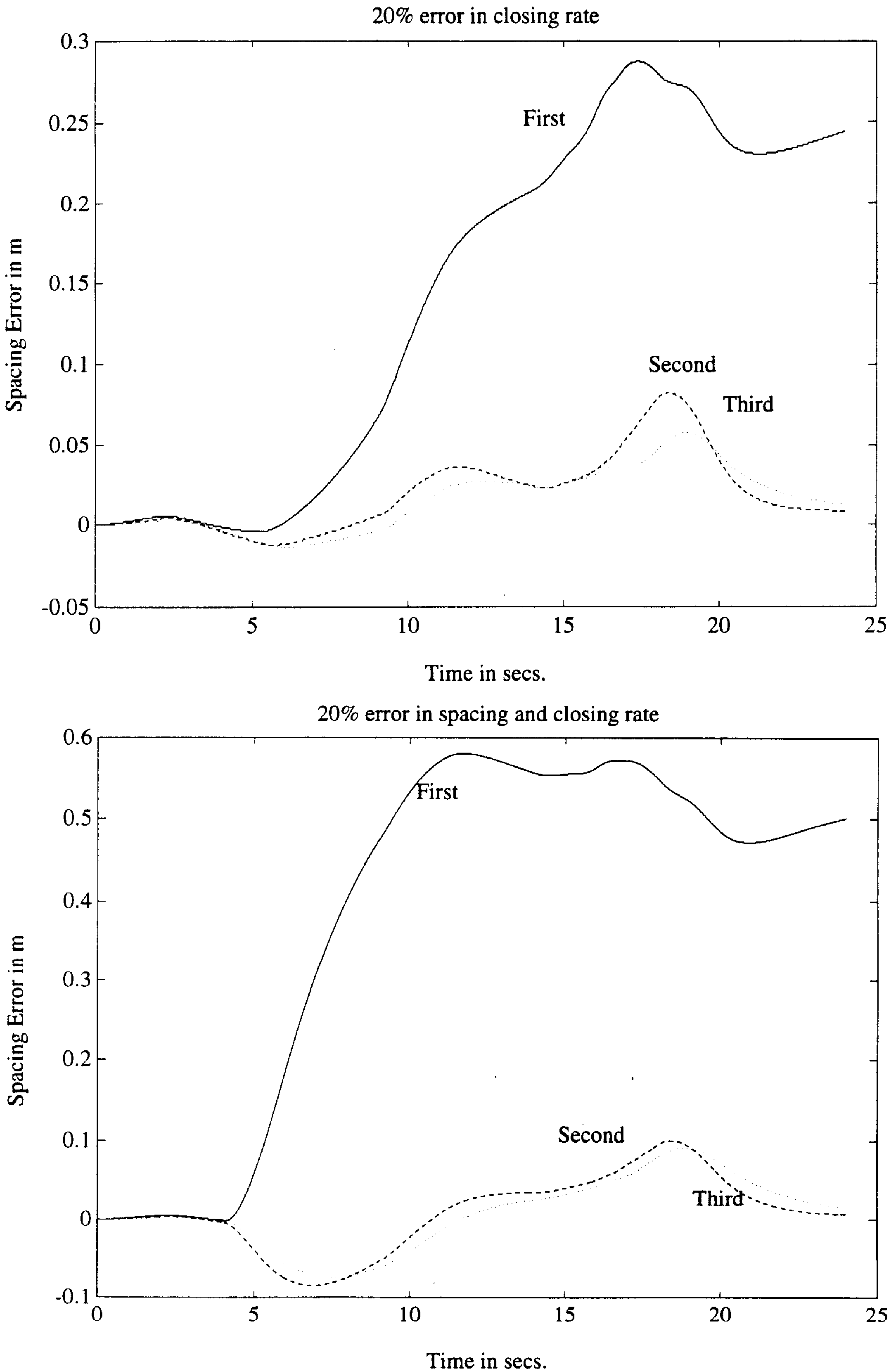


Figure 3.3: Radar fault mode in Vehicle #1

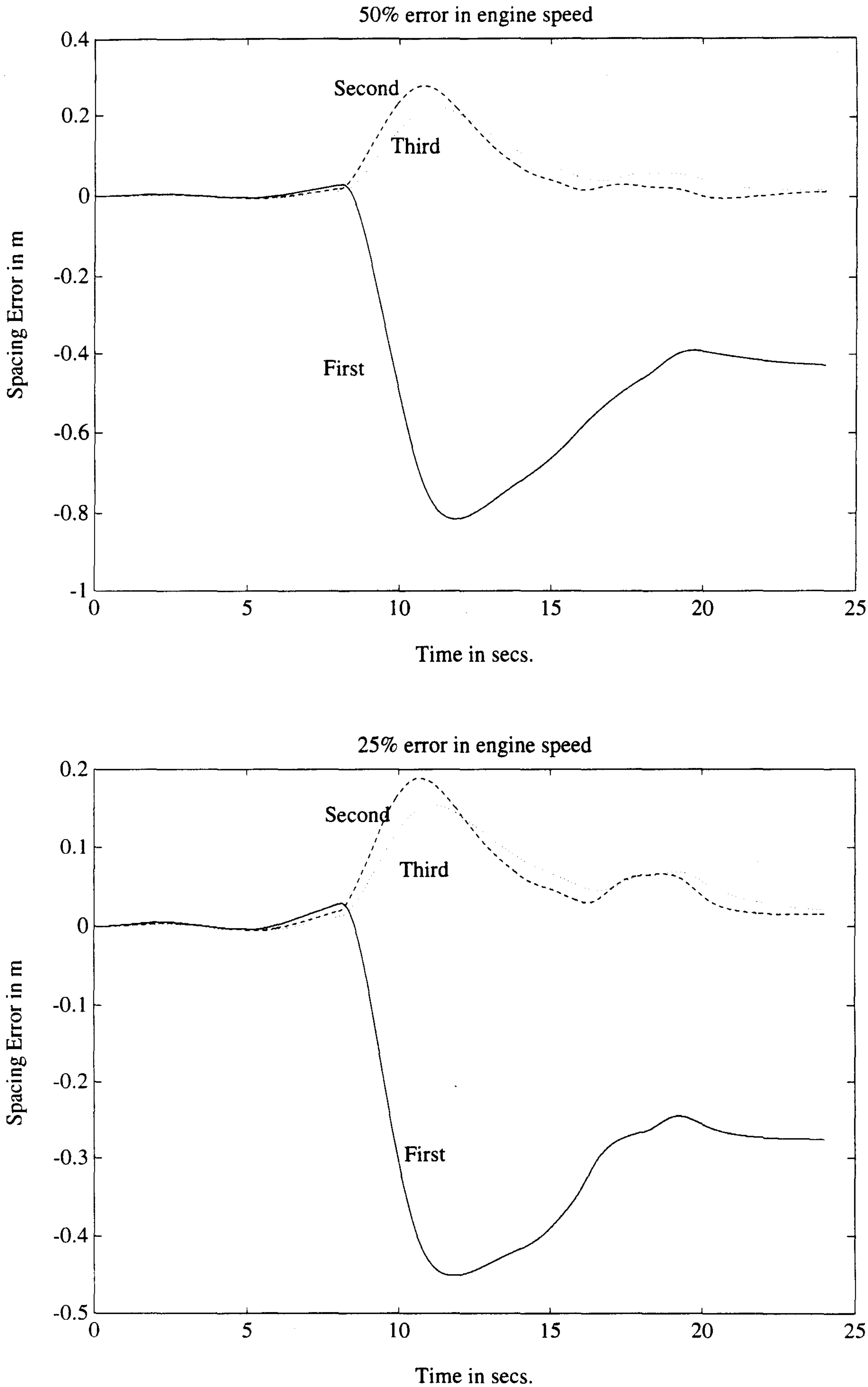
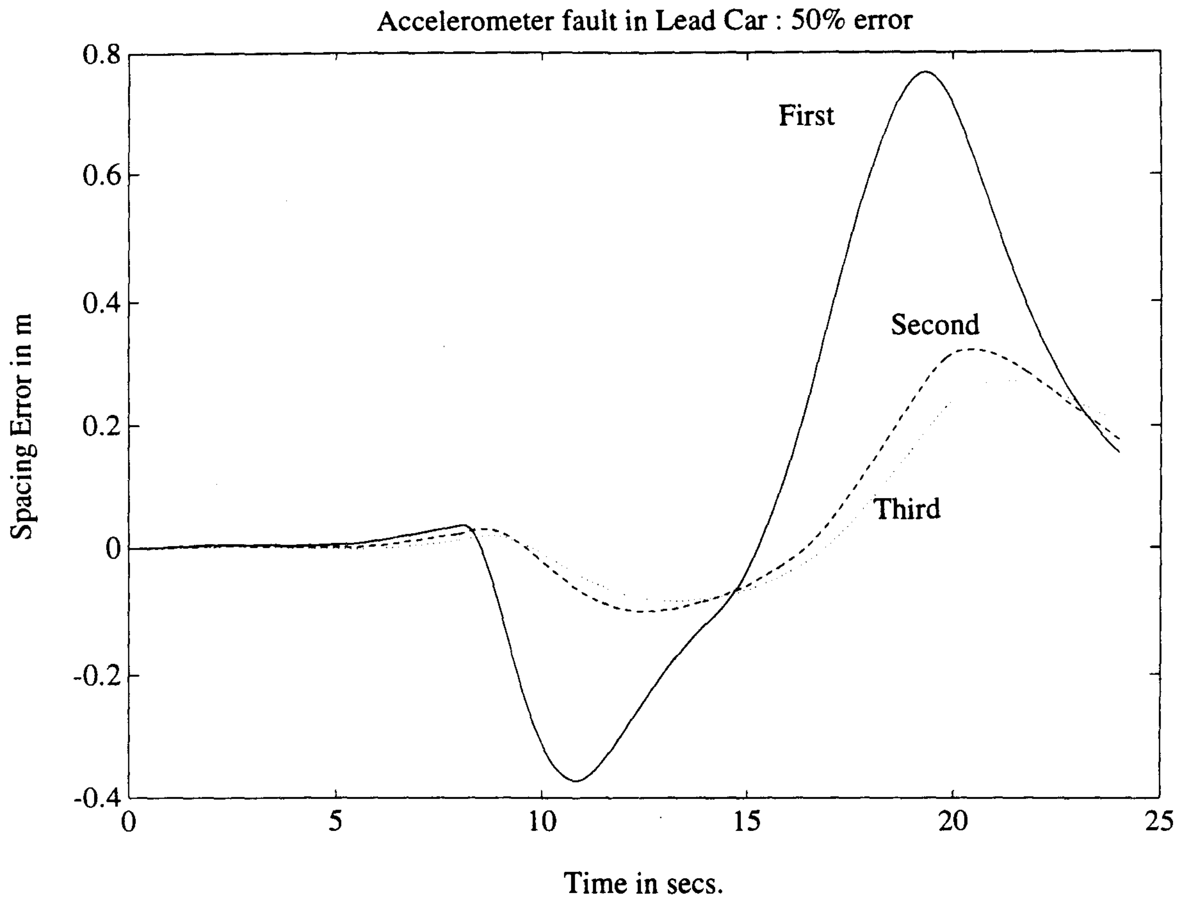


Figure 3.4: Engine Speed sensor fault mode in Vehicle #1



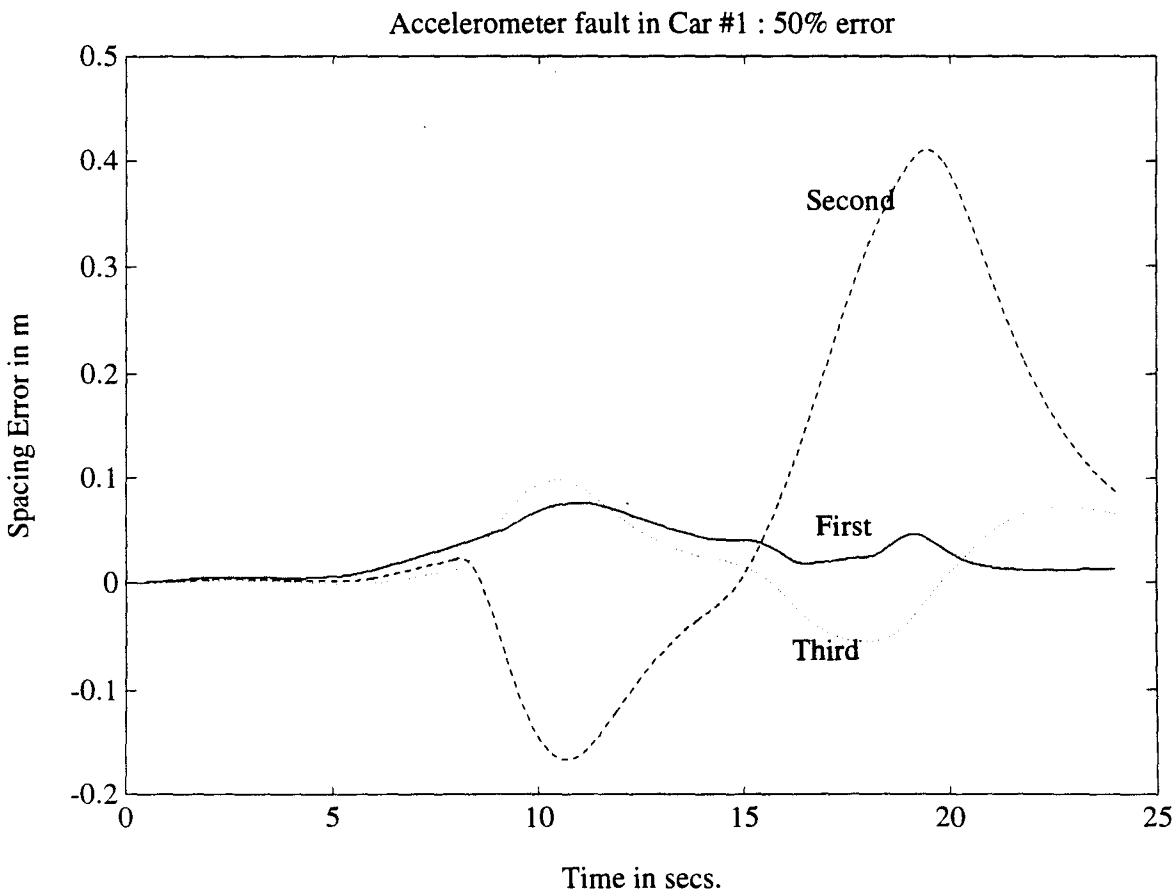


Figure 3.5: Accelerometer Fault Mode

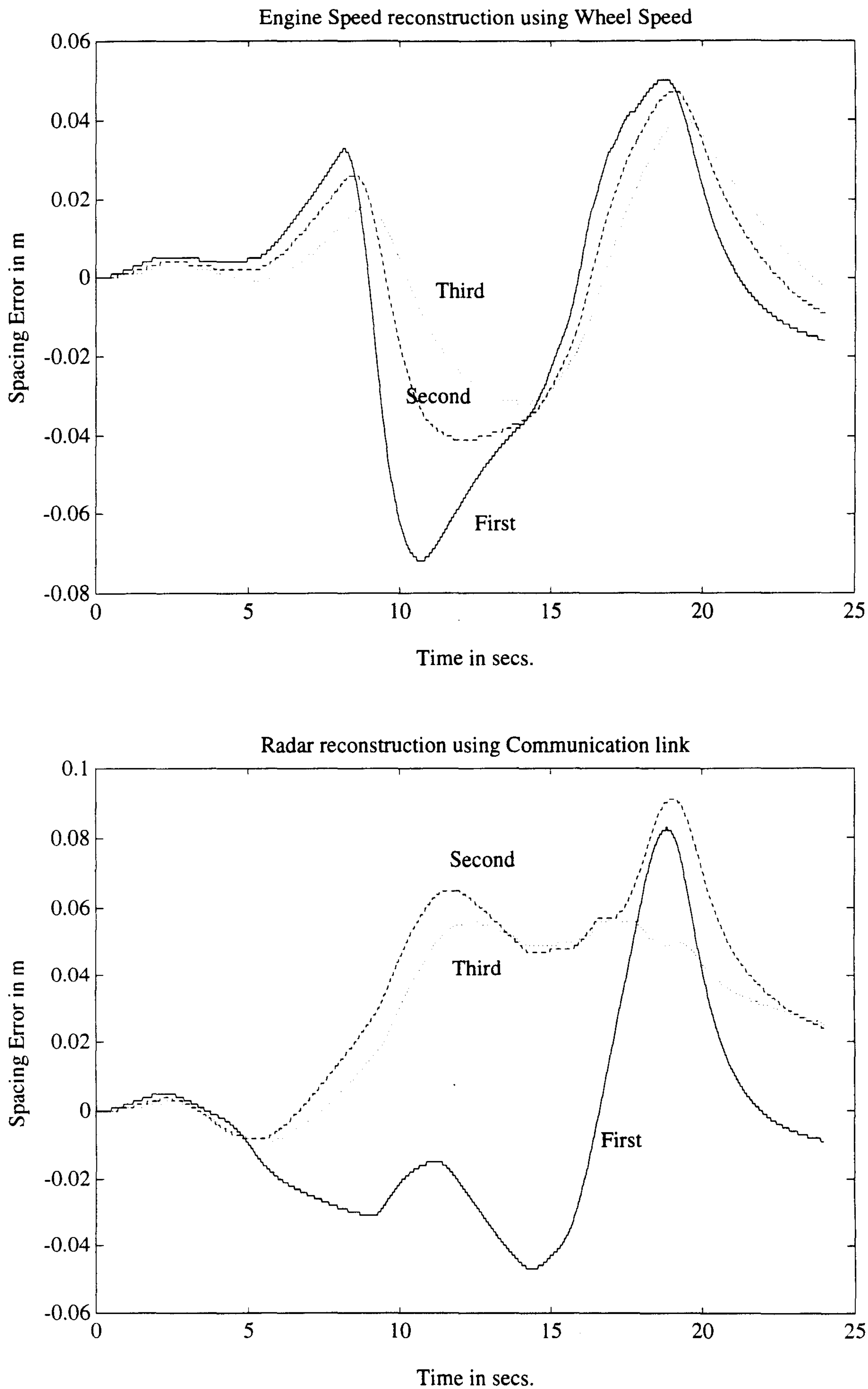


Figure 3.6: Reconstruction of sensor measurements

Chapter 4

Fault Detection

Sensor, actuator and process faults would first have to be detected and identified before implementing the reconstruction schemes suggested in the previous chapter. The general methodology suggested here is to exploit the redundancy in sensor measurements in the system, create doubly redundant sensor output sensor information and use simple voting schemes for fault detection and identification. In double redundancy systems, if one of the sensor outputs differs from the other two then it can be concluded to have developed a fault.

- Radio and Radar : In these communication components there are in-built fault flags that indicate the occurrence of faults. Ceilings can be set on maximum values of vehicle acceleration or speed that can be expected so values outside those limits can be ignored. Similarly if the change in a measurement is more than that expected in a regular maneuvre a fault could be declared after inspecting the measurement for a predetermined amount of time.

- Engine speed sensor and Transmission speed sensor : Create double redundancy by estimating
  1. engine speed using transmission speed sensor
  2. using closing rate from radar and velocity of car in front obtained from radio link to estimate engine speed.

- Mass flow rate sensor and manifold pressure sensor : These two sensors, together with the nonlinear observer built for estimating manifold pressure constitute a double redundancy system.

- Accelerometer of own and front car : Create double redundancy again by :
  1. using accelerometer reading in front car through radio and differentiation of closing rate(radar).

2. differentiating vehicle speed output from transmission speed sensor. This method can be reliable only if the sensors in question are relatively noise free.

- Throttle Actuator and throttle angle sensor: If throttle angle sensor output differs considerably from the desired throttle angle and if tracking of the cars is fine then the angle sensor must have failed, but if tracking worsens too, then the throttle actuator must have developed a fault. In eventuality of a throttle actuator fault the only alternative would be to notify all other cars in the platoon and convert to manual mode and exit the automated lane in the freeway. A redundant throttle actuator could solve that problem.

4.1 Detection Filters for nonlinear systems

Clearly fault detection in the methods proposed, though very simple in structure, demand extensive book-keeping of sensor data. Therefore, it is desirable to have some technique for fault detection in nonlinear systems similar to detection filters in linear systems. The only technique in the literature dealing with nonlinear systems is based on extended Kalman filtering. The drawback with this method is that the filter gains need to be updated continuously, which calls for great computational effort. Therefore, we are trying to extend detection filter concepts to nonlinear systems. We have been able to accomplish that for a class of nonlinear systems of the following form

$$\dot{x} = f(x) + Bu + \sum_{i=1}^{m} h_i \mu_i(t); \; y = Cx; \tag{4.1}$$

Here, the input enters linearly and the nonlinear function is assumed to be Lipschitz. The second assumption is usually easily met at least in the operating range. Another assumption is availability of all states. The longitudinal model we are considering in the PATH program is of the form

$$\dot{x} = f(x) + g(x)u; \; y = Cx;$$

The Lipshitz condition is satisfied by f(x) in the longitudinal model. The theory developed for the linear input case is easily extendable to this case.

Fault detection in the system (4.1) is effected by building a model of the system and designing the control in the model to keep the output residuals (output of the system and the model) small in the absence of a fault. In event of a fault, the residuals would grow in specific directions depending on the independence of the fault modes being considered. The observer form is of high gain and hence the measurements should be filtered for best results. The condition on state availability is necessary to guarantee directionality property for the nonlinear system.

Chapter 5

Conclusions and Future Work :

- Preliminary study of Fault analysis of vehicle follower control systems was done.
- Various failure scenarios of sensors and actuators were studied and reconstruction techniques were simulated with good results.
- An FDI strategy has been developed for a class of nonlinear systems and this strategy is being tested on various examples. A fault detection technique for general nonlinear systems is our primary research objective currently.
- Robustness issues in failure detection for example false alarms due to modeling errors, measurement and process noise etc. need to be looked into. Patwardhan and Tomizuka [5] are addressing this issue at UCBerkeley using a linearized system model. Stochastic fault modeling is necessary to simulate more real situations.
- Experimental validation of the fault detection algorithm and of the reconsruction schemes is another immediate goal of this project.

Bibliography

[1] White, J. E. and Speyer, S. L. , "Detection Filter Design : Spectral theory and algorithms", IEEE Transactions on Automatic Control, pp. 593-603, Vol. AC-32, No. 7, July 1987

[2] Willsky, A. S. "A survey of design methods for failure detection in dynamic systems", Automatica, Vol.12, pp. 601-611, 1976.

[3] R.V.Beard, "Failure Accommodation in linear systems through self reoganization," Man Vehicle Lab., MIT, Feb. 1971.

[4] J.J. Gertler, "Survey of model-based failure detection and isolation in complex plants", IEEE Controls Systems Magazine, Vol. 8, No.6, December 1988, pp. 3-11.

[5] Satyajit Patwardhan, M. Tomizuka, "Robust Failure Detection in Lateral Control for IVHS", ACC, 1992.

[6] R.Patton, P.Frank, R.Clark, " Fault Diagnosis in Dynamic Systems", Prentice Hall, 1989.

[7] De Benito, C. D. , Eckert, S.J. " Control of an active suspension system subject to random component failures", ASME Trans. JDSM&C, Vol. 112, March, 1990

[8] E. Y. Chow, and A. S. Willsky, "Analytical redundancy and the design of robust failure detection sytems", IEEE AC, Vol. AC-29, No. 1, July, 1984.

[9] D.T. Horak, "System Failure Isolation in Dynamic Systems", AIAA J. of Guidance, Control and Dynamics, Vol. 13, Nov-Dec. 1990.

[10] D.T. Horak, "Failure detection in Dynamic systems with modeling errors," AIAA J. of Guidance, Control and Dynamics, Vol. 11, No.6, Nov.-Dec. 1988, pp. 508-516.

[11] Dan Cho and P. Paolella, "Model based FDI of automotive power train systems", Proc. of ACC, 1990, pp. 2896-2905.

[12] D. Cho and P. Paolella, " Automotive powertrain sensor diagnostics using analytical redundancy", submitted for publication.

[13] W. C. Merrill, J.C.Delaat and W.M. Bruton, " Advanced detection, Isolation and Accomodation of Sensor Failures - Real time Evaluation", J. of Guidance, control and Dynamics, vol. 11, no. 6, Nov.-Dec. 1988.

[14] H.L. Jones, "Failure detection in linear systems", Ph.D thesis, Dept. of Aeronautics and Astronautics, M.I.T., Cambridge, Mass., Sept. 1973.

[15] W.B. Ribbens, G. Rizzoni and P. M. Olin, " Failure detection in 4-wheel steering systems", sent for publication.

[16] R. C. Montgomery and A. K. Caglayan, "A self reorganizing digital flight control system for aircraft", AIAA 12th Aerospace sciences meeting , Washington, Feb. 1, 1974.

[17] D. McMahon, V.K. Narendran, D. Swaroop, J.K. Hedrick, K.Chang, P. Devlin, "Longitudinal Vehicle Controllers fo IVHS : Theory and Experiment ", Proceedings of American Control Conference, June 1992, Vol. 2, pp 1753-1757.