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

Towards a Fault Tolerant AHS Design
Part I: Extended Architecture

John Lygeros
Datta N. Godbole
Mireille Broucke

California PATH Research Report
UCB-ITS-PRR-96-14

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.

June 1996

ISSN 1055-1425

4 Fault Classification

Appendix A contains a comprehensive list of faults, for both the vehicle and the infrastructure. Because the list is so large, we would like to be able to design controllers that deal with whole classes of faults or combinations of faults. In this section we show how the capability and performance structures can be used to induce such a classification. The classes reflect the potential available in the system in the presence of a combination of faults and adverse conditions. Faults in the same class will lead to the same predicates in the capability structure returning zeros. Using this principle as a guide we are able to distinguish the following classes:

Vehicle stopped, must stop: This class contains the most serious vehicle faults. The vehicle can not continue moving on the AHS safely and has either already come to a stop or it should be commanded to do so and wait to be towed away. Because of the severity of the situation, all the layers of the control architecture will undergo some degradation in performance and assist in resolving the fault condition.

Faults in this class will typically lead to a false "Capable of being a free agent" predicate in the regulation layer supervisor. This will in turn lead to predicates returning zeros all the way up to the link layer. Depending on the type of fault we identify three subcategories which are differentiated by the technique that is used to stop the faulty vehicle. The subclasses and the faults contained in each one of them are listed in the appendix.

Vehicle needs assistance to get out: The faults in this class are slightly less serious. The vehicle may continue moving but has lost some essential capability and it must therefore exit the AHS as soon as possible. Moreover, it needs the assistance of its neighbors to do so. Typically, faults in this class will result in the normal mode coordination layer predicate returning a zero without any of the link layer predicates being affected. Therefore, these faults can be handled locally and need not involve the higher layers of the architecture (link and network). As before, the faults are divided into subclasses according to the affected capability.

Vehicle needs no assistance to get out: The faults in this class are even less serious. Typically the vehicle is fully functional but should leave the system soon to avoid further problems and hazards (in case a second fault occurs for example). Typically faults in this class result in regulation layer predicates returning zeros, without any coordination layer predicates being affected. They are handled by special controllers in the regulation layer and neither the neighboring vehicles nor the roadside need to be alerted.

Vehicle does not need to get out: This class contains minor faults that require no special action but should nonetheless be recorded and the driver should be notified in case he needs to alter the travel plan. They result in only physical layer predicates returning zeros.

Infrastructure failures: This class includes all faults that induce a reduction in the capability of the infrastructure. They usually lead to severe degradation in performance. Some of them can be handled by the normal mode controllers of the link and network layers, but some may need drastic changes in the operation of the system. The faults reflected in the infrastructure predicates discussed in Section 3.1.5 are contained in this class. They result in link layer predicates returning zeros, without any changes in the coordination layer predicates.

Driver–Computer interaction down: Problems in this class mainly occur during the entry and exit to the system. We assume that once on the freeway, the driver may not interfere with the system operation (except for route/destination selection) and therefore can not induce any special faults. These faults are resolved by simple additional strategies that do not interfere with the rest of the design (see [Godbole *et al.*1995b] for details).

It should be noted that, even if the list in the appendix is not exhaustive, any additional faults we come up with can be uniquely classified using this scheme. Moreover combinations of faults can also be classified similarly.

Note; The classification of faults and the design of degraded mode maneuver control laws *do not* assume existence of a *breakdown lane*. If such a lane is provided, then in case of certain faults, it might suffice to take the faulty vehicles to the breakdown lane and wait for emergency roadside assistance rather than exiting the highway or stopping on the highway lane. This amounts to a refinement of the classification introduced above. The maneuvers and control laws developed based on the current assumption can be easily adapted to accommodate for the breakdown lane.

A List of Faults

All faults are listed in their corresponding classes and subclasses, according to classification of Section 4.

A.1 Vehicle stopped/must stop

1. no throttle control, no engine power, out of gas, no power transfer, vehicle to vehicle communication down (Radio - Needed for coordination)
2. no steering control, uncontrolled object ahead, no control computer, magnetometer failure, no sensing of distance and velocity of car ahead (long and short range)
3. no brake control

A.2 Vehicle needs assistance to get out

1. no control of transmission / selection of gear
2. no long-range (longitudinal) sensing of vehicles
3. no short-range (longitudinal) sensing of vehicles
4. no lateral sensing of vehicles
5. flat tire - reduced steering capability
6. Vehicle - Vehicle communication down (Infra-Red: Needed for Follower operation)

A.3 Vehicle needs no assistance to get out

1. Non-crucial Sensor fault: engine sensor (e.g. intake manifold pressure sensor), accelerometer, wheel speed, etc.
2. low on gas
3. Single fault in a redundant sensor set
4. Vehicle-roadside communication down because of on-board equipment failure

A.4 Vehicle does not need to get out

1. Lights won't go on
2. In vehicle displays not working
3. Out of range of magnets, magnetometers working, not changing lanes

A.5 Infrastructure Failures

1. Network layer down or communication between link and network down
2. Link layer down or communication between link and vehicle down in the entire link due to roadside equipment failure
3. unable to communicate with object on AHS
4. Roadside sensors not working
5. Lane(s) blocked
6. Exit(s) closed
7. Entry(s) closed
8. Robustness spill over and environment
   In this category we group all problems caused by unfavorable conditions that the normal mode controller is not robust enough to handle. These problems may not be the result of faults, but may arise due to gradual performance degradation. Since they result in certain normal mode predicates calculating as false, however, degraded modes will have to be designed for them. If the gradual performance degradation is limited to a single vehicle then it will be classified into one of the classes 3.3.1 through 3.3.4. Here we consider the effect on the infrastructure. This is mainly caused due to environmental degradation such as rain or snow. They will be grouped in two subclasses:

   - loss or reduced traction with road (lateral & longitudinal)
   - reduction in sensor range or accuracy (caused by rain, dust, sunshine, etc.)

A.6 Driver/Computer Interaction Down

Problems in this class mainly occur during the entry and exit to the system. We assume that once on the freeway the driver may not interfere with the system operation and therefore can not induce any special faults.

1. Improper Exit: Driver unable to take control and/or system unable to transfer control at exit
2. Improper Entry: Wrong destination/route entered by driver or system unable to start automatic control at entrance or manual driver tries to enter automated TL

A.7 Faults not considered

1. Software implementation errors
2. Design errors such as protocol design errors, control design errors
3. Communications errors including: wrong message, message to wrong car, etc.

B Causes of Gradual Performance Degradation

B.1 List of Causes:

Environment

1. Longitudinal Wind
2. Lateral Wind
3. Sunshine
4. Sunrise-Sunset
5. Ice
6. Snow
7. Fog
8. Rain
9. Wet Road
10. Oil on Road
11. Pot Holes
12. Gravel
13. Other Debris
14. Road Slope
15. Road Bank
16. Road Curvature
17. Slip Stream of Other Vehicles
18. Magnet Damage
19. Lane Marker Damage

Vehicle

20. Vehicle Make
21. Tire Pressure
22. Brake Fluid Pressure
23. Suspension
24. Longitudinal Sensors
25. Lateral Sensors
26. Radio Link
27. Radar
28. Accelerometer
29. Cameras
30. Steering Error
31. Accelerator Error
32. Braking Error
33. Brake Fade
34. Brake Wear
35. Yaw Rate Sensor