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

Methods of Analysis of IVHS Safety

Anthony Hitchcock

**PATH Research Report
UCB-ITS-PRR-92-14**

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 author who is 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.

December 1992

ISSN 1055-1425

CONTENTS

GLOSSARY OF TERMS

In this paper, a number of specially-defined terms of art, and a number of abbreviations are used. The following refers the reader to the section where the terms are defined and spells out the abbreviations.

Term	*Section*
AL - automated lane	2.7.2
AL license	2.8.4.7
AR - asynchronous register	2.8.3.4
bem - block entry marker	2.8.4.4
busy flag	2.8.4.4
block	2.4
CA mode - Closed-Ahead	2.8.4.8
change-lane manoeuvre	2.8.4.11
Crashstop Mode	2.7.3
dormitory	2.7.2
emergency-change manoeuvre	2.8.4.11
fence	2.7.2
free agent	2.8.4.3
forced-split manoeuvre	2.8.4.11
full braking	2.7.1
full platoon braking	2.7.1
gate bit	2.8.3.4
hazard	2.7.1
identifier	2.8.3.2
iterator	2.8.3.4
loc - lane number and odometer reading	2.8.4.4
manual spacing	2.7.1
maxspeed	2.8.3.4
merge manoeuvre	2.8.2.11
NE mode - No Entry	2.8.4.5

SECTION 1. INTRODUCTION

This is the final report of the PATH Program's MOU (Memorandum of Understanding) 19 — "Methods of Analysis of IVHS Safety." The total report comprises six separate documents. This is the primary one. There is also an executive summary, which summarises what is said here. Section 2 of this report describes two complete specifications of possible automated freeway systems and fault tree analyses of them. Full details of these, including definitions of each module expressed in a formalised language are published as four separate reports (Hitchcock, 1991c, 1991d, 1992c, 19924). These reports should be regarded as appendixes to this one.

1.1 Overview of Achievements

The two principal sections of this report, Sections 2 and 3, each start with an "Overview of Research Achievements." Effectively these sections are executive summaries of the content of that section. Overviews of Sections 1 and 4 follow.

This section explains the administrative background to the research. Details are given of the achievements on the minor tasks required by the contract. The first of these was to carry out a literature survey. A bibliography on safety of IVHS was prepared and sent, in draft, to the librarians in the Transportation Library at the Institute of Transportation Studies, University of California, Berkeley. There it formed one of the bases for the PATH bibliographic database. Since this database was thereafter maintained professionally, there was no point in duplicating any further work in this area within MOU 19. Inevitably, the original bibliography was largely ephemeral. However, for the sake of completeness the original is reproduced as an appendix.

Section 4 sets out the consequences of the research and discusses how it can be applied. Application of this work is necessary if IVHS is to be used in California. Yet it raises major administrative, political, and institutional problems, especially in the area of automated freeways.

Basically, the problems arise because an automated freeway, and its safe operation, cannot be the sole responsibility of any one person or institution. Further, absolute freedom from risk is a phantom. Trade-offs can be made between the efficiency of the system and its safety. Here efficiency is equivalent to the capacity in vehicle-miles/hr of the automated freeways, while safety will be measured in casualties/person-trip or person-mile.

In Section 4 the concepts of the separate management of design and verification are picked up from the earlier sections. System safety requires that one group is responsible for specification of the system. The same group is responsible for engineering design to meet the specification. Another group must be responsible for verification of design and validation of specification. There are needs for formal communications and documentation.

However, there is also a very complex **meta-system.** This is the process which determines with what objectives the complex process shall be managed. Here too, perhaps, there is a need to specify, design, verify, and validate. To put it another way, it has to be decided how the interests of the parties concerned can be reconciled. These parties include vehicle and equipment manufacturers, highway authorities, travellers, and others.

Section 4 offers no solution to this problem. Hopefully, however, it does help to define it. But the problem has to be grappled with. Unless the design and operation managers know what they are trying to do when they make a system acceptably safe, they cannot do it. Until they can, there can be no automated freeway.

1.2 PATH's MOU 19

The objective of this work was:

> "To develop and demonstrate methods by which safety of IVHS (Intelligent Vehicle/Highway Systems) can be assured, assessed, and evaluated."

The individual tasks were:

1. Literature Survey — Bibliography

2. Accident data sources and cost-benefit analysis

3. Methods of analysis of AVCS-1 systems — report

4. Specification and analysis of hazards (AVCS-2/3 systems):

    a. Development of techniques
    b. Application of techniques to system #1
    c. Application of techniques to system #2

5. Communication of results to industry, administration, etc.

6. Final report.

Data collection was expressly excluded from the work.

In the remainder of this section the first five of the tasks mentioned above will be considered. The achievements and remaining problems of each will be briefly reviewed. (This report itself, of course, is the sixth task.) Sections 2 and 3 describe the work done under the two principal headings. These are tasks 3 and 4. In Section 4, some conclusions are drawn about the way in which this work can be applied.

There is an appendix which reports on task 1. In addition, five independent publications supplement this report (Hitchcock, 1991c; 1991d; 1991e; 1992c; 1992d). These refer to tasks 3 and 4. They can be regarded as appendixes to this report.

1.2.1 Cost-Benefit Analysis

The concept of cost-benefit analysis of IVHS in California presents policy problems. There is not only the usual technical problem of predicting how increases in capacity would be taken up. There is also the policy question of deciding how to value the changes.

Compression (shortening in time) of the peak would certainly occur. There is little data about the extent to which it would occur, and no policy about how it would be valued. Increases in capacity would also result in:

a. changes of the time at which trips were made;
b. changes of the destination of trips for a given purpose;
c. changes of the association of trips with one another (“unchaining”);
d. generation of new trips.

For only the last of these is there a standard method of valuation. For none is there a policy about valuation. On the safety side, there is no policy about the valuation, in dollars and cents, of life, pain, suffering, and bereavement.

Thus we cannot state the values of benefits in a cost-benefit analysis. The cost side is also deficient. At the time there were no designs, even conceptual ones, of an automated freeway. If we do not know what it is we are talking about, how do we know what it costs?

True cost-benefit analysis thus requires policy decisions which have not been made. However, it is possible to make some cost-effectiveness calculations which compare the benefits of improving one road rather than another. The comparisons can take no account of network effects. To allow for network effects requires something like the present study of the SCAG (Southern California Association of Governments) network currently in progress in PATH.

Data can be taken from the annual Caltrans Route Segment report, together with the delay measurements which each district of Caltrans makes by probe car methods. Regrettably, while these data are adequate for its primary purpose, the accuracy is such that random uncertainties in the relative benefits of automation calculated are large. There are also large systematic uncertainties due to the assumptions. There is therefore no point in pursuing this question further. This is particularly the case in the light of the existence of the SCAG study, which will give fuller results and to which policy guidance is available.

1.2.2 Communication of Results

Research is of little value if its conclusions are not made known to those who can use them in an appropriate form. The discipline of science also requires that results be recorded, so that others can perceive that they are repeatable. The results of this work are concerned with the systematic safety problems of IVHS. The results clearly have both technical and policy implications.

The technical results have been communicated in the following ways:

a. Publication of technical papers. The references list eleven papers under the authorship of Hitchcock prepared during the period of this contract. Jovanis, et al. (1992) is a twelfth, and this paper a thirteenth. Two others are in preparation.

b. Presentation at professional meetings. Eight of the papers referred to have been presented at professional meetings held under national auspices. Two presentations have also been made which do not involve papers. A third is planned.

c. Attendance at committee meetings of professional institutions at which the implications of research, both technical and policy, are discussed. Under this contract, membership of three committees, three subcommittees, and one working party of IVHS America has been accepted, and most meetings of them have been attended. One of the subcommittees and a workshop have been chaired. Contributions have been made at all, based on the research reported here. There has also been membership of one TRB committee, and contributions made to two others.

The committees of IVHS America have a national policy role, as well as a technical one. The results of this research have been noted in IVHS America's Strategic Plan.

At state level, the original contract envisaged a Caltrans Safety Policy group, which would develop a safety policy. There would be dialogue, it was suggested, between this research and other partners. In fact, only now is any such body emerging and it is too early to say what the impact of this work on policy thinking in California will be.

SECTION 2. SAFETY CONSIDERATIONS FOR AUTOMATED FREEWAYS

2.1 Overview of Research Achievements

This research has as its field the safety of IVHS devices in areas which are relevant to PATH. These include automated freeways. The work started in April 1990. Virtually nothing of a scientific character was known about safety of automated freeways. There was neither research nor practical experience on any aspect of IVHS safety in North America.

The safety problem for an automated freeway is not like that on ordinary roads. Most road accidents (90% +) are due to human error. Automation eliminates all these. But faults do arise in machinery, automated or not. The probability that a fault will arise, in motion, on a familiar machine, like a car, can be determined by observation. If there are new components, like vehicle control systems, fault probabilities can be deduced from experience of similar devices in other places.

Most faults will not lead to casualties, however well or ill the system is designed. But automated freeways, as will be seen in Section 2.3, operate with platoons of vehicles (groups of ten or more, closely-spaced) moving at high speed. If two platoons collide, or if one platoon hits a stationary object, the number of killed and injured is likely to be large. One has to design so that such accidents are very infrequent. It is of course impossible to design so that they will never occur. It will always be possible to imagine some combination of simultaneous unrelated faults which will cause a catastrophe.

A first step is to ensure that no single fault can lead to casualties. This must be true in any of the numerous configurations that can arise in normal operation. This can be done, at the cost of some degradation in performance and/or increase in cost. But faults are not uncommon, and two or more may interact. A safety criterion must be selected. As it becomes more stringent, so does the cost in money and performance. Trade-offs must be made.

So the first problem that the work set out to solve was:

A. How do you specify a safety criterion for an automated freeway? Can you design an automated freeway which will not permit casualties if that criterion is satisfied?

However, even though drivers on automated freeways cannot make human errors which lead to casualties, designers, too, are human. Their human errors, too, must be guarded against. So the second question was:

B. How can you demonstrate that your design does what question A requires?

It might be imagined that B is trivial: all you do is to consider each component in turn, and determine the ways in which it can fail. Then, for every possible configuration of normal operation, consider each possible failure — one at a time, two at a time.. . . and so on. This would work. Even if it could be computerized it would take centuries. Another way must be found.

We have solved both these problems. The solution is a demonstration — two such designs have been constructed; both have been verified. That is, demonstrations have been made for each design that each will not admit casualties, even if any two components fail at once. In both cases the methods are generally applicable. The design method is called *complete specification* and the verification technique is called *fault tree analysis.* Both techniques are analogous to those in use in other fields.

The first example system was chosen to have one automated lane on a freeway with other lanes devoted to ordinary traffic. Most of the intelligence in it is contained in the infrastructure. The second one has many automated lanes and mainly vehicle-borne intelligence.

The primary purpose of the examples was to provide two very different systems which could be used to test methods of determining their freedom from design errors. One way of doing this would have been to design a system without concern about whether it was safe or not. Then the verification method could have been applied to it. If the methods proved that the design was unsafe, the methods would have been shown to be effective. However, it was a secondary objective of the work to demonstrate that it was possible to design a safe system. At the time, no one knew if safe systems existed. At the time, the judgment was made that, if systems did exist which met the safety criterion, some, at least would have infrastructure-borne intelligence. Such a system was therefore chosen for the first example.

The second example should clearly be different from the first. A multi-lane system with vehicle-borne intelligence and many lanes was appropriate. Happily, by the time the work on the second system was due, Hsu, et al. (1991) had produced a partial design of such a system. This was therefore adopted as the basis for the second example. The original work did not include the possibility of faults. Conditions for entry and exit were also absent. Also, there were no features to maintain safety in the presence of faults.

In the present work, therefore, the first step was to complete the design work reported by Hsu et al., by making allowance for the potential presence of faults in vehicles. Procedures for entry and exit were also designed, all conceptual. Then safety could be tested. It turns out that it is possible to design a system meeting the safety criterion chosen with mainly vehicle-borne intelligence. A small amount of intelligence in the infrastructure is, however, necessary for both normal operation and safety in fault conditions.

Some special physical infrastructure is, however, necessary. Here our results are proved rigourously and generally. Conformity to the safety criterion requires that the automated lanes are separated from the rest of the freeway by a small barrier or “fence. " If there is more than one automated lane, there must be fences between them. If there are no fences, small, damage-only accidents inevitably develop into multi-casualty catastrophes. There are also some other general limitations, which constrain the physical layout severely.

Besides answers to the two questions there are spinoffs. One has just been mentioned — there are designs for automated freeways which are safe. Another is that it would be unwise, if the design were intended to be implemented, to have the same person or team do both the design and the verification. It would be too easy for the same error to be made twice. People do have blind spots, and they must be guarded against.

This means that there must be two teams, equal in status, in the responsible organization: one is concerned with design, and the other with verification. It also means that great care must be taken by both teams to ensure that everything is defined with mathematical precision, and that decision-logic is recorded precisely.

In the current work, while one person did have to wear both hats, great care was taken to define everything precisely and to record everything in detail. This would have been necessary if there had been two teams. A special formalism was developed for this, resembling the languages used for computer programs based on mathematical logic. This material is being published (Hitchcock, 1991c; 1991d; 1992c; 1992d), so that this project’s work does conform to its own recommendations. Reference can be made to this very detailed material. The extreme detail is not suitable for this summary.

2.2 Structure of Section 2

In this section the work just reviewed is presented in greater detail. As has been explained, where the two examples are concerned, greater detail can be found in the four reports just cited. Here:

a. A short introduction describes what an automated freeway is, and why it is being researched in PATH. Some basic concepts developed before this work started are introduced, and commented on.

b. An account of the system architecture indicates the different information requirements and range of action of different “levels” in the system. It is pointed out that the legal provisions under which the system operates affect its design. Law is the highest layer in the architecture.

c. An overview of the safety problem is followed by discussion of appropriate safety criteria.

d. It is proposed that the basic safety needs can be met by adopting the design, verification, and validation procedures which are developed.

e. The feasibility of what has been developed on theoretical grounds is demonstrated by means of two examples.

f. From the experience of working the two examples, some conclusions are drawn and some speculations set out about some basic design concepts for automated freeways.

2.3 Why Automate Freeways?

2.3.1 Mission of PATH

In California, most adults have the use of a car. Land use patterns reflect the wishes of the electorate to adopt a spacious lifestyle. Consequently many daily journeys are long. If speeds are constrained, even to 20 mph or 30 mph, the amount of time occupied by travel becomes irksome or intolerable to many people. In such conditions the demand for regular use of restricted-access roads (e.g., freeways) is large and inelastic.

But as the lifestyle spreads, and more and more people want to live the Californian way, congestion increases. Travel by car in congested conditions is associated with environmental pollution (the climate and topography of much of California makes it sensitive to air quality, though there are other factors also). Travel, too, is associated with traffic casualties. Congestion threatens something very important.

The general level of wealth in California is among the highest in the world. Californians are prepared, apparently, to see large sums spent to ameliorate these problems. One ingredient of a possible solution is to automate the existing freeways. In principle, automation could eliminate congestion in most places forever. Because automation constrains vehicles to precise lanes it can make inductive pick-up of electric power a practical proposition, thus reducing pollution from vehicle exhausts. It offers major possibilities for reducing road accidents. It may well have a lower public cost than alternatives.

Automation also has disadvantages. In particular it will remove control of the vehicle from drivers. It will enforce movement on constricted, fenced lanes in platoons. It may turn the dream of the open road into a claustrophobe's nightmare.

These arguments urge not necessarily the adoption of automated freeways, but at least their development to a point where decision-makers can see enough to decide. This is the role of PATH in its work for Caltrans. This research is concerned with the safety of the concept, which is one of the decisive areas.

2.3.2 Previous Work

Some work by others, before this research started, had caused the bulk of the work in PATH to be carried out on the basis of some technical assumptions. The most important is that traffic on automated lanes is platooned (organized into closely-spaced groups of up to ten or twenty vehicles, separated by much longer gaps). This was originally demonstrated by Shladover (1979). It is right that the present work follows the general basis of work in PATH. However, since the argument for platooning is a safety one, it should be reviewed here.

Automatically-controlled sensors can detect a vehicle ahead at least as quickly as a driver. Automatic controls can initiate a control action more quickly than a driver, and they do not suffer from the lapses in vigilance to which all drivers are liable. However, a control action — a steer to left or right, or an adjustment of throttle or brake — is a mechanical action. There will always be an interval of time — perhaps 100 milliseconds — between initiation of an action and the full response of the vehicle control. Then, of course, further time will elapse while the vehicle changes speed or direction. But 100 milliseconds is a much smaller total response time even than the 0.2-0.3 seconds sometimes achieved by young fit drivers when highly aroused. Certainly it is less than the 1 to 2 seconds or so which is all that can be expected of an average driver who has no reason to have alerted himself. This reduction in response time makes much closer spacing possible without compromising reliability.

Shladover (1979) argues, on safety grounds, that platooning is to be preferred to more uniform spacing. In a platoon, a number of vehicles, between perhaps three and twenty, follow one another at very short spacings. Platoons are separated by such a spacing that if a leading platoon is brought to rest abruptly, a following one can brake to rest without a high-speed collision. For full details, reference should be made to the original report. Briefly, it is well established that collisions between vehicles with relative speeds of 15 mph or more are progressively more likely to injure or kill the occupants than ones that occur at high speed, but low relative speed (delta-V). If vehicles are platooned, the short spacing means that if there is a failure in one vehicle there is no time for its speed to change very much before collision with its successor. If spacings are in the range of 5-10 m, potentially lethal delta-Vs can be built up.

After the low-delta-V collision, however, the vehicles are both still moving at high speed Often they will be damaged and not respond to controls. If injury is to be avoided they must still decelerate to rest tolerably sedately. In particular they must not undergo a second high-delta-V collision with another vehicle or with the infrastructure. If the platoon is on an ordinary freeway lane, there can be no protection against this. Indeed, a second, potentially fatal, collision is very likely. However, as will be seen, there are ways to ensure safe deceleration to rest. Therefore, it is argued, if vehicle density in a lane is to be high, platooning is preferable to uniform spacing.

This argument is not flawless. The topic of the research in Shladover (1979) is Personal Rapid Transit (PRT). Tracked vehicles are thus under consideration. On tracks, derailment can occur. The deceleration of a leading, derailed car is indeed much greater than can be achieved by braking. In the case of road vehicles the position is less clear.

In the first place, vehicle faults which cause so large a deceleration that the automated controls in its successor cannot cope are certainly very rare. (The resulting accident will be called a follower’s crash here.) Failures which induce follower’s crashes do exist — engine seizure and a ruptured transmission shaft falling onto the road are two examples. It may be, however, that they are so rare that the number of multiple-fatality accidents which would result if spacings were uniform would be acceptably low. Further, if this is the case, it may also be that with closer spacings there would be more total collisions. Even if there were no effect on casualties, the effect on continuity of service — reliability — is negative. Conceivably, again, some of these additional accidents could turn into serious ones because the platoon was in the process of formation. So the positive effect of platooning on safety, if indeed follower’s crashes are very rare, may be illusory. The effect on reliability may well be negative. However, in an automated system failure of the system which causes braking on a car is possible. Since it is important to maintain the capability of braking, there will be a tendency to bias the system towards “failing safe,” that is, with brakes full on. This will result in a follower’s crash.

A second reason why road vehicles are different from PRT arises from the need of platoons to form and dissipate. If they are formed at speed, there will be times when spacings of 5 - 50 m exist, and if a follower’s crash occurs at such a time a high-delta-V collision will result. It will depend on the mode of operation chosen how frequently conditions occur.

On the other hand, it may be that platooning has an operational advantage, in that it is easier for vehicles to enter the automated lanes if there are large gaps between platoons.

Within the PATH project, however, platooning has been generally assumed, and is the basis on which most research has been done. In spite of these doubts, therefore, it did not seem wrong to study the safety of platooned designs only — and indeed the topic has proved large enough for the resources available.

In all the following work, only platooned systems are considered. Steps are taken to ensure that if a platoon crush should occur, the vehicles can decelerate to rest without encountering another vehicle or solid obstruction. A *platoon crush* is the name given to a multi-vehicle accident in which several members of a platoon suffer a series of low-delta-V collisions and come to rest without a further high-delta-V collision. If a follower's crash occurs in a platoon, a platoon crush will normally follow.

Platoon crushes, it must be assumed, will occur. They cause property damage, and interrupt the service. They are to be avoided if possible. From the point of view of safety, however, the only important thing is to ensure that a platoon crush cannot lead on to a high-delta-V accident. In particular, things must be so arranged that only in very infrequent circumstances will another platoon run into the debris.

However, "very infrequent" is not the same thing as "never." "Low probability" is not the same thing as "zero probability." Automated freeways ought to be designed to be safer than existing ones, hopefully by orders of magnitude. But accidents will happen, and there will be deaths. In an automated, platooned system, one should expect that, as compared with a manually-controlled situation:

the number of accidents will decrease;
the numbers of vehicles involved in accidents will decrease;
the mean number of vehicles involved in an individual accident will increase.

Similarly,
the number of fatal accidents will decrease;
the number of fatalities will decrease;
the mean number of fatalities per fatal accident will increase.

More research is needed here. It will involve collecting new data — an activity expressly excluded from the terms of reference of the present work. This topic was not covered in the course of the present work, and will not be discussed further. In all that follows it is assumed that traffic on automated lanes is organized into platoons. Within-platoon collisions, including those arising while platoons are in formation or dispersion, are not considered.

2.4 System Architecture of an Automated Freeway

2.4.1 Architecture and Models

After the work described here had started, Varaiya and Shladover (1991) published a description of the system architecture of a particular type of automated freeway (one in which the bulk of the intelligence is vehicle-borne) in terms of five levels, each associated with a model of behaviour of the system or its components. Their purpose was to discuss volumes of information flow between the levels in the architecture, and make some deductions about communication system requirements.

However, the architecture is much more general than this. It seems likely to apply (with some reinterpretation and extension) to any well-designed automated freeway system. It does not matter whether there is one lane or many, vehicle-borne or infrastructure-borne intelligence, this model is valid. The architecture of the systems considered here will therefore be discussed in Varaiya and Shladover's language. The architecture is illustrated in Figure 2.1. A top layer has been added so it contains six levels or layers. Each level of the architecture is associated with a model which explains how the system reacts to the controls applied at that level.

Level 0, the *physical* level, describes how vehicular motions are affected by vehicle controls. The corresponding model will indicate how, for example, engine torque and vehicular speed react to changes in the angle of the throttle pedal. Within the infrastructure a physical-level model may indicate how a vehicle presence detector will deliver a signal when a vehicle is present.

Level 1, the *regulatory* level, includes vehicle-borne control systems. The corresponding model will describe, for example, how a vehicle is maintained in position in a platoon. On the infrastructure side, it could describe how the closing of one vehicle on another, as a platoon is formed, is monitored by interpreting the readings of vehicle position detectors.

Level *2,* the *platoon* level, concerns itself with the manoeuvres of platoons. These include formation and dissolution. Thus for example, the strategy for accomplishing journeys could require that a vehicle change lanes and join onto the rear of a platoon. The platoon level would then issue commands to both vehicle and platoon. The effect would be to induce an appropriate relative orientation. Then the moment to change lanes would arrive. Platoon level would check that no other vehicle had entered the space in the other lane. If the check failed the vehicle would not change lanes. This set of control actions might be entirely vehicle-borne. More likely the process would involve some interpretation of the behaviour of infrastructure-based equipment. It is likely that all equipment at platoon level would be local. One set of infrastructure equipment could control one to five miles of freeway. We shall call a length of freeway controlled by one set of platoon-level controls a *block*.

Level 3, the *link* level, is concerned with the organization of platoon formation, choice of lane, and choice of exit point, for all vehicles on a length of freeway. Its operation assists in the optimization of capacity. Clearly, since its operation affects many platoons, it is infrastructure-based, and probably remote from the roadside.

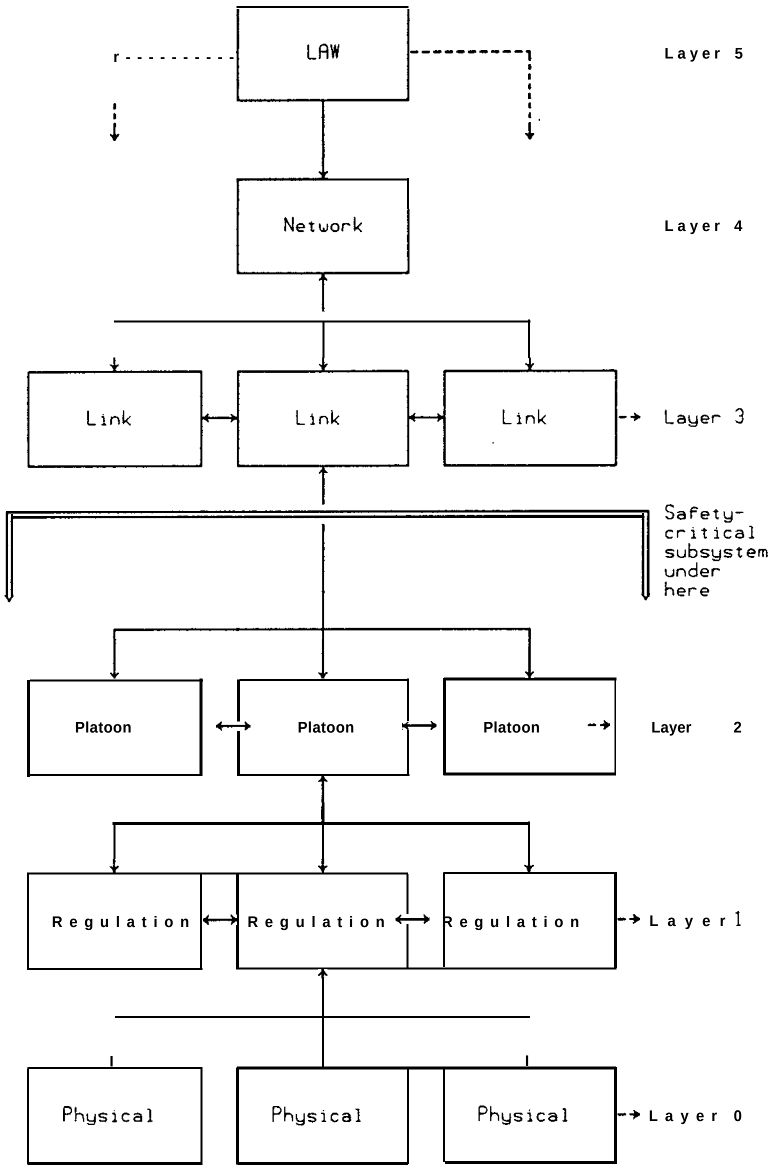

Figure 2.1. IVHS Control Architecture (after Varaiya and Shladover, 1991).

Level 4, the ***network*** level, incorporates any general route-choice control necessary to balance flows on different parts of the network. It will also be responsible to set parameters which determine speeds and spacings. Such parameters may be set manually or automatically. The parameters will depend on the weather, road surface conditions, and the like. The network level is centralized. There is one per conurbation.

Level 5 is ***law,*** covering many cities. Clearly automated freeways will require some regulation, and present highway law is irrelevant to many of their problems. It is not part of this research to predict legislative action or make recommendations about it, but some assumptions have been made. In particular it is assumed in the examples which are part of this research that the law will require:

(a) Vehicles using the automated lanes will require a special license, additional to the ordinary one, which will be capable of being interrogated by the system. Its presence certifies that the vehicle is equipped with a control system of approved design which has been inspected at some stated date.

(b) If a vehicle's control system develops a fault, the license can be so marked electronically, and the vehicle may be lawfully refused entry until the vehicle has been inspected.

(c) It will be an offence to fail to resume manual control when invited to do so.

(d) It will be an offence to enter the system while carrying an external load, or with a trailer which is not licensed and equipped with control and communication devices.

(e) It will be an offence to emit signals which represent falsehoods to the system (i.e., "hacking" is illegal).

The analyses do not assume that the law will always be obeyed. Failure to do so, however, counts as a system fault.

This is all we need to assume here. In addition there will have to be a considerable legal and institutional superstructure to all automated freeway systems. An automated freeway differs from other large systems with potential to generate catastrophe. It is not under one ownership. No one is responsible for the whole. Thus the phrase "of approved design" in (a) above implies a gamut of law and regulation; standards, guidelines, and standard-making bodies; inspection, approval and enforcement procedures; and more. All this will have to be thrashed out by all concerned to work in a way which is equitable. We shall return to this policy question in Section 4.

In Figure 2.1 the architecture ***also*** shows a ***safety-critical subsystem,*** and a modular structure. These are discussed below.

2.5 Nature of the Problem

No automated freeways currently exist. They do not closely resemble anything that does'exist. We want, for good reasons, to investigate how automated freeways would perform if they were designed. Performance, here, includes safety performance. Equally, we want to know how to design them to be as safe as possible, given other constraints.

Our task is therefore to find out how to design a complex system to be safe, when there is no closely relevant practical experience. The experience we do have means, however, that we know a good deal about the components from which the system could be assembled, and about their reliability and failure modes.

Such problems have arisen in the past whenever new systems or processes have been proposed. Analysis shows that there are three kinds of questions:

(a) What can go wrong? What would be the consequences of the various possible failures? How likely is each?

(b) How can the system be designed, or redesigned, so as to reduce these probabilities? By how much will they be reduced? How much would this cost?

Note. The word "cost" here is used in a generalized sense. Loss of system performance or capacity, increased delays, and reduced reliability are all costs in this sense.

(c) Is the gain in safety worth the increased cost?

Question (c) is a policy question. Perfect safety — zero accidents or zero deaths, ever, is not an achievable goal. If an automated freeway is ever built it will almost certainly have many fewer accidents, many fewer casualties, and much less property damage than present ones. But it seems likely now that the trade-offs will ensure that, if the system covers a whole state, there will be accidents every month, and casualties every year.

"Every dog is allowed one bite. " Historically, several types of solutions have been found to both questions (a) and (b) above. Long ago, safety engineering was carried out by a designer on the basis that he foresaw certain possible dangers as being obvious, and took obvious steps to avoid them. This is apparent from the design of the earliest steam engines, for example. The designers did appreciate that valves and joints could leak hot steam in jets. They provided baffles or casing around these vulnerable points which would deflect any leak likely to scald the operator, or some other person who was passing. They also knew that boilers could explode, and so provided relief valves.

Later, experience grew. Designers learned that relief valves had to be large enough to accommodate flow. Sometimes they would not open and a back-up was necessary. They learned that provisions should be made to allow them to lift periodically, so they were not cemented closed by rust or scale. And so on. Each advance in design and operational practice was achieved at the cost of substantial losses of output. All too often, it seems, deaths and injuries were part of the price of knowledge.

Later still, the concept of a checklist evolved. Typically this was a list of the ways in which particular kinds of industrial plants could fail, or had failed in the past. Codes of practice were drawn up. These identified design and operational practices which avoided hazards.

Codes of practice, in their turn, developed into standards, and the standards are often followed by designers and operators who have no knowledge of the original observations. Operators may not know why a particular practice is advised. This line of safety development is based on the idea that every accident type is to be allowed to happen once. After that, the experience can be cited, and there will be an addition to the code of practice.

A very good example of the results of this approach is found in the "Rule Book" developed by the railways in Britain. It started in 1830, with some observations about modes of operation in the presence of pedestrians. This followed the death of a prominent politician, Mr Huskisson. He did not appreciate how much faster a railway engine was at 25 mph, than a horse-drawn carriage. He stepped over the track to greet a constituent, and died beneath the wheels of Stephenson's "Rocket." Since then, there have been additions following each new kind of accident that occurred, and some others as designers appreciated new dangers without benefit of previous damage. Nothing has ever been removed. Rail people in Britain are deeply inculcated with this lore, and are reluctant to depart from these well-tried operational practices. Use of the Rule Book does indeed now lead to an enviable safety record, as well as to a great deal else which is less desirable.

Perhaps, if a similar California "IVHS Rule Book" were started now, IVHS would become very safe by the year 2150. This is not, however, the recommendation of the research described here.

2.6 Safety Criteria

In ordinary traffic, casualties are nearly always (90% +) associated with some kind of human error by a driver. On an automated freeway, the driver is not controlling anything, and any errors he/she makes will not affect safety. Any accident which occurs will be a result of one of these:

(a) One or more components has failed, and is not behaving in the way specified by the designer;
(b) The designer has made an error, and a situation has arisen in which proper operation of the system leads to a breach of the specification;
(c) The specification is in error, and actions which meet the letter of the specification fail to meet its intention — that casualties will not occur.

Further, on an automated freeway, vehicles move in platoons. Any accident which does occur can well involve whole platoons. These will not be like most crashes in ordinary traffic — they will involve many vehicles, and if the collisions involve large speed differences there will be many casualties. The safety problem on an ordinary road is to reduce the number of accidents. No one really believes that some day there will be none. On an automated freeway, the problem is to eliminate catastrophes.

2.6.1 Component Failure

We shall discuss (b) and (c) later. Here we are concerned with (a), single or multiple component failure.

In guidelines issued for the civil airlines, the policy is explicit in the Federal Aviation Regulations Section 25.1309 (b), (c) and (d) (FAA, 1988). Designs must be "fail-safe," that is "major failure conditions are improbable and [that] catastrophic failure conditions are extremely improbable." In demonstrations of compliance with the regulation:

"The following basic objectives pertaining to failure apply:

> "(1). In any system or subsystem, the failure of any single element, component or connection during any one flight (brake release through ground deceleration to stop) should be assumed, regardless of its probability. Such single failures should not prevent continued safe flight and landing, or significantly reduce the capability of the airplane or the ability of the crew to cope with the resulting failure conditions.
>
> "(2) Subsequent failures during the same flight, whether detected or latent, and combinations thereof, should also be assumed, unless their joint probability with the first is shown to be extremely improbable."

This suggests that what needs to be done is to consider every component, and then every pair, triplet, etc. of components and assume simultaneous or consecutive failure. Then one must demonstrate that, for every configuration or manoeuvre which the airplane may execute during a flight, either:

(a) safe flight may continue, or
(b) the combination is extremely improbable.

Even if it could be computerized, which is not currently possible, this process would take years, if not centuries. Moreover, every time there was a significant change in the configuration, one would have to do it all over again. The present point, however, is that "extremely improbable" does not mean and can never mean "never. " Any element can fail, and any combination is possible. Whatever "it" is, however unlikely it is, it can happen and it does. Airplanes do crash and passengers do die.

The research here therefore seeks (and finds) techniques by which the objectives of an analysis like that rejected above can be achieved at reasonable cost in time and money. Further, by introducing the concepts of a *safety-critical subsystem* and *modular design,* the techniques avoid the need to repeat the analysis every time a motor manufacturer introduces a new model (for instance). Incidentally, the same analysis can diagnose other kinds of difficulties. These include the avoidance of ways in which the system could tie itself into knots and become unnecessarily congested.

2.6.2 Tvpes of Safetv Criterion

However "fail-safe" a design is made, catastrophes cannot be made mathematically impossible. A lesser safety criterion must therefore be made express. In practice making the criterion more rigorous will incur a cost in system performance.

To make the trade-off between safety and capacity, it would be most useful to express the safety criterion in terms of casualties per vehicle-mile or per year. At the time this research started this was not possible. Some components of the system (vehicle control systems, communication, sensors) were totally unknown, and there could be no idea of their reliability. Instead, therefore, the criterion *no casualties without at least N independent faults at the same place and time* was chosen. Following current practice in aerospace and other industries, a value of N = 2 has been chosen for the examples in this research. That is, in the examples, *there must be at least three independentfaults in the same place and at the same time before a catastrophe can occur.* However, the techniques, in principle, allow for values of three, four, or larger numbers for N.

When design concepts for all the components have been realized, and the pattern of demand is known, this "number of faults" criterion can be developed into a "casualties per vehicle-mile" criterion. The former formulation does have the additional merit that it makes it possible to point to those components whose reliability is of greatest importance to safety.

2.7 Hazard and Operational Analysis

2.7.1 Hazards

What is proposed in this research is a logical process of design and subsequent verification which will ensure that the specified safety criteria are met, and that if changes to the design are made, the need for reverification is minimized.

The process is described in detail in the following paragraphs, which also discuss the need for organization which it implies. A brief overview of the process may be useful at this point. The process can be carried out at a conceptual stage, after everything is ready for production or at any intermediate stage. At any stage except the last, assumptions about what is still not ready must be made. These assumptions must be set down in a formal, rigorous manner. They act as a specification for later design.

(a) The first step is to define what it is that must be guarded against. Nothing is perfectly safe. We must specify what will be regarded as good enough. This is the *safety* ***criterion.*** It has been discussed above.

(b) Next, the situation must be analyzed so as to describe the situations which must be avoided. Here, this is done by specifying ***"hazards."*** A hazard is a situation where one further system failure can result in catastrophe.

(c) There is general guidance about other desired characteristics of the system (e.g. a system for end-to-end travel on a dedicated freeway, or multiple automated lanes on a freeway shared with ordinary traffic). One now sets out to specify a system completely, taking account of the need to avoid hazards within the specified criterion. Complete specification requires that what is specified is recorded in a standardized, totally rigorous manner. Care is taken to ensure that the design is ***modular,*** with communication between ***modules*** only at specified interfaces. Similar care is taken to identify the ***safety-critical subsystem.*** The safety critical-subsystem should not include anything that does not need to be there. We shall explain later more precisely what the italicized terms of art mean in this context.

(d) Considering each hazard in turn, a fault tree analysis is carried out to discover where the safety criteria are violated. If violations are absent, or the conditions under which they arise are rare enough to live with, the conclusions are documented in a formal, rigorous, manner. The task is complete until the next design stage is ready. Otherwise, one returns to step (c) above.

2.7.1.1 Design Error. Before proceeding, we shall consider the additional causes of catastrophe, (b) and (c) in 2.7.1 above; (b) concerns a possible error by a designer.

Designers, like everyone else, do make mistakes. They do have blind spots. So do system operators, maintenance managers, and all others whose actions can affect what the system is and what it does. Therefore, the same person should not be responsible for both design and verification. Indeed, the status of the two within the organization must'be parallel — it must not be possible for either to brush the other aside.

Further, great care needs to be taken that there is no possibility of misunderstanding between the two. The designer must specify his design precisely. Precision makes sure that the verifier does not miss the point. If nothing is assumed, the verifier cannot fall into the less obvious trap of making the same tacit false assumption as the designer. In the defense and avionics sectors, where teams are large, great emphasis is laid on formal recording and documentation (see RTCA, 1985).

In actual practice, the designer and the verifier are teams rather than individuals. Indeed for verification in particular it is very desirable that there be a multi-disciplinary team, so that the chance of a blind spot being a characteristic of one profession be avoided also. Kletz (1986) has described the appropriate organization of a verification team in the chemical industry. He calls the initial process a "HAZOP" for “Hazard and Operational Analysis. "

All this implies, incidentally, that the senior management must be committed to the concept of verification, that there are training programs, that the verification process is audited, and so on. The whole question of how these activities should be organized and managed is one which the IVHS sector will need to address at some time. Researchers can do little more than describe what is done in other industries (each one is a little different). They can also point out that there is a non-research problem which needs solution. This has been done here. These topics will not be discussed further. (For some suggestions arising from the petroleum industry, see API, 1990.)

2.7.1.2 Specification Error. This refers to (c) in 2.7.1 above. Just as the customer must specify a product and what it is to do, so must he/she specify what it is not to do. The verifier as well as the designer needs a requirement specification, and it needs to be precise. If it is not — and this is common — the designer or verifier will often see that something is missing, and ask. But, as is particularly apparent in the design of software systems, specification error can pass right through a design process.

In principle, formal procedures can do little here. They start from the specification. If what is specified is not what is wanted, some human insight is needed. In practice, however, this is not going to matter much in the case of automated freeways. Here casualties result only from some high-speed collisions. The hazard specification section below covers all reasons why high-speed collisions can occur. Therefore specification error is not important.

Or so it seems to the author. But we have just been arguing that blind spots can appear anywhere. In this work there have not been two multi-disciplinary teams, but just one person wearing a lot of different hats. If the author has a blind spot here, perhaps it is apparent to the reader. Please advise the author if this is the case.

2.7.1.3 Some Definitions. Statement of hazards will require some terms to be defined. If vehicles are in a platoon, it may, in cases of dire emergency, be desirable for each vehicle to brake to the maximum extent. This will be called ***full braking.*** Since brake efficiencies differ, full braking will normally be accompanied by intra-platoon collisions, with associated property damage. The maximum deceleration that can be achieved without loss of control of intra-platoon spacing will be called ***full platoon braking.*** Full platoon braking may well be around 0.3 g on dry roads.

For design purposes, a standardized version of the follower's crash (see Section 2.3) will be posited. In this, a vehicle follows another at a given speed, with constant spacing. Then, the leading vehicle decelerates, unheralded, at a rate to be chosen, say 1.0 g. The following vehicle, after some mechanical reaction interval (0.1 sec?), decelerates at full platoon braking, and comes to rest before it strikes the leader. This requires a separation between the vehicles, which depends on the speed. We call it ***platoon spacing.*** At high speeds it will be 100 m or more. Ordinary drivers habitually drive at closer spacings, and are comfortable at them. We shall define a minimum spacing at which drivers feel comfortable at a given speed, and call it ***manual spacing.*** It may correspond to a 1.5 sec headway — say 50 m at high speeds.

Vehicles will bear a forward-looking vehicle detection sensor. Its specification will be such that it will certainly detect (and measure distance from) a vehicle ahead of it, provided that vehicle is within the sensor ***range.*** The speed at which platoon spacing equals sensor range is called ***sensor-range speed.***

Some of these speeds and spacings will be affected by the weather. It is envisaged that they will vary from day to day and perhaps from place to place. They are parameters which can be set by the system operators at the network level.

2.7.1.4 Definition of Hazards. There must be some place on some lane in the system where vehicles are passed from manual to automatic control or the reverse. In this lane vehicles of both kinds must be present. If a vehicle is under manual control, no design of the automatic part can guard against all aberrations of a driver. All one can say is that accidents caused by errors of manual drivers, and resulting casualties, would have happened anyway, and are therefore not to be ascribed to automation.

There is another possibility. Some people may find ego gratification in trespassing onto an automated system, or even in tampering with it in some way. Also the possibility of a terrorist “hacker” cannot be disregarded. Clearly such activity should be illegal, and it may well be possible to design the system so that such people can be detected, and perhaps apprehended automatically so that the potential dangers they present are reduced. However, automatic law-enforcement — the rights and wrongs — is a big subject and it is not an objective here. It is therefore omitted from the hazards.

With these points out of the way, we can consider what can be guarded against. Collisions may occur:

(a) when all platoons involved (a solo vehicle is a one-member platoon) are under control, automated or manual; in this case vehicles were too close before a final control failure;

(b) when one platoon is not under control; this will happen if automatic control is switched off before the driver is ready, or not switched on when the driver lets go;

(c) when the final failure is a failure to brake or to communicate that brakes should be applied.

In case (a) above, we are only concerned when the rear platoon is under automatic control. In this case (remembering that a single vehicle is a one-member platoon), a further failure (viz the follower’s crash deceleration of the vehicle ahead) will cause a catastrophe if:

Hazard 1. A platoon is separated from one ahead of it, or from a stationary object in its path, by less than platoon spacing, or:

Hazard 2. A vehicle, not under system control is at an unmeasured or unknown distance in front of a platoon.

Case (b) above refers to the case where neither driver nor system is in fact controlling the vehicle, or where a driver is placed in a situation where he cannot control it.

Hazard 3. A vehicle is released to manual control before the driver has given a positive indication that he/she accepts it.

Hazard 4. A vehicle is released to manual control at less than manual spacing from the vehicle ahead of it; or at such a relative speed that manual spacing will be realized in less than 2 seconds; or while the brakes are being applied.

Danger may arise if a driver tries to surrender control before the system accepts it. But, as already explained, aberrations of manual drivers do not give rise to hazards.

Case (c) refers to what happens on one vehicle. Either by duplication or by some other kind of redundancy, vehicle brakes and their applicators must satisfy the safety criterion. Equally so must the communication system (the latter has implications for message protocols as well as equipment).

At present vehicle braking control systems have not reached the design concept stage. Neither have communication systems. The illustrative examples worked on in the research reported operated at a higher level in the system. In this position there is only one choice. The behaviour of these systems is posited to have the appropriate reliability.

Many repetitions of this statement will not add anything to the value of the work. Such repetition would detract from clarity. Therefore, although the relevant hazard is stated in this part of the report there is no need to refer to it later.

Hazard 5. A vehicle under automatic control is in such a condition that if instructed from the infrastructure to brake, it will not do so.

2.7.2 Initial Design Considerations

There are some features of the design process and some constraints on actual designs which follow at once from the definition of the hazards. Some arise from the fact that the safety criteria require that a hazard and operational analysis be made. Others are the consequence of the hazard specifications.

2.7.2.1 Modular Design and the Safety-Critical Subsystem. In any system, the behaviour of any part of the system can ultimately affect any other. If these interactions are disorganized, then a safety analysis must take account of the whole. For example, if a vehicle contains, as part of its control system, a feature which enables the driver to select a new track on the CD, or which will call his home on the cellular phone, it must be included in a safety analysis, because some malfunction of these devices might cause the brakes to be applied.

This is clearly undesirable. It will probably be fairly easy to arrange that some interlock or other design feature would prevent any such occurrence, but:

(a) The need to include interlocks (or whatever) of this kind would affect costs.

(b) The increased complexity of the safety analysis also adds to costs. More importantly it makes it more likely that something would be overlooked in the analysis.

(c) The analysis would have to be repeated every time some irrelevant feature of the design was changed.

To avoid these problems, two features of the design process are necessary. First a *safety-critical subsystem* (S-CS) must be defined. This includes all the parts of the automated system which affect vehicle manoeuvres. Steering, acceleration, braking, lane-changing, joining and quitting the system must all be included, along with the sensing and communication equipment; but this should be all. In particular, the link level in the architecture is excluded. This is important, for the link level determines capacity, and its exclusion from the S-CS means that it can be improved or replaced whenever a development is made. The S-CS should be designed as a set of interacting modules. Each should have a clearly-specified interface with other modules.

The interface defines what inputs the module can receive from other specified parts of the system, and what outputs it can pass to others. The terms "module," "interface," "input," and so on suggest software, but hardware components are also modules. A valve in a hydraulic braking system, for example, inputs torque from an actuator and outputs flow, or pressure, to brake pads. The point is that the valve cannot receive other inputs, or pass output to other places. If perhaps under fault conditions it can do so, this needs to be stated. One can imagine, for example, a poor design in which if another valve stuck open (a fault condition), the braking valve could cause pressure to be transmitted to a steering actuator. This would have to be foreseen and included in the interface specification.

Therefore in order to prove that the safety criteria are satisfied, it is sufficient to consider the S-CS only. The design must be modular, and each module must have specified interfaces, which detail all the ways in which each module can affect any other. The design process is therefore to design a series of modules, and specify their interfaces. Physical designs must conform to the specification, and in particular, even in fault conditions the interface specification must stand up.

If this is done, the task of verification becomes:

(a) to verify that everything that can directly affect the motion of a vehicle is included in the S-CS;

(b) to verify that the physical design corresponds to the specification of the safety-critical subsystem; and

(c) to use the module specifications as a basis for a fault tree analysis.

The link layer is outside the SC-S. Condition (a) therefore means that every action advised by the link level is checked up on by *(mediated through)* the platoon layer. For example, the link layer has to advise that a vehicle change lanes and join a platoon. The link controller is remote from the scene. It acts on the information available to it. The safety of the operation must be verified by the platoon layer. Some vehicle fault could mean that the vehicle would side-swipe if it tried to change lanes. The platoon layer checks its more detailed data. The platoon layer will not issue the control commands that the link layer advised if they lead to a hazard. We shall see in the examples (see Section 2.8) some ways in which this mediation may be achieved.

‘At the current conceptual level, (b) above is not relevant. One may question, outside the verification analysis, if the performance specified is achievable. In the absence of evidence, the question cannot be resolved.

2.7.2.2 Constraints on Physical Layout. For the remainder of this report, some limitations on what is being asked for will be assumed. They are:

(a) Only some lanes of any freeway will be automated; some lanes intended for ordinary traffic will be present too.

(b) Use of the automated lanes is not restricted to end-to-end travel. It is possible to join or leave in the middle.

(c) Lateral (steering) control is a feature of any automated system. It makes it possible for vehicles to travel at high speeds on lanes too narrow for manual use. Advantage will be taken of the substantial increase in capacity that narrow lanes offer. Thus it will not be possible for the fully automated lanes considered here to contain manual traffic, or vehicles other than cars. (Of course, there may also be truck-only or bus-only automated lanes. We shall not discuss them in any detail.)

The first of these seems reasonable for any freeway adapted for automation in the next 25 years. However, some have advocated end-to-end travel as an initial stage of automation. It is permissible to doubt if this would bring enough benefit to users to encourage the purchase of equipped automobiles. However, a report on safety is not the right place for discussion of this. If proposals of this kind are made, a safety analysis can be made by the methods described in the earlier part of this report. What is said in what follows may not apply to end-to-end designs.

Restriction to cars on narrow lanes may be more controversial. Again, if there are proposals to have mixed traffic, or if it is desired to introduce trucks or buses to automated lanes, the necessary safety analyses can be carried out by the methods stated here. In this case however, the author suspects very strongly that elementary considerations would show:

(a) If heavy vehicles are present in platoons with cars, the result quoted earlier from Shladover (1979), that low-relative-speed collisions can be tolerated, is not valid.

Shladover (1979) says as much. Automation on the lines considered here then becomes impossible.

(b) Manual traffic on the automated lanes violates the hazards.

Strong suspicion is not evidence, and the work required to justify these assertions has not been done. The safety argument referred to in (a) may be sufficient to justify the assumption without it.

A third assumption is implied by the use of platoons:

(c) A follower's crash (in which a leading vehicle decelerates, unheralded, more quickly than a following vehicle can brake) will occur from time to time if traffic is platooned. If it does, the vehicles behind the two in the platoon will also crash. Of itself, this causes no casualties.

What follows refers to the hazards 1 to 4 specified in Section 2.7.1 above.

To avoid hazard 1, objects not moving at traffic speeds must not enter an automated lane (AL). A crash will occur from time to time, on the *unconcerned lanes (ULs)*. ULs are the lanes on which ordinary traffic runs. (We shall call the lane between the ALs and the ULs the *transition lane* or *TL*.) After such a crash, debris or wrecks may move in an uncontrolled way and could finish up on an AL. This must not happen. Therefore the ALs must be separated from the TL by a barrier, which we shall name the *fence*.

Further, on an AL, a follower's crash will occur from time to time. Although there are no immediate casualties, the wreckage will be moving at high speed. Particularly if the road is curved, it is not reasonable to suppose that the wrecks will always stay in their original lane. Indeed the force of the crush may cause "snaking" — consider what happens if one pushes on a chain. If unconstrained, therefore, the crushed platoon will wander over the ALs until it strikes the central median barrier or the fence. In doing so it is quite likely to be struck by a platoon in another AL. The resulting high-relative-speed crashes will be followed by yet more when all the vehicles affected finally hit barriers at high speed. This is catastrophe, resulting inevitably from the simple chain of physical events following a follower's crash.

To avoid this there must be further fences between ALs, if there is more than one. They have to be strong enough and high enough to hold the crushed platoon which follows a follower's crash, and to prevent vehicles leaping it. It is apparent that this will be a good deal easier if the vehicles in the crushed platoon have only very little chance to depart from the regular line of travel. Safety is augmented and the cost of the fences reduced if the lanes are as narrow as possible. This provides a strong additional reason, if one is needed, for rejecting wide vehicles, and manually-controlled vehicles, on the ALs.

The fences cannot be continuous, for vehicles must get on and off. There must be gaps in the fence, for vehicles to join and leave. These will be called gates. Gates need to be some 80 m wide. At this length passengers will suffer lateral accelerations of 0.1 to 0.15 g in lane-changing. At a length of 80 m there is clearly a chance that a wreck from the UL can enter by the gate, or that a crushed platoon will protrude onto another lane. Something can be done here by ensuring that gates are only found on straight sections, so that crushes do not protrude because of curvature. But what remains must be regarded as a foreseen, and acceptable, hazard if it is decided to go ahead.

Decision here should depend on the frequency of serious crashes. Data are not yet available to compute it.

There may be a way out of this, by making the gates not mere gaps, but solid gates with moving parts. The only conceivable motion is vertical, though it is not clear that even this is possible. The gates would be heavy and would have to move quickly. Space for the driving mechanism may not be available. Even if there is space, high reliability cannot be expected with heavy moving parts. If a vehicle strikes an incompletely receded movable barrier, catastrophe will ensue. There will also be catastrophe if the barrier moves while a vehicle is crossing it, producing rollover. The cure is worse than the disease.

As a vehicle passes through a gate, there is a danger that it will be brought to rest by hitting edges of the gate itself. This will induce hazard 1, unless the gate is equipped with instruments which will warn an approaching platoon of the obstruction. Further the platoon must be separated from a lane-changing vehicle by platoon spacing. Having changed lanes, the vehicle must either have joined a platoon at once or have platoon spacing ahead of it. That is to say, a vehicle changing lanes must do so into a large gap, which is not always possible, or do so at the rear of a passing platoon.

This constraint applies also to vehicles joining the ALs. Therefore, a vehicle on the TL wishing to enter must be under automatic control when it does so. Equally, a vehicle must quit the system under automated control, so as to avoid hazards 3 and 4. Therefore the TL must have facilities to accept automated vehicles as well as those under manual control. There does not seem to be any way of excluding unequipped vehicles from the TL. However, drivers may find that driving on the TL, if not seeking entry to the ALs, is uncomfortable.

To avoid hazard 2, each automated vehicle must be a known distance from any manually-controlled vehicle which may be present. Both kinds will be present on the TL. It is possible that every automated vehicle will bear a sensor capable of detecting unequipped vehicles, and that the sensor range exceeds platoon spacing. If this is the case, the distance of any manually controlled vehicle is automatically known. Otherwise, there must be *vehicle presence detectors (VPDs)* up-stream of the on-gates and down-stream of the off-gates. These VPDs may also be of value in providing information to the link level, so that the link level can know where vehicles are for the purpose of organizing them into platoons.

TLs may not be continuous. If they are not, an automated vehicle cannot run on them indefinitely. To avoid Hazard 3, the last gate should then be an on-gate, so that a vehicle whose driver has (illegally!) failed to resume control can be readmitted to the AL. This is not applicable at the end of the line. Here a ***dormitory*** must be provided, where vehicles can be parked until their drivers resume manual control. It may be useful to provide dormitories at intermediate points also.

The hazards thus constrain the physical layout very considerably. There will be one or more ALs, separated by fences, from each other and from the TL. The fences contain gates to permit access. Vehicles pass through these under automatic control, always entering a wide gap or at the rear end of a platoon. Unless a long-range sensor is available, there must be vehicle presence detectors on the TL. At the downstream end of the system there must be a dormitory.

The presence of the fences and gates clearly limits the capacity — to what extent is not known. The limitation may be such that the economy of automated freeways is severely reduced. If this is the case, and it is still desired to proceed, the hazards must be relaxed. In this case some very careful thought about acceptable casualty levels is necessary.

2.7.3 Degraded Modes

In general terms, however, the design method for the S-CS is prescribed. The designer decides what he wants normal operation to be like. He also decides how the system will respond if things go wrong. One possibility would be simply to stop everything until whatever went wrong can be put right. If the fault is serious enough, this may be necessary, at least for some lanes or lengths of freeway. However, it may be possible to operate safely in some degraded mode, even if normal operation is liable to lead to hazards. Degraded modes are a matter of the designer's choice. If the normal speed exceeds sensor-range speed, then reducing speeds to sensor-range speed will ensure that vehicle control systems alone can prevent many hazards. To operate at sensor-range speed is therefore a natural choice for the first level of degraded mode. There seems little point in having another in which vehicles are moving. At the next level of degradation, therefore, all automatically controlled vehicles on an AL should be stationary.

Even with long-range sensors, it seems sensible, if there are reasons for unease, to reduce speed. One reduced speed that might be chosen is the ***same-capacity speed.*** For the patterns of platoon sizes likely to be encountered, the capacity of a lane in platoons/hour depends on speed, and passes through a maximum at somewhere around 50 mph. Normal speeds will be above this, so there is a minimum reduced speed at which full capacity can be maintained. This could be a good choice for the speed in a degraded mode.

2.7.3.1 Access to and from Degmded Sections. There are a few additional points. If a block on one AL is stopped, the traffic on the upstream block will need to quit the lane before it gets to the stopping point. Since there is likely to be a line at the gates, the whole lane should be degraded to operate at reduced speed, for one or two blocks upstream of the stopped one. In order to facilitate their exit, it may be useful to operate the adjacent lanes at reduced speed also. This illustrates the two alternative reduced-speed degraded modes. In one degraded mode the traffic must leave at the end of the block. In the other it may continue, and very likely accelerate to full speed again after it has left the block. We shall refer to ***speed-reduced exit*** mode (SRX) and ***speed-reduced-continue*** (SRC) mode.

Equally there are two kinds of behaviour that may be required when a lane is stopped. Usually platoons will brake to rest at full platoon braking. There will be no in-platoon collisions to damage vehicles. Occasionally, however, an obstruction will be detected at such a distance that full platoon braking will lead to a collision with a stationary obstacle — perhaps accident debris from the ULs which has passed through a gate. If this happens, it will be better for any platoon just upstream of the obstacle to sacrifice vehicle damage in favour of reducing speed before a collision in which people might be hurt. We shall refer to ***stop*** mode and ***crashstop*** mode.

2.7.3.2 Operation in Emergencies. If there is a crash, operations should be under human control. Delicate judgments are necessary, and the system does not have data on which to make them. The first actions must be automatic. The relevant lane (for one block) enters stop mode directly or after crashstop. After that, a Highway Patrol person, on the spot or by remote television, will advise the system supervisors of the operations that are needed. These might include permitting access by emergency vehicles along the length of the stopped lane in either direction or transversely from an adjacent one. Undamaged vehicles, trapped by an incident between fences will wish to proceed on their way and will need to move, perhaps in reverse, to do so.

All this points to the need for vehicle control systems to have some special features, including certainly the ability to back up, in lane, under automatic control. This topic needs more research.

After an incident is over, reduced-speed or stop, normal operation will be resumed. This too, will require special control features, and again, will probably be done by the automatic system under close human supervision. This area too needs research.

2.7.4 Design Process

In the preceding section, we were able to reach definite conclusions about the physical layout based on the hazard definitions only. To go further, choices must be made. The choices will be constrained by the performance of such subsystems as vehicle control systems, sensors and communication. The designer will tend to make prejudgments. For example some people may want to show off by entering the system without automatic controls. This is dangerous. If the designer thinks this is very important he/she will choose accordingly. (Perhaps surprisingly, this is more basic than it may seem.) Choices will also affect the balance between investment in vehicles and in infrastructure.

In fact it seems probable that there are fewer big choices than appears at first. The hazards do not constrain the rest of the design as straitly as they do the physical layout, but they do constrain choice to a considerable extent.

2.7.4.1 Design for Verification of Safety. The important requirements for the performance specification of the safety-critical subsystem are:

(a) Nothing outside the S-CS can affect vehicle motions without being mediated through the S-CS.

(b) The specification is consistent with the kind of system wanted.

(c) The specification is complete, that is to say, it is possible to deduce what will occur next in any situation that can be achieved.

One way of achieving these results is as follows:

(1) Decide on the behaviour of system and vehicles that will be expected under normal conditions. Start to specify this beginning at some logical point (e.g., when a vehicle requests entry) and proceed to the end.

(2) Express events which must occur as the effect of the actions of a series of modules. Specify each module fully. One class of events here is manoeuvres such as a vehicle joining a platoon. The other is the periods of staying in relative position within a platoon or behind a leading platoon.

(3) Ask, as each manoeuvre is specified, "What must happen for this to meet the safety criterion? How is it known that it does?" If it is not known, a new procedure needs to be added in the form of one or more additional modules. Specify these fully. Then ask "What will happen if the information indicates that the manoeuvre does not meet the criterion? Will the system know if the manoeuvre is not

completed? What will happen then?" If the specification does not already imply the appropriate actions, specify a new procedure fully (i.e. add more modules).

(4) Ask, in each period of maintenance of position, "What will happen if a vehicle or system component fails at this point? Will the failure become known? Do following events meet the safety criterion?" If they do not, specify a new procedure.

These steps involve specifying modules. A standardized way of doing this is desirable because it helps to ensure that nothing is omitted.

2.7.4.2 ***Formal Specification of Modules.*** At some time in the future, it may become possible to demonstrate conformity to specification by mechanical application of mathematical logic. Indeed, one example of application of such a technique to a design of an automated freeway already exists (Hsu, et al., 1991). Examples also exist of computer languages which may contribute to verification and validation. They all contain ways of specifying modules.

These ways were used as guides in drawing up the form of a complete specification of a module used in this work. As has been seen, part of this specification must be a specification of the interface. This is a complete statement of inputs and outputs of the module, including origins and destinations. In some cases the only input will be the invoking of the module, so the input specification should include the name of the invoking module. In addition, the specification must contain a statement of what the module does. A module may contain a branch, so that its output is affected in kind by what happens internally. The branching condition is an important part of the description. Also a module may only be functional in certain conditions, e.g., while a vehicle is exiting, or while it is operating in a degraded mode.

The whole specification is easier to understand if it is also represented as a flow diagram, showing the relation between the modules. Cross-references are needed. Thus a form for a module specification was derived. It contained the following headings:

Module Name
Modes in which operable
Input: origin and content
Branch condition (or nil)

Flow Diagram Reference
Modes in which passive
Invoking module(s)
Action

This listing is similar in form to a module specification used in predicate-logic computer codes. However, no corresponding axiom-based language exists in this case.

2.7.4.3 ***Completion of Specification.*** If the procedure described in Section 2.7.4 above is carried out in full, and nothing is overlooked, the specification of the totality of modules must be complete. Further the use of a standard form helps to ensure that each module is also fully specified. In particular each module's interface with every other module is defined with formal rigour. As explained in Section 2.6, the specification is now ready for fault tree analysis.

A full specification must be produced and fault trees must be generated at several stages in the design process. Just when and how often is a matter for management decision. All the authorities are agreed, however, that it is important that the first analysis be carried out at the conceptual design stage. Thereafter, in many cases, subsystem requirement specifications will be produced, and different subsystems will be designed by different teams. Different subsystems may well require different procedures or be developed in companies with different customs. In particular, the verification of software and hardware may be carried out in different ways at different times.

The final full specification will be followed by a final verification and validation. At this point it will be necessary to rely to a considerable degree on what has gone before. In particular, if a subsystem has been fully specified, and a verification team has certified that what is produced conforms to that specification, it is unlikely that the matter will be examined further. Of course, it can happen, and sometimes does, that at this final stage it is realized that the subsystem specification is faulty. Certainly the final fault tree, working with the system at some degree of aggregation, will be intended to detect such a mistake.

2.7.5 Fault Tree Analysis

It has already been pointed out that it is not practical to demonstrate that a design meets the safety criterion by considering each fault, and each combination of faults, in turn (see Section 2.6). It is necessary to know how a component can fail, and how it will behave if it does. To this extent, some consideration of the failure modes of each component is desirable. When a component has been designed as hardware, it could well be appropriate to use some formal method for this, such as a Failure Modes and Effects Analysis.

Most faults and most combinations of them do not lead to a problem, but there are a very great number of combinations. To pursue a forward failure-effect analysis up to full system level is not practical, for it would take many centuries. In this research, therefore, the use of a fault tree analysis is investigated.

A fault tree analysis argues backwards, from effect to cause, within the limited universe totally defined by the full specification. We start with one of the hazards. Then we ask "How could this happen?" The answer is normally that it could happen in a number of ways. The first answer will normally classify the possible causes in terms of different times, places, vehicle movements, or something similar. Then, for each possible situation revealed by an answer, we ask again “How could this happen?” and so on, until one of the following happens.

(a) We realize that “this” could happen. In this case the safety criterion has been violated, and we have found a design error.

(b) It turns out that there is just no situation in which “this” could happen. We record ‘as much, and go on to the next branch of the tree.

(c) “This” ***could*** happen. In order for it to do so, however, there would have to be a combination of unlikely events that is not excluded by the safety criterion (e.g. four unrelated, simultaneous, failures of components). Again, we record the conclusion and proceed to the next branch.

It may seem initially that this would be just as complicated and lengthy as arguing forwards. But in practice it has been found that after a very few steps, all the branches of a tree terminate. The process is in practice one which does work. Further, although it cannot guarantee to find incompleteness in the specification, it nevertheless often does.

In this research we are seeking an effective method of design and verification. One is now proposed. To show that it is effective we must show:

(a) that it is possible to construct a full specification of a design in the way described here;

(b) that, in practice, fault trees terminate quickly;

(c) that fault trees do detect design errors in practice.

The demonstration has been made by taking examples. In the two cases considered, the design technique worked at the conceptual level. That is to say, it has proved possible to specify S-CSs of two systems, as concepts, on the basis that such subsystems as vehicle control systems can be designed. (Such subsystems are the subjects of parallel projects in PATH.) Fault tree analyses were applied to these systems. They were completed in a reasonably short time. The fault trees did detect some errors.

It is reasonable to conclude that the design, verification and validation processes described here are effective and practical in arriving at system designs which conform to the safety criterion.

2.8 Examples of System Design, Verification, and Validation

2.8.1 Origins of the Examples

The previous parts of this section present a body of theoretical argument and some experience from other sectors. They have led to a detailed prescription for a design, verification, and validation process for automated freeways. Some observations of the way the whole process should be managed have also been made.

Theoretical argument is all very well. It is necessary to verify its predictions in practice. That is to say we should present examples of these processes which have been carried out successfully. One way to do this would have been to start with a conceptual design, externally developed. It should have been specified in concept. Then we could have given an example in which full specifications, in modular form, of its S-CS were developed. Later a fault tree analysis would have been carried out.

This was not possible in mid-1990, the time the work started. Little thought had been given to the way vehicles might join or quit an automated freeway. No consideration had been given to fault conditions, component failures or degraded modes. Therefore it was necessary to create a complete specification of an automated freeway with very little in the way of a lead.

Work on Example I, as described below in Section 2.8.1, was therefore started. While this work was in progress Hsu and her colleagues were engaged on a partial specification of a very different system (Hsu, et al., 1991). Example I is characterized by only one AL and has intelligence concentrated in the infrastructure. The Hsu system had many ALs and mainly vehicle-borne intelligence.

Hsu and her colleagues' concern was to demonstrate completeness of her partial specification by logical means. The desirability of doing this for a full system has been appreciated in the present work. However the completeness of a full system has not been demonstrated. The method used by Hsu, et al. will not achieve this without more development.

It had always been intended to present two examples of systems in the present work. They were to be very different. When Hsu's work appeared, therefore, permission was sought, and granted, to use this work as a basis for Example II. Considerable further development was necessary, besides writing formal specifications of the modules. The original specification involved only normal, fault-free operating conditions. It contained no provisions for entry to the system or exit from it. Nor did it conform to the physical layout shown in Section 2.7.2 to be required. There were no fences or gates. A great deal therefore had to be added to Hsu's original concept to form Example II.

2.8.2 Management Aspects

Both the specifications and the fault trees in the examples are therefore largely the work of the current author. Earlier in this work it has been explained that work of this kind should be carried out by two multi-disciplinary teams, separately managed, and communicating by defined procedures. In this case this has not been possible. The recommendation about two teams, however, applies to cases where the process is intended to result in a real freeway. On such a freeway flesh-and-blood people would ride, and, hopefully, keep their flesh and blood to themselves. There is no intention to build systems based on the two examples. The examples demonstrate the technique and its feasibility. The lack of independence of designer and verifier does not affect the demonstration.

However, they do not demonstrate the management process. The examples do show that the recommendations about complete specification and fault tree analysis are practical. They say nothing about the comments on the way the processes may be managed.

2.8.3 Example I

The first example of a system specification for an automated freeway will now be described. A brief general account is given here. The approach here is to describe small parts of the work as examples. The reader is asked to perceive how such examples could be repeatedly applied to produce a whole. Two other reports present the design (Hitchcock, 1991c) and the fault tree analysis (Hitchcock, 1991d) in full detail, including full specification of every module in the standard form described in Section 2.7.4. These reports are written as reports standing on their own. They should also be regarded, however, as appendixes to this one. Much detail is omitted in what follows, but this detail is to be found in the reports cited. We forbear from boring reiteration of the reference.

At the time this example was produced there were few ideas of what a design should look like. There had been no systematic work, for example, on how vehicles would join or leave platoons. Thus, it was not certain that an automated freeway which met safety criteria was possible.

In drawing up the specification of this example the prime objective is simply to produce a complete specification. The purpose of the whole project is to demonstrate the method of full specification and fault tree analysis as applied to an automated freeway.

As explained in Section 2.7.2, it is only necessary to specify the safety-critical subsystem and its interfaces. This means that we must specify the platoon, regulatory and physical levels of the architecture (see Section 2.4). Interfaces with the link level must also be specified. For the reasons explained in Section 2.6, a safety criterion "No hazard without two independent failures" was taken. The hazards are the hazards 1 through 5 in Section 2.7.1.

The fault tree analysis might show that the example specification satisfied the safety criterion. More probably, since only one iteration was intended, it might show that the specification could be modified so that it did satisfy the criterion. It was also possible that it might appear that the design was on the wrong lines and it might then appear that no simple modification would enable the design to satisfy the criterion.

It was decided that the third outcome should be avoided if possible. It was desirable to show that there were "safe" automated freeway designs, even if one had to lean over backwards to produce them.

2.8.3.1 ***Initial Considerations.*** It was decided to consider a single automated lane (AL) on a freeway which also admitted manually-controlled vehicles. The automated lane would be the leftmost one. Vehicles would enter the freeway via existing on-ramps, and make their way to the TL (transition lane — see Section 2.7.2). The TL would be the next to leftmost. It would be open to all traffic.

At the start, the following seemed important to the designer:

(a) The responsibility for vehicle maintenance, and therefore for vehicle control system maintenance was the vehicle owner's. Not all owners could be relied on to discharge this properly. Further, "hacking" would be possible, though illegal. It would be possible to falsify vehicle signals so that a vehicle appeared to be properly equipped and properly maintained when it was not. Some people would find ego-gratification or economic benefit in hacking.

(b) There would be a great deal of communication. It might be between vehicles, between vehicles and the roadside, or between different roadside controllers. The last could be hard-wired, and would not interfere with other communication traffic. Interference between the others was possible. By means of suitable protocols it would be possible to avoid a transmission being misinterpreted by the intended recipient because it was garbled. By identifying the intended recipient of a transmission, the possibility that it would be acted on by the wrong entity could readily be avoided. But interference due to noise would be a real problem, and needed to be avoided by having only short-range transmissions, and also by adopting a strict sequencing discipline.

(c) Roadside components would be under public control. This would not guarantee good maintenance but would make it possible, compared with the certainty that at least a few vehicles would be ill maintained. Therefore roadside components should determine whether each manoeuvre demanded has in fact occurred. As explained in Section 2.7.4, the design method requires that, if it has not, suitable alternative action should be specified also.

Consideration (a) pointed to an emphasis on infrastructure-based intelligence. In turn this implied a good deal of vehicle-roadside communication. This could be very short-range (as required by (b) above) if roadside transmitters and receivers were replicated or otherwise extended along the road. Leaky coaxial cables, as used for radio communication in rail tunnels, might achieve this. However, the way in which concepts are instantiated is not important here. Direct vehicle-to-vehicle communication over a longer range would not now be necessary. Information could be passed via the roadside, thus eliminating one source of noise.

With hindsight, the reader may feel that these considerations were the best ones to start with. However they are the ones that were in fact present. What is being explained here is why this example was chosen. The considerations above are not shown to apply to all possible designs. It is just that we have to start somewhere, and the place may as well be one that has some built-in safety.

2.8.3.2 Physical Layout. The constraints on physical layout have been discussed above in Section 2.7.2. The design selected is shown in Figure 2.2. It will be noted that, as already explained, the AL is separated from the TL and the rest of the freeway by a fence. Gates in the fence permit entry and exit. They are grouped into LONRs and LOFRs. Automated vehicles may move on both AL and TL. Both must be equipped with a lateral guidance reference. It is not assumed that this reference is continuous on the TL. The instrumented part of the TL in each block stretches from some way (half a mile?) upstream of the first gate to just below the last gate, which is an on-gate. Vehicles are not under automatic control on the TL outside this length.

Vehicles enter the freeway by the existing on-ramps, and make their way to the TL. The TL is therefore next to leftmost and is open to all traffic. An equipped vehicle wishing to join the AL would say so, and indicate its intended exit point. Then it would enter the AL under system control.

The AL is fenced off, so entry would be through a gate in the fence. It was envisaged that a set of on-gates, called a logical on-ramp (LONR), would be sited at suitable points along the AL, and be associated with a similar set of off-gates forming a logical off-ramp (LOFR). There need be no one-to-one correspondence between LONRs and physical on-ramps. It made sense to say that each block would contain one LONR and one LOFR and that the block boundary would be immediately downstream of the last gate. (A block is defined in Section 2.4 as the length of freeway controlled by one set of local platoon-level controllers.) If there were left exits from the freeway some additional structures would be necessary. Otherwise, the system is seen as needing no extra road space.

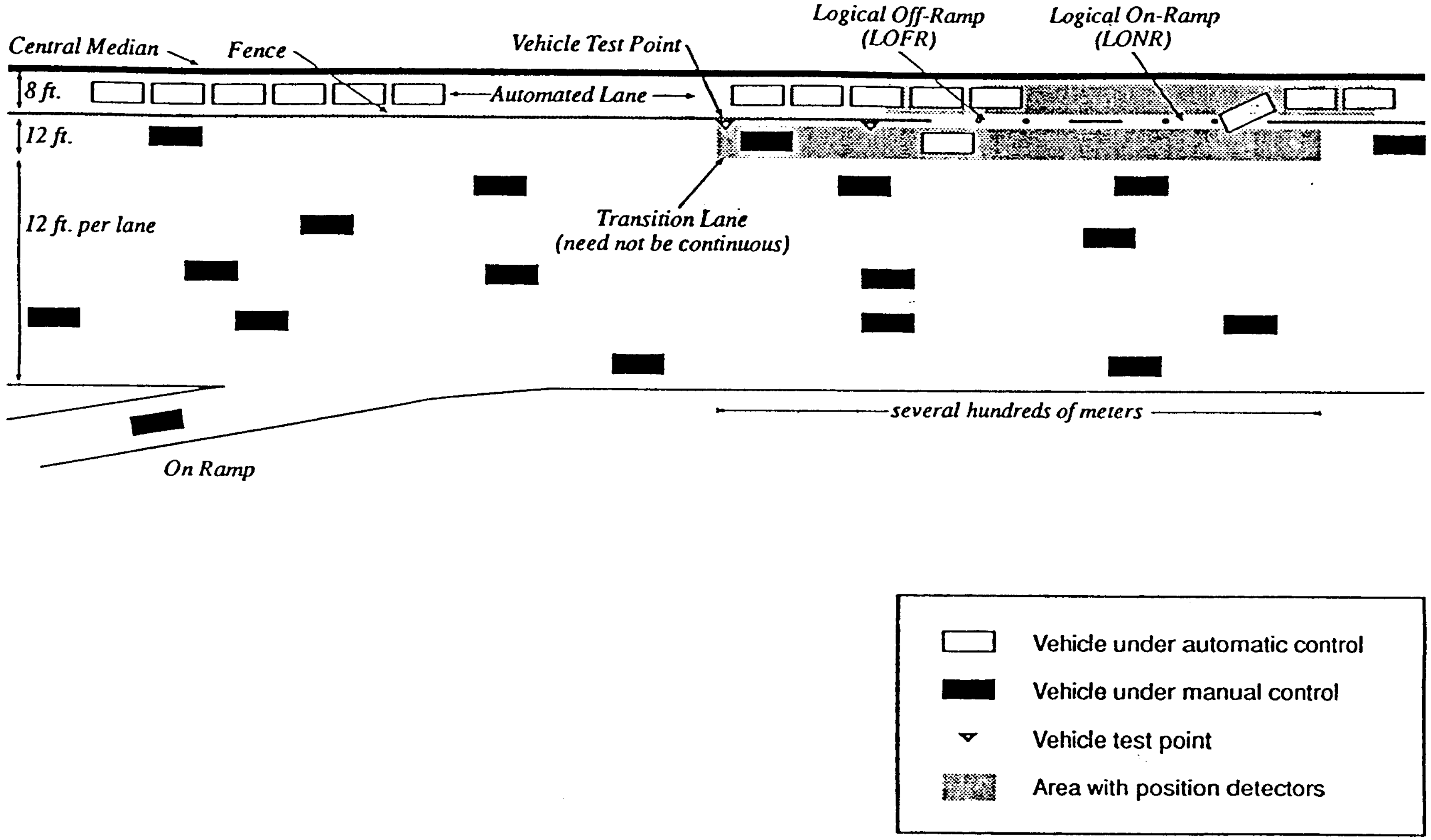
Central Median
Fence
Vehicle Test Point
Logical Off-Ramp (LOFR)
Logical On-Ramp (LONR)
8 ft.
Automated Lane
12 ft.
12 ft. per lane
Transition Lane (need not be continuous)
several hundreds of meters
On Ramp
Vehicle under automatic control
Vehicle under manual control
Vehicle test point
Area with position detectors

Figure 2.2. Layout of One-Automated-Lane Freeway.

This is clearly a type of installation which could be of interest early on in the introduction of automated freeways. There are lots of other choices which could have been made instead. This is no worse than any of them.

It is not assumed in this case that the vehicle-borne forward-looking sensors have very long ranges. It is explained in Section 2.7.2 that in this case ***vehicle presence detectors*** **(VPDs)** must be provided in places where there may be both manually-controlled and automated vehicles present. **VPDs,** therefore, cover the TL. In this case there are also **VPDs** on the AL upstream of gates.

Figure 2.2 also shows three other features. On the lateral guidance references, associated with each gate, there is a ***turning point.*** This is a special reference marker, which indicates to a vehicle which needs to change lanes that the manoeuvre should start. It is important that motion through the gates be the same for every vehicle. Otherwise, a vehicle might strike the fence instead of passing the gate.

Next, at the upstream end of the TL, and probably also at other points, there is an ***identifier.*** Here a vehicle wishing to enter identifies itself. The vehicle represents that it is equipped, licensed, and in good working order and also indicates its intended destination. In accordance with the general approach, the system verifies these data, which are relevant to safety. At the reverse ***turn,*** a little later, a vehicle is instructed to accelerate, decelerate and move to left and right. The responses are tracked. Apparent external dimensions are also checked and compared with those stored in the vehicle. If they do not agree, then the vehicle has an illegal external load, and is barred. If the vehicle's responses are satisfactory, the vehicle is cleared for entry to the AL. The movements need not be large. Passengers will not be discommoded. The lateral accelerations at the reverse turn will be much less than those at the reverse turns on Grand Prix racing circuits.

2.8.3.3 Architecture, Level 0 — Physical Components. The physical level of the architecture describes how vehicles respond to movements of the throttle pedal, the steering axle and the brakes. In the roadside aspect it describes how a vehicle affects the **VPDs.**

2.8.3.4 Architecture, Level 1 — ***Regulatory*** *Components.* This level controls and monitors the movement of individual vehicles. On-vehicle components are:

(a) A ***vehicle-borne state vector (VSV).*** This is a software record held physically in an ***asynchronous record (AR).***

An asynchronous record is a computer-controlled store which can be read from and written to by other computers and communication equipment. The accessing messages do not have to be in sync with the computer which controls the AR. Nor do they have to be in sync with one another.

The VSV is part of the method by which data are transferred from the roadside to the vehicle. Roadside parameters can be written by the communication equipment to appropriate fields of the VSV. Subsequently they can be read by the vehicle-borne control systems. Or it can work the other way around. Vehicle controllers thus do not have to be synchronized with the roadside controllers.

The content of the VSV refers partly to the vehicle itself — its identity, date of its license, external dimensions, etc. The VSV also stores data relating to the current position, including both longer-term data, such as the destination, and ephemeral control data for immediate use.

(b) Longitudinal control system. This maintains position in platoon. If a vehicle leads a platoon, there is a target speed stored in the VSV which the control system usually has to maintain. However the control system also has a parameter set externally to the VSV, a maximum speed, which must not exceeded. This is called the ***maxspeed.***

(c) Lateral control system. This keeps the vehicle on track in lane. When appropriately stimulated it causes change of lane at a turning point.

(d) Communication equipment. This is for sending and receiving messages from the roadside. Most messages refer to the identity of the vehicle affected, and will be ignored by other vehicles. A few are general and meant to apply to all vehicles in a block.

(e) A self-monitor, which checks that the other systems are working and warns of faults if they are not.

On the roadside, the regulatory layer contains:

(a) One ***roadside state vector*** *(RSV)* for each vehicle. Again these are contained in ARs. One computer can control all the ARs for a block. The RSV contains similar information to the VSV, but it also contains the data about the vehicle's position and speed derived from analysis of the responses of the VPDs. Data about possible vehicle faults is also held. For example, if a vehicle fails to respond to one routine message, it would be wrong to exclude it — perhaps the line of transmission was intercepted by mud from another vehicle. If it fails repeatedly, it should be treated as faulty. The RSV contains a count of consecutive failures.

Manually-controlled vehicles on the TL also have RSVs allotted to them.

The RSVs serve as a means of communication between different controllers in one block, between controllers in different blocks and between controllers at different levels in the architecture. However, levels outside the S-CS have read-only access, with one exception. Target speed is written to the RSV by the link level.

(b) A VPD controller which analyzes the data obtained from the VPDs and converts it into speed, position, and other data. These are recorded on the RSVs.

(c) One or more vehicle controller which systematically works upstream through the ' vehicles in a block. Vehicle controllers receive information from vehicles about speed, lateral displacement, contact with the vehicle ahead, and so on, some of which is passed to RSVs. Vehicle controllers also transmit information from the RSV to the VSV. Data about a platoon leader, needed for platoon control, are passed from and to the relevant vehicles by this route. Vehicle controllers pass messages to platoon level if a fault count gets too high.

(d) Associated with each gate are ***gate bits.*** These are single-bit ARs, set by the VPD controller. If the bit is set, the gate is within platoon spacing of the nearest vehicle upstream of the exit side of the gate. Passage through the gate should therefore be denied.

Both VPD controller and vehicle controllers ***are iterators.*** They carry out the same analytic process on one vehicle after another (or one VPD after another). When they get to the end of the block they start again. (Some sums suggest that, within present technology, this implies that each vehicle will be addressed about every 100 milliseconds.) Maxspeed is communicated by these vehicle controllers via RSV and VSV to the vehicle. Changes in maxspeed are also sent directly to a separate AR in the vehicle by the platoon level, using a different vehicle-borne receiver. If only one of these is received, the self-monitor will indicate a fault and the vehicle will not be permitted to enter the system again. Thus there must be two faults before a maxspeed change is not acted on. In this way, conflict with Hazard 5 (see Section 2.7.1) is avoided.

2.8.3.5 Architecture, Level 2 — Platoon Components. These components are one or more roadside controller and corresponding vehicle-borne controllers. The roadside controllers communicate with vehicles directly to the vehicle-borne platoon level. Roadside controllers also communicate with the regulatory level in vehicles via the RSV-VSV link. The roadside controllers receive suggestions from link control that a vehicle should join or quit a platoon, change lane, or carry out some other manoeuvre. The roadside controllers also use the data on the RSVs to discover if a vehicle is too close to the one ahead or if a vehicle is displaying faults.

In response, a roadside controller will check whether the situation revealed by its input is acceptable or not. If the situation is acceptable, safety criteria will not be violated. Then, instructions will be issued to commence the manoeuvre, or to continue as before. If the rules in its programming indicate that safety criteria will be violated, the roadside controller will correct the situation. The roadside controller may do this by failing to implement a new manoeuvre, or by devising a different new manoeuvre. Often the only action will be the issue of a new maxspeed. A new maxspeed will be communicated to the vehicle directly and via the regulatory level RSV-VSV link.

The vehicle-borne controllers at platoon level mostly oversee lane changes. Other operations, like joining a platoon, can be accomplished at regulatory level by changes in target speed and maxspeed. In such manoeuvres the vehicle-borne controllers receive messages from the roadside. They react by writing temporary data to the VSV which modifies the objectives of the regulatory level. When the manoeuvre is complete, the old data are restored.

Much of the description which follows is concerned with these messages. They, and the modules they call, have been given mnemonic names, which helped to ease the designer's task. The message, for example, which calls a platoon member to enter the AL is called Comeinp. On receiving it, the vehicle platoon-level controller causes the lateral controller to change its objective, and to change lane when the turning-point marker is detected.

2.8.3.6 Architecture, Level 3 - Link Components. Link level lies outside the S-CS. Its interfaces with the lower levels must not, therefore, directly affect vehicle motion. Nevertheless, the influence of link level on the economy of operation is profound. Link level sets target speeds for platoons and single vehicles. Link level indicates to platoon level that a platoon should be formed or dispersed. The objective is to meet as many of the demands for travel from entry to stated destination as possible. Thus link level determines, and maximizes, system capacity.

Link level contains a single controller, centralized in a district. Each link-level controller is associated with many platoon-level ones. The operation of link level is, as has been seen, mediated by the lower levels. It does write target speeds directly to the RSVs. But target speed is subordinate to maxspeed, set by platoon level. Similarly the link level may indicate that a platoon should enter the AL. This operation, however, is controlled by the platoon level. The platoon will enter only if the platoon-level's check of the gate bit reveals no potential hazard.

2.8.3.7 Normal Operation. As explained above, the design process starts by specifying normal operation. Normal operation will not be formally specified here: it will be described only. We shall consider the progress of a vehicle from origin on freeway under manual control to resumption of manual control near the off-ramp. Figure 2.3 illustrates this progress.

Initially a driver enters the freeway in the usual way. As soon as he/she enters the part of the TL where there are VPDs the system notes the vehicle's position and speed. These may become relevant to the movement of automatically controlled vehicles. For instance, the vehicle may have entered between two which were in the process of joining

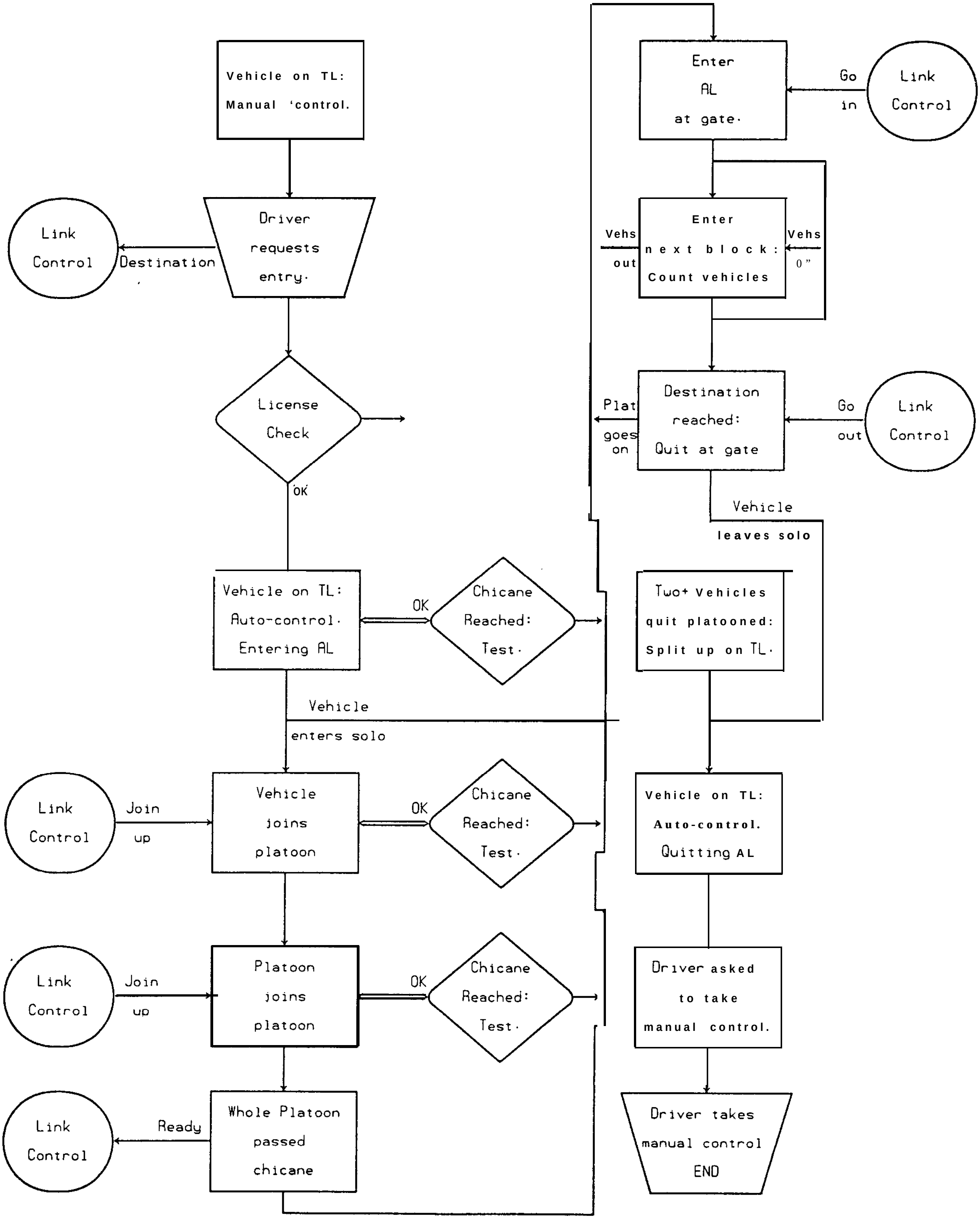

Figure 2.3. Progress of Vehicle in Normal Operation.

to make a platoon. In due course an identifier is reached. The driver has instructed the vehicle to join the automated system. A destination has been identified. At the identifier, a message is sent, and after checks to the license, automatic control takes over. Action by the driver on steering wheel, throttle or brake pedal will now have no effect. At this point the driver is permitted to have a change of mind. However, the effect of this is not to restore manual control at once. The vehicle will be treated in the same way as one which has just left the AL.

The choice of whether or not platoons may be formed on the TL is one of the major decisions which shape the design. Here we permit pre-formation of platoons on the TL. This has these advantages:

(a) Pre-formation probably increases capacity by allowing several vehicles to join the AL at once.

(b) If desired, platoon formation can take place at reduced speeds. This diminishes the magnitude of the injurious forces which would arise if a follower's crash occurred before the platoon was complete.

The disadvantages are:

(c) The number of vehicles is increased, which are affected if debris from an accident on the other lanes intrudes onto the TL.

(d) The lane-change manoeuvre through a gate may be made more complex.

After entry to the system, but while still on the TL, a vehicle may be invited to join a platoon. Another possibility is that an existing platoon is invited to join onto the vehicle. A third is that, having joined a platoon, the platoon joins another. Alternatively, the vehicle may first come to a reverse turn, where its control system is tested. Since we are discussing normal operation, we shall suppose that the vehicle passes the test.

If the vehicle is already a member of a platoon when it encounters the reverse turn, it is tested nonetheless. A platoon containing members which have not passed the reverse turn may not be admitted to the AL.

These manoeuvres are carried out according to a strategy derived by the link-level controller. The link-level controller is advised of vehicles' speeds, positions, and destinations via the RSVs. The strategy also involves control of target speeds of both TL platoons and AL platoons. The effect will be that when a gate is reached, the rear of the AL platoon is just ahead of the leader of the TL platoon. (Either platoon may be just a single vehicle.) The platoon level checks that the RSVs and gate bit indicate that this is indeed the situation. Vehicle by vehicle, members of the platoon are called onto the TL.

In this design, further merging of platoons does not take place on the AL. As platoons leave the instrumented part of the AL they enter a new block. They are counted. The total is compared with the number which entered the old block, corrected for entry and exit. There may be intruders or lost vehicles. We consider, however, only the normal case here. A target speed and maxspeed is given to the new platoon members. This is calculated to be such that the platoon will just attain platoon spacing plus, say three vehicle lengths, behind its predecessor when it reaches the VPDs in the next ‘block.

During motion on the AL, link control will wish to adjust target speeds, to enable platoons to reach gates at appropriate times. Only speed reductions are permitted. Speed reductions must be applied equally to all platoons in the block on the uninstrumented part of the AL. This avoids hazards. The vehicle is now passed, in a platoon of changing membership, from block to block. Gaps appear in the platoon because vehicles leave, but they are closed expeditiously. Eventually the destination is approached. The link-level controller selects the departure gate, and advises platoon level. Just as in the joining procedure, a platoon-level controller examines the evidence from RSVs and gate bits before issuing the command to rejoin the TL to the vehicle.

It is not known whether it is necessary for small gaps to open to permit a vehicle to quit a platoon. If so, this is done, and the vehicle exits at the gate. If the following vehicle(s) also must leave at this gate, two or more vehicles leave as a platoon. If this happens, the exiting platoon proceeds normally until all vehicles have passed through the off-gate. Then the rear vehicle brakes and drops back, thus leaving the platoon. Then the new rear vehicle brakes, and so on.

As soon as a single exiting vehicle is on the TL, and its brakes are not being applied, the driver receives a message asking him/her to resume manual control. He/she signals readiness, and manual control returns. He/she drives off the TL and to an off-ramp in the normal way,

2.8.3.8 Completing the Specification. The description above gives an account of normal operation, with a deal of detail elided. But full specification requires that all the detail be shown. Figure 2.4 shows a complete flow chart for the regulatory-level control of vehicles in *preplatoons.* Preplatoon is the name given to a platoon on the TL composed of vehicles seeking entry to the system. Vehicles in preplatoons may or may not have passed the test at a reverse turn, as explained above. There is no starting point on Figure 2.4, because the iterator goes round the loop shown indefinitely.

The principle stated earlier is that every action of a vehicle’s control systems be checked at the roadside. Therefore the regulatory level roadside controller must:

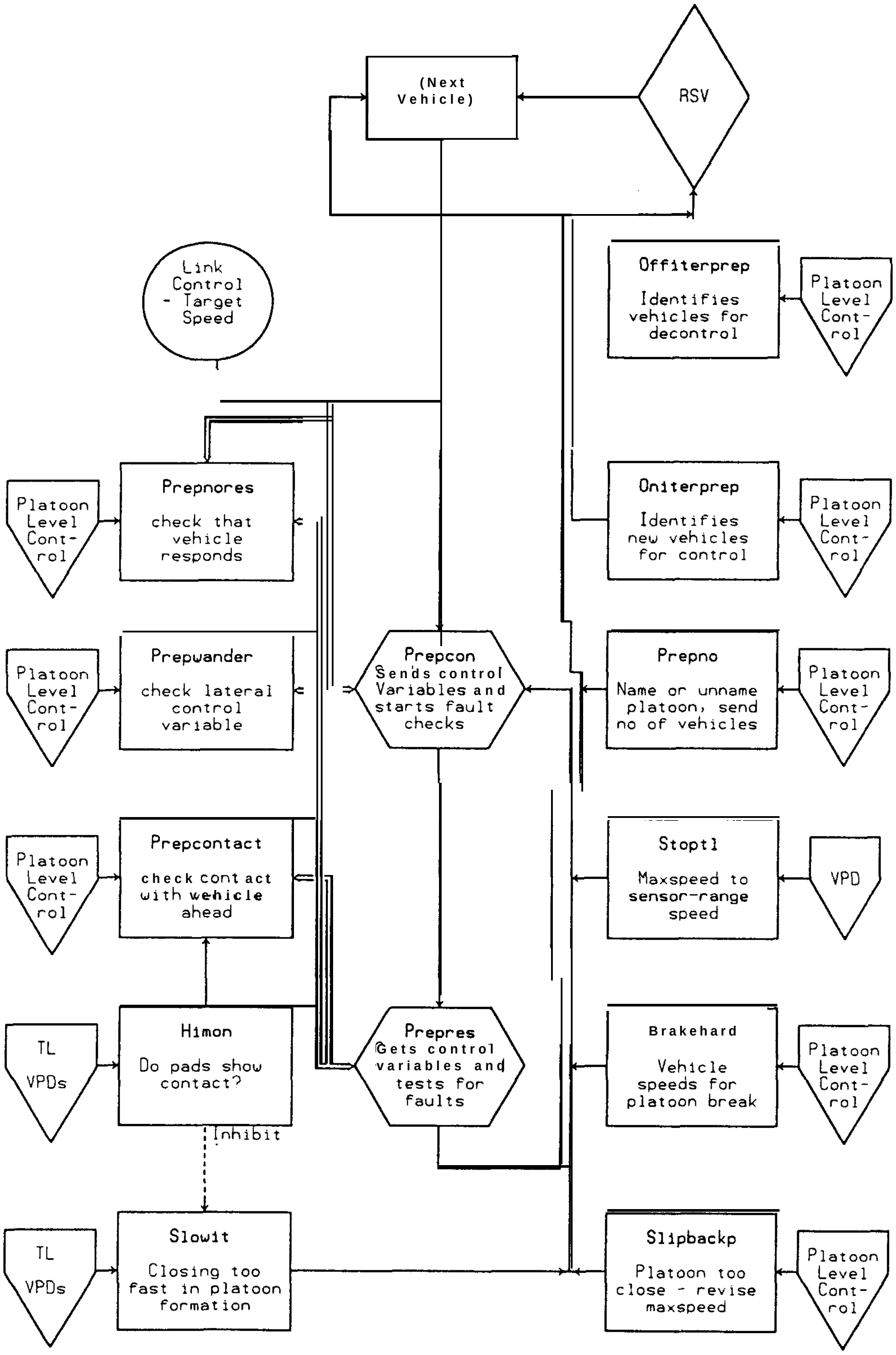
(Next Vehicle)
RSV
Link Control - Target Speed
Offiterprep
Identifies vehicles for decontrol
Platoon Level Cont-rol
Prepnores
check that vehicle responds
Platoon Level Cont-rol
Oniterprep
Identifies new vehicles for control
Platoon Level Cont-rol
Prepwander
check lateral control variable
Platoon Level Cont-rol
Prepcon
Sends control Variables and starts fault checks
Prepno
Name or unname platoon, send no of vehicles
Platoon Level Cont-rol
Prepcontact
check contact with vehicle ahead
Platoon Level Cont-rol
Stoptl
Maxspeed to sensor-range speed
VPD
Himon
Do pads show contact?
TL VPDs
Prepres
Gets control variables and tests for faults
Brakehard
Vehicle speeds for platoon break
Platoon Level Cont-rol
Inhibit
Slowit
Closing too fast in platoon formation
TL VPDs
Slipbackp
Platoon too close - revise maxspeed
Platoon Level Cont-rol

Figure 2.4. Modules in “Prepiter. "
(Regulatory level, roadside, control of entering platoons)
(VPD = Vehicle Presence Detector RSV = Roadside State Vector)

(a) send control data from the RSV to the VSV. This will include maxspeed and target speed, which will usually be unchanged. It also includes any data about the speed and acceleration of the platoon leader which may be required by the control algorithm.

(b) receive data from the VSV for the RSV. Some of this data, from a platoon leader, will later be passed to other platoon members. The rest of it will be tested, to ensure that things are proceeding as they should.

(c) access data from the VPDs, via the RSV, to enable the checks described below to be made.

The possible faults that are tested for are:

1. No ***response.*** No reply is received to the passage of control data to a vehicle. (It will be remembered that the communication of maxspeed follows a duplicated route.) This condition can have a temporary cause, like interception of a signal by a water splash. It may also indicate that a fault has developed. The fault could be in either the receiver or the transmitter on the vehicle.

2. Excessive lateral deviation from the lateral reference. Again there may be temporary causes: a touch of oil on the road, for example, but this may also indicate the beginning of a fault in the lateral control system.

3. Loss of contact with the preceding vehicle in the platoon. As in 1 above, this can be an isolated event or a first indication of a developing fault.

4. Closing too fast on the vehicle ahead during formation of a platoon. This is probably a consequence of some disturbance in the system, which link control has not caught up with.

2.8.3.9 Regulatory-Level Controller — The Prepiter. The primary regulatory-level controller is an iterator. Its operation is shown schematically in Figure 2.4. An iterator operates in a cycle, addressing each vehicle in a platoon in turn, going upstream, and then going on to other platoons of the same kind. Thus, in Figure 2.4, there is no starting point. Explanation, however, will begin with the box “next vehicle.”

The designer found it helpful to give a mnemonic name to each module and each controller component. These module names, “Prepcon, " “Prepres, " "Himon, " etc., are simply labels. They are repeated here so that the reader can tell which box in the figure is referred to. Thus, the first action of the controller (called the preplatoon iterator or ***prepiter)*** is to call the module Prepres. A message with the vehicle ID and control variables is sent using the RSV as data. The variables include target speed and maxspeed. The vehicle communicator stores these in the VSV, and should respond with its own variables.

In any event once the message is sent, the prepiter calls the module Prepnores. This should have been updated by Prepres on the previous cycle. If it has not been, the difference between the stored time of last call and present will be too great. The module Prepctnores (platoon level, not in figure) is called. We shall not follow this further. In the end, the pattern of non-response may suggest that the problem lies outside the vehicle. If so, there will be no action. If, on the other hand it seems that the vehicle is faulty, the platoon will be broken, the vehicle license will be marked so that it cannot re-enter, and the driver will be invited to resume manual control.

All this happens (if it happens at all) in the platoon-level controllers. The regulatory level, in the meantime, proceeds to call the module Prepres. This waits, briefly, for a response from the vehicle invoked by Prepcon. If there is no reply, the prepiter moves on to the next vehicle.

Normally, however, there is a reply from the vehicle. Prepres stores the appropriate data in the RSV. It then passes the current time to Prepnores, thereby inhibiting a call to Prepctnores on the next cycle. It then calls the modules Prepwander and Prepcontact.

Prepwander checks on the behaviour of the vehicle's lateral control system, as indicated by the magnitude of the lateral control error signal. If the signal is within bounds it updates an internally stored time. If the latter is out of bounds, and if too great a time has elapsed since the signal was within bounds, Prepwander will call the module Prepctwander (platoon level, not shown on figure). Prepctwander behaves very similarly to Prepctnores . The idea is to allow a reasonable time for the control system to recover from any large disturbance. If, however, the control system repeatedly fails to recover, the vehicle should be excluded.

The next module called by Prepres is Prepcontact. This checks on the continued ability of the vehicle to determine where its predecessor is. It also checks that once a vehicle has joined into a platoon, its predecessor stays in range. If the predecessor should fall out of range, this indicates some serious failure. However, no contact is to be expected if the vehicle is the platoon leader, or if the gap has not yet closed during platoon formation. Prepcontact therefore also needs the output of a module named Himon. Himon is a module in the VPD controller. It sets a bit in the RSV if the distance between a vehicle and its predecessor is such that sensor contact ought to be made (i.e., the distance is less than sensor range).

If no contact is reported when Himon indicates that there should be contact, a platoon-level module Prepnocontact counts up the number of failures, just like Prepnores. Repeated failures are followed by platoon break-up and exclusion of the faulty vehicle.

Also, if there has been contact, as reported by Himon, but Himon now indicates that the vehicle has dropped out of sensor range, it is immediately isolated by platoon break-up.

To conclude this example, the formal specifications of some of the modules mentioned in this description are reproduced in Table 2.1. A concerned reader can follow how the specification fills out and makes precise what has been sketched out.

'What has been discussed here represents about one-fiftieth of the whole formal specification.

2.8.3.10 Design of Platoon Level Controller. This partial account of the prepiter's actions illustrates how every action of the vehicle controllers is checked by the roadside. The second principle of design, as stated in Section 2.7.4, is that execution of each manoeuvre called for at platoon level shall similarly be verified, and action following failure to carry it out shall be specified.

To illustrate how this was done we shall consider actions of the system as a vehicle exits from the system. In Figure 2.5 we start at the point where a vehicle has reached the end of the automated part of its journey. It has left the AL, and is a solo vehicle, under automatic control on the TL. An iterator is still sending and receiving control signals from it, link control is still adjusting its target speed, and so on. At platoon level a message to the driver, "Please take control" is sent. Normally, the driver sends a positive reply, takes control, and the automated part of the journey is over.

But, we must ask, what happens if the driver does not take over? Since the TL is not continuous, the vehicle cannot be allowed to proceed indefinitely. If there is a dormitory at the end of this block, the vehicle will enter it automatically, and come to rest there. Usually, however, this solution is not available. The solution adopted in this design is to try, first, to cause the vehicle to re-enter the AL. Then it can be caused to leave the AL in the next block, and, if necessary, the next, and the next. In the end, either a block is reached in which there is a dormitory, or the driver does succeed in taking control.

The decision point is the last gate in the block, which is an on-gate. If there have been no intermediate disturbances, the rear of the platoon which the vehicle has just left will be available for it to rejoin. The appropriate instruction is given by platoon level, and the entry manoeuvre starts. If the manoeuvre succeeds, all is well. The driver, of course, has been carried past his/her destination, either because the vehicle is faulty, or because of a failure to pay attention.

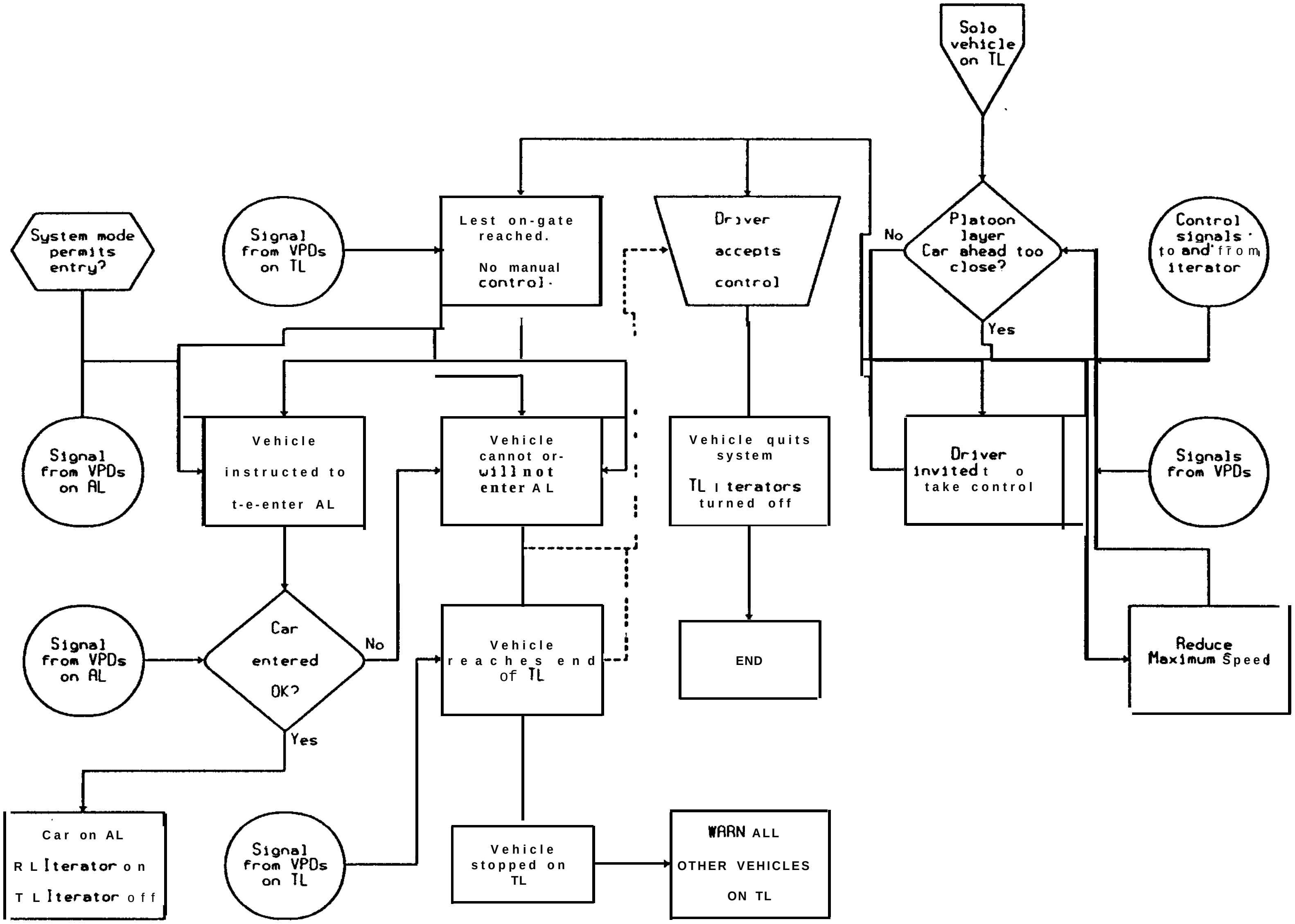

Figure 2.5. Vehicles Leaving TL.
(VPD = Vehicle Presence Detector)

Table 2.1 Formal Specifications of Some Modules

Name: **Prepcon** ro: Vehicle **ID:** Preplatoon **Requires:** Oniterprep: repeated each cycle simulated by clock. **If branch?** No (but see below) **Effect:** a. Passes control vars to vehicle. b. Passes current time to, and calls Prepnores. c. On return, signals for Prepres from same veh.	**From:** Prepiter **Other Input:** Target speed, maxspeed, (from link); other control variables. **Condition:—**
Name: Prepres **To:** Prepiter **ID:** Preplatoon **Requires: Prepcon** **If branch? Yes** **Effect:** 1. If message received, a. Updates veh control vars. b. Passes current time to Prepnores. c. On return, passes current time to Prepwander and calls it. d. On return, calls Prepcontact. e. **Endif;** 2. Call **Prepcon** for next veh.	**From:** Vehicle **Other Input:** Lateral control variable (LCV), sensor contact variable (XV). **Condition:** Message rcvd?
Name: Prepnores **To:** Lonr ID: Preplatoon **Requires:** a. Prepres b. **Prepcon** **If branch? Yes** **Effect:** a. Sets restime to current time; returns to Prepres; b. If (current time - restime) too large, calls Prepctnores; sets restime to present: else no action: returns to **Prepcon.**	**From:** Prepiter **Other Input:** Nil **Condition:** Intl var restime
Name: Prepctnores **To:** Lonr ID: Preplatoon **Requires:** Prepnores **If branch? Yes** **Effect:** Intl var N initially 0 (set on entry to platoon). Incremented each time **Prepctnores** is called; if N is too big, calls **Sorrybut2p; endif;** returns to Prepnores.	**From:** Lonr **Other Input: Nil** **Condition:** Intl Var N too large?

Note: The module Sorrybut2p starts the process of denying entrance to the AL, breaking up the platoon, and inviting the driver to resume manual control.

But, again we must ask, what if re-entry is not successful? Then, although this is likely to cause congestion, the vehicle must be brought to rest on the TL. The figure shows as much. It also shows that other vehicles on the TL are warned of this. Illuminated variable-message signs on the fence could be used to warn manually controlled vehicles, while the system will prevent automatically controlled vehicles from colliding. This least desirable outcome does not violate the safety criteria.

‘Two questions arise. First, assuming that for some reason the driver cannot resume control, what happens? The same thing as if the driver had never entered the system, but had come to rest on the freeway. The Highway Patrol will first get him out of there. They may ask the system controllers to close some off-gates while they do so. Then they will find out what went wrong and do what the law requires.

Following the design technique, we should ask “What if the vehicle does not stop at the end of the TL?” In this case, there have been two simultaneous faults on the vehicle. Maxspeed should be zero, and this should have been communicated to the vehicle by two independent routes. Both have failed. There is no violation of the safety criterion. The circumstances are therefore very unlikely. Any resulting accident is of the type for which the expense in money or capacity is too great to guard against. In this case, however, if the driver is capable of any action, there are some that can be taken. For example, deleterious consequences can be avoided or made less severe by switching off the engine. This is as much as will be said here about the specification of the first example.

2.8.3.11 Design Choices. In the account above, it is asserted in two places that a design choice was made for this example. We chose here, it has been said, to form “preplatoons” on the TL, of vehicles seeking admission to the AL. We also chose that a vehicle which did not resume manual control when invited to do so should be forcibly readmitted to the AL. Earlier, and more fundamentally, we did choose that this would be an infrastructure-intelligence, one-AL system. We saw no need to instrument the whole of the AL, or to have a continuous TL.

We had expected, when the process started, that there would be a great many points where it seemed that a satisfactory system could be produced in several ways, and we would have to choose one. Perhaps if we had made different initial choices, there would have been more subsequent ones. But in this design, we were not aware of making more choices than those just listed. The hazards determine the physical layout, as has been seen. They also constrain the number of operational schemes. It seems that the number of choices here is very small.

This applies, of course, at the conceptual level. As soon as alternative hardware designs enter the picture, the number of choices will presumably multiply.

2.8.3.12 Fault Tree ***Analysis.*** A full account of the fault tree analysis described briefly in the following paragraphs is to be found in Hitchcock (1991d). As with the specification, detail is omitted in what follows. The omissions are rectified in the report referenced here.

The process of fault tree analysis has already been described. It is pointed out that the objective in the examples is to determine whether the fault trees do terminate quickly, and to discover if they do detect faults.

Ideally, perhaps, we would find out if faults could be discovered by having both a design team and an independent fault tree team. The design team would insert deliberate errors into a design. The fault tree team would discover if the fault tree detected all the deliberate errors. In addition, it would probably pick up some real errors. However, this was not possible here, since there is only one worker. Under these circumstances it seemed unlikely that the insertion and detection of deliberate errors would convince anyone. The work therefore relies on the fallibility of the investigator. The fault tree searches for real mistakes.

The fault tree started with the four hazards. The first step was to identify the position of the entities concerned: on AL, on TL, or changing lanes. One went on to identify such entities as might be concerned: platoons, manually-controlled vehicles, accident debris or dropped loads, and so on. From here on the selection of branches depended on the circumstances; no generalization is perceived.

2.8.3.13 Results of Fault Tree Analysis. As may be seen from Hitchcock (1991d), no branch of the fault tree had more than four steps. Most had fewer. There were some 60 steps only. This demonstrates readily that fault tree analysis is a practical method for proving conformity to the safety criterion. Further, the investigator was found, to his annoyance but not to his surprise, to be fallible. Four design errors were found.

1. On the uninstrumented part of the AL between gates, a following platoon may gain slightly on its predecessor. No mechanism is provided to correct this. In any one block the effect is trivial, but it could accumulate, causing a hazard.

2. Care is taken to check that a vehicle joining the AL does so only at the rear of a platoon or into a large gap. However, no check is made of the vehicle's speed when it enters the AL. If this is much greater, or much less than the platoon's speed, a hazard can arise.

3. If a vehicle develops a fault, it is detected. The vehicle is taken out of a platoon and onto the TL. The driver is invited to resume manual control. No special precautions are taken, before he/she does take control, to keep other vehicles away from the danger presented by the faulty vehicle. This can lead to hazards.

4. A vehicle can be released from a platoon. A vehicle can be admitted to the TL on its way out of the system. In either case its separation from the vehicle in front is controlled to avoid hazard. Controls also ensure that the vehicle is not moving much faster than its predecessor. Thereafter its distance from preceding vehicles is controlled, although a manually-controlled vehicle can always cut in. However, at the moment of release no check is made on the vehicle's speed relative to its predecessor. This can lead to hazards.

Errors in design have been detected. If this were a real case there would be an intention to proceed further. In the end a system would be built. In such a case it would be necessary to repeat the conceptual design to correct the errors. One would then repeat the fault tree analysis. In this case, it is reasonably simple to correct the design. Even if the subsequent fault tree picked up more errors, it is reasonably certain that a fault-free design can be created.

However, no attempt has been made to design a link level. Thus nothing can be said about the capacity of this system. We will discuss the second example before drawing more general conclusions.

2.8.4 Example II

The first example of a complete specification was a single-AL system with intelligence concentrated in the infrastructure. The primary objective, however, is to demonstrate the method of complete specification and fault tree analysis, and test its efficiency, with as much generality as possible. Therefore it was decided that the second example should be as little like the first as possible. It should have many ALs and its intelligence should be concentrated in the vehicles.

Here, as in the first example, we describe and discuss both specification and fault tree analysis. For a complete account of the specification, including formal specification of all modules, see Hitchcock (1992c). For a full account of the fault tree analysis see Hitchcock (1992d). These are written in the form of free-standing reports. They are also appendixes to this one.

2.8.4.1 Safety Criterion. Here, as in the first example, we adopt the hazards set out in Section 2.7.1. We also adopt the safety criterion that a hazard shall not be permitted to occur unless there are two or more independent faults at more or less the same time and the same place.

We shall also, in this example, make use of the same concepts of platoon spacing, manual spacing, and the rest, which are defined in Section 2.7.1.

2.8.4.2 Work ***of Hsu, et*** al. (1991). At the relevant time, Hsu and her collaborators were just completing their own work (Hsu, et al., 1991). Their primary objective was to investigate the use of predicate logic based on state machines as encapsulated in the program COSPAN. Their chosen instantiation was a demonstration of conformity to specification of an automated multi-AL freeway system on which vehicles run in platoons. The conceptual level of definition in the specification is basically the same as that in our Example I.

HSU, et al. achieved their objective. COSPAN can aid a logically unassailable demonstration that the design of Hsu et al. does meet specification and is complete. The design therefore achieved its objective. Regarded, however, as a specification for an automated freeway, it is incomplete. No consideration was given to the physical layout. No consideration was given to the detection of faults, or to operation in fault conditions. Not least, there was no account of how vehicles would enter or leave the system. The interface between automated and manual operation was not defined.

Hsu's system is an account of the way in which, under no-fault conditions, a vehicle which has entered an automated platooned system may proceed through it, and arrive at an appropriate exit point. A number of parameters are communicated from the link level wayside system to each vehicle on entry. These include:

(a) a route through the multiple lanes of the system;
(b) maximum speeds in each lane;
(c) maximum size and optimal size range for platoons.

Apart from these, the intelligence — the whole of the platoon and regulatory layers — is vehicle-borne. Manoeuvres are initiated following exchanges of messages between platoon leaders. Sometimes other vehicles are involved also. There are three, and only three, basic manoeuvres:

> *Merge.* There are two platoons on the same lane. The follower contains fewer than the optimal minimum number of vehicles. The two together contain fewer than the maximum number. The platoons merge into one larger one.
>
> *Split*. A platoon contains more than the optimal maximum number of vehicles. Alternatively, one vehicle in a platoon is instructed, internally, to become a free *agent* (that is, a one-vehicle platoon). The vehicle requests a platoon split. In either case the platoon does split.
>
> *Change lane*. A free agent is instructed to change lanes. It creates and reserves space for itself in an adjacent lane by constraining the movements of other platoons. The free agent then moves into the lane. Restrictions on the other platoons are then lifted.

2.8.4.3 Completion of the Specification. It was decided to adopt the Hsu, et al. specification as a basis for the second example in this work. Accordingly the specification has been extended to include both a treatment of fault conditions and provision for entry and exit. All that Hsu, et al. say is true for the current system in normal operation, excluding exit and entry.

There is a section in Hitchcock (1991c) which explains what features of the system specified here are due to Hsu, et al., and which are new. Because some features are implied by Hsu, et al. but not specified, the distinction is not clear in every case. However, one point is important. In Hsu, et al. (1991), all intelligence is vehicle-borne. The additions include infrastructure-based intelligence. This can easily be seen to be necessary by considering entry and exit.

A manually-controlled vehicle on the ALs would create hazards. Therefore a vehicle which has entered the system cannot be permitted to resume manual control. But this must be allowed after it has left. Therefore either a signal from the infrastructure must confirm to a vehicle that it has left, or such a signal must actually induce relinquishment of automatic control. There must be, in either case, both some minimal capacity for communication with the infrastructure, and some minimal infrastructure intelligence at platoon level. In any case there must be intelligence in the infrastructure at link and higher levels.

In developing the design, the amount of infrastructure-based intelligence at platoon level has been kept as minimal as possible. This reflects the spirit of the original concept. But no alternative was found to using it in some fault conditions.

In the first example we adopted the principle that every manoeuvre and control action should be checked by the infrastructure. This arose from a distrust of all vehicle-borne actions, which might have been maliciously tampered with. When we are concentrating on vehicle-borne intelligence, such mistrust cannot be maintained. Accordingly, we now rely on elements outside the system to avoid hacking. A vehicle bears a self-monitoring system, which is regarded as reliable.

However, we also adopted, as a basis for design, the principle that whenever a manoeuvre was made, some check was made that it had occurred. If the manoeuvre had not been made, what did happen also had to be specified. This principle appears to be essential to meeting the safety criteria. It has been retained.

2.8.4.4 Physical Layout. In this case there are several ALs. Each has a lateral guidance reference. The layout has been discussed in Section 2.7.2. Some of what is said in Section 2.8.1.2, in relation to the first example also applies. As discussed on those pages, there must be a fence separating the ALs from the TL and also similar fences between the ALs. There are no manually-controlled vehicles on the ALs. Therefore, there are both manually-controlled and automated vehicles on the TL. In this case, there may or may not be other manually-controlled lanes. If the entire freeway is dedicated to automated vehicles there will be gates in the fence at the physical on-ramps and off-ramps. The on-ramps must have an escape route for any vehicle which is refused admission. Otherwise, there are lanes containing manually-controlled vehicles between the on-ramps and off-ramps. There will then be groups of gates with LONRs and LOFRs just as in the first example.

'At both the internal gates and those on the LONRs and LOFRs, there will be a *turning point,* just as in the first example. However, there is a vehicle-borne self-monitor. Its assurance that the vehicle is equipped and operational at entry is accepted. Therefore, there is no need for an identifier or a reverse turn in this example.

The ALs are divided into blocks. There is no compelling consideration which determines their length — perhaps they are 1 to 5 miles long. At the beginning of each block, a *block entry marker* @em) acts as a reference for measurement along the block. The bem can be precisely located by vehicles. Corresponding points on adjacent lanes should not have distances which differ by more than a metre or so. If there are sharp changes in direction, the blocks will have to be appropriately sited. A vehicle's distance from the last bem, plus its lane number, is called the Zoc.

Further, we assume here, that each vehicle is equipped with a forward looking sensor whose range exceeds platoon spacing in all weathers. (Platoon spacing may be increased above its dry-road value in adverse weather conditions.) The sensor is supposed to be able to detect and measure distance to the vehicle ahead of a platoon leader at all times, provided this range is less than some distance exceeding platoon spacing. It is also supposed to be able to distinguish a vehicle in its own lane from all others.

Therefore, in this case there is no need to equip the TL with VPDs or to track vehicles up to gates. The gates can send signals to vehicles which are received through the vehicle's lateral receivers. The gates can also receive signals from vehicles' lateral transmitters. Further, there are VPDs on the receiving sides of each gate. The turning points are active, and can be energized by infrastructure-based controls at the gate. If the turning-point is not energized it will not be detected by a vehicle.

2.8.4.5 Degraded ***Modes.*** Because there is a long-range sensor, the definition of sensor-range speed has no meaning. There is thus no natural choice for the speed to be chosen for the degraded modes. Strict analysis may show that there is no point in having the speed reductions in degraded modes at all. Nevertheless such reductions are included in this design.

In this design, the system modes apply to each section of each lane. The modes are:

a. Normal }
b. Stop } Defined above in Section 2.7.3
c. Crashstop }

d. Closed-ahead (CA). This applies when there are sections of the lane ahead in stop or crashstop modes. It also applies in some other fault conditions. Speed in the lane is reduced. Speed in the adjacent lanes is also reduced. (The adjacent lanes enter SA mode, to be described below.) Turning-points which would admit vehicles into the lane are switched off. Messages at each gate advise vehicles how far they can continue in the lane. (This stimulates the vehicle-borne controllers to change lane.) If they pass the last gate but one, their speed is further reduced. If need be, they stop to line up for exit at the last gate.

e. Slow-ahead (SA). This is called when an adjacent lane is in CA mode, and in some other fault conditions. The only effect is to reduce speed.

f. No-Entry (NE). Vehicles proceed at normal speed, but turning-points permitting entry to the lane are turned off, so that vehicles cannot enter. This is used in some fault conditions.

As ever, the system can degrade operation. In order to return to normal, direct action by the system supervisors and human supervision is usually needed. An exception is made, however, where NE mode is imposed because of the presence of a faulty vehicle in a lane. If the vehicle changes lanes or exits, the no-entry condition is lifted by the system.

2.8.4.6 Architecture, Level 0 — Physical-Level Components. The physical level in the architecture contains no controls which need to be designed.

2.8.4.7 Architecture, Level 1 — Regulatory-Level Components. This level controls and monitors the movement of individual vehicles. The on-vehicle components are:

a. Forward sensor. This has been discussed in Section 2.8.4.4. It provides a reading of both distance to the vehicle ahead and relative velocity. These are stored in an AR and are accessible both to other regulatory-level components and to platoon-level ones.

b. Message stores and flags. When any message is received by any communicator, a flag is set in an AR, a counter is incremented, and the message itself is stored in another AR. For a message received from outside the platoon, this is all. An acknowledge-control message is also not passed on. A message containing control data is passed to the longitudinal system and also passed on to the following vehicle in the platoon. All other messages are also passed on up or down the platoon by the regulatory level. There are obvious exceptions for the first and last vehicles in a platoon.

c. Forward transmitter and receiver. These are able to send and receive messages to vehicles ahead. Their range is at least equal to the minimum sensor range. If the vehicles are some distance away, there may well be several vehicles with which communication is possible. Since most messages refer to the vehicle communicated with, there will, in general be no confusion. There are many exceptions, however, and here some message passing, containing locs, is required to establish who wishes to communicate with whom. In platoon, however, the vehicle can distinguish the vehicle ahead from all others.

d. Rearward transmitter and receiver. These have the same abilities as the forward ones, except that they react to messages from behind.

e. Lateral transmitter and receiver. These communicate with vehicles to the side. They can also communicate with gates as they pass. They have a forward and rearward range equal to the forward and rearward ones.

f. System transmitter and receiver. These similarly communicate with the system.

Note. The failure of any two of these transmitters simultaneously can lead to a hazard. The transmitters cannot, therefore, all be combined. There are several ways in which transmission functions can be combined in pairs and only three transmitters are needed. Equally the transmitters may be combined in triplets, and only two are needed. The same is true of the receivers. It is however convenient in this paper to speak of them as independent.

g. An odometer which can determine the distance travelled since passing the bem.

h. A vehicle state vector (VSV) is stored in an AR. The VSV contains the AL license data. This is the vehicle ID, date of last inspection and a validation marker, which the system may reset, to invalidate the license. The VSV also contains fields saying where the vehicle is (lane, block, loc). Further there are fields describing the control conditions (block length, platoon sizes, speeds, lane mode, identity of any fault conditions, etc.). A “busy” marker in the VSV helps to ensure that each vehicle is engaged in only one manoeuvre at once.

i. A self-monitor (MON) which checks the behaviour of the regulatory-level components, and sets a fault marker in the VSV if any fail. It is assumed that the transmitters and receivers are “looping, " and that errors will consequently be detected at once in normal conditions. If an error here is undetected, there are two faults, one in the equipment itself and one in the self-monitor. As a vehicle passes each gate, it will receive a message from the gate, which gives the loc of the gate.

This enables MON to check the odometer. The other equipment is also put through regular testing in a way which enables MON to detect equipment as faulty when some logical paradox occurs.

j. A longitudinal control system, which is supplied with control data from the VSV, the forward sensor and the within-platoon communicators. It will maintain a vehicle in platoon. If the vehicle is a platoon leader or a free agent the control system will maintain the vehicle at platoon spacing from the platoon in front. An exception arises when a merge, split or split-change-lane manoeuvre (see later) is being carried out.

k. A lateral control system, which will keep the vehicle on track in lane. Lateral control will also carry out lane changes as required when a turning-point is identified.

2.8.4.8 Architecture, Level 2 — Platoon-Level Components. In the work of Hsu, et al. (1991), on which this design is based, the route is inviolable. In our case, however, faults can arise. Lane sections can, for example, enter stop mode. Vehicles cannot be admitted to a lane section in stop mode. There must therefore be dynamic changing of route of vehicles about to enter such a lane section.

In this design, therefore, a vehicle receives updated data for the relevant fields of its VSV whenever it passes a gate. Some of that data, such as the mode of the lane the vehicle is entering, are safety-critical and are supplied by the local intelligence at the gate. The maximum speed associated with the lane entered is a parallel example. Other data, such as a route change, come from the link level.

There is an overall on-vehicle controller. The off-vehicle link-level controller passes information to this on-vehicle controller on entry to the system. This information determines the vehicle’s route. As discussed later, this data may be modified during the trip. The other functions of the vehicle controller are:

(a) to initiate manoeuvres which enable the vehicle to follow its prescribed route, from entry to exit; to communicate with other vehicles, in the same platoon or another, using the appropriate message protocols; these messages start and maintain manoeuvres to receive messages from any position; to take part in platoon manoeuvres, after being invoked with messages using the right protocols.

(b) if platoon leader (including a free agent), to initiate merge and split manoeuvres designed to enable optimum platoon sizes to be maintained; if such initiation is untimely or impossible, to initiate test procedures designed to check that safety-critical equipment continues to function.

(c) to check the output of the self-monitor, and to take appropriate action if a vehicle fault arises.

(d) to switch the regulatory level automatic controls off and on when appropriately stimulated by messages from driver and system.

Other platoon-level functions are situated at the roadside. Many are contained in some minimal roadside intelligence located at each gate. In the following description we shall refer to “the system. " It does not matter whether all this intelligence is located at the gates or if some of it is centralized. The local communication at each gate is short-range and location-specific. MON uses these signals to check the odometer.

The roadside platoon-level controllers have the following functions:

(a) The gates “overhear” messages between vehicles engaged in the change-lane and emergency-change procedures. The final message names the gate at which the change will take place. If and only if a relevant message has been received and the receiving side of the gate is not occupied, the turning point will be activated for a limited period.

(b) Under some fault conditions, messages are transmitted to the system for echoing to other vehicles.

(c) Certain incidents, collisions, or a report of a breach in a fence, for example, require immediate change of mode for one or more lane sections.

(d) In joining and leaving the **ALs,** vehicles must establish their fitness to enter. Vehicles also need to be advised, when exiting to the TL, that manual control needs to be resumed, and must be brought to rest at the end of the TL if they have not done so. The exit messages need to be sent by both system and lateral communicators, in case the vehicle has developed a fault in one of these two.

(e) The system needs to be advised if a vehicle has developed a fault, and to take action if it does not soon report that it has left the **ALs.**

(f) A number of events can arise in operation which are indicative of a fault of some kind, but do not certainly identify the vehicle or element concerned. A vehicle is not declared faulty on the basis of perhaps being responsible for such an event. Sometimes the system can establish definitely that a fault is in a vehicle other than the one reporting. All vehicles or gates which might be responsible are listed by the system (and also all gates). If incidents occur repeatedly, involving one particular vehicle, that vehicle is declared faulty and excluded. Similar action is taken if a gate is associated with too many such incidents.

2.8.4.9 Architecture, Level 3 — Link-Level Components. The influence of link layer on system capacity is less profound in Example II than it was in example I. Link level selects the route. In a multi-AL system, this clearly has a significant influence on capacity, but it is less clear, in this case, that the influence is critical.

The manoeuvres which enable a vehicle to change lanes into a suitable vacant space are now controlled by the vehicle-borne platoon level controller. Only the choice of lanes to be followed rests with the link level. (If a lane is put into CA mode, the vehicles will change without prompting by link.) The communication with platoon level consists of the route instructions. Execution is entirely a matter for the platoon level. Thus the link level is outside the S-CS.

2.8.4.10 Treatment of ***Faults.*** In this design, diagnosis of faults is primarily vehicle borne, though there are a number of circumstances where faulty operation of a vehicle is deduced by the system, and communicated to the vehicle. In either case the vehicle sets appropriate fault flags.

If fault flags are set, vehicle directives change. In normal operation a vehicle will follow its route, as advised by the link level controller. As soon as a fault flag is set, however, it will exit the system as quickly as possible. It is shown in Hitchcock (1992c) that this is necessary. Two faults on the same or different vehicles can interact and this can result in a hazard. There is no fault which cannot be involved in a hazardous interaction. Therefore, it must be a remote contingency for two faults to meet. This requires that faults on the system must be rare. Therefore, faulty vehicles must leave as soon as possible.

The fault may result in a vehicle becoming immobile. If this happens, it will call for help to the system. The system will respond by calling stop mode for the lane section in which the vehicle rests. The system controllers are warned, and send appropriate manual help. In other cases the vehicle is capable of some movement, and can exit under its own power. To achieve this:

(a) If a faulty vehicle is invited to merge with another platoon, or to accommodate a vehicle wishing to change lanes, it will react as though its “busy” flag was set. This means that it will send messages declining to become involved.

(b) As soon as a fault is detected, a faulty vehicle in a platoon will attempt to become a free agent by initiating split or forced-split protocols. If the fault lies in lateral communication, the system will put the lane containing the vehicle into NE mode.

(c) It will then, using the emergency-change protocol (see Section 2.8.2.1), change lanes successively to the right until it has left the system if this is possible.

(d) If (c) above is not possible, it will transmit a “help” message to the system controllers, who will modify system modes to allow it to exit.

(e) When it has left the system, the validation and fault flags will remain set. It will not be able to reenter until the vehicle has been repaired and inspected.

2.8.4.11 Manoeuvres. In operation a vehicle may be in continuing motion on AL or TL, as a free agent or platoon leader, or as a member of a platoon. Only free agents are possible on the TL. Under these circumstances it may be engaged in a ***probe.*** A probe is a set of actions designed to test vehicle-borne equipment. Alternatively it may be engaged in a manoeuvre, which changes the composition of one or more platoons or free agents, or the lane of a free agent.

When a manoeuvre is in progress, the “busy” flag in the VSV is set. Except for the forced-split manoeuvre (see Section 2.8.2.1) a vehicle with a busy flag set will decline to engage in any other manoeuvre.

Manoeuvres are initiated by a vehicle which is so stimulated by its route instructions, or which has developed a fault. In normal operation there are three manoeuvres. These ***are*** called ***merge, split*** and ***change-lane.*** To these the present design adds the ***forced-split*** and ***emergency-change*** manoeuvres, which arise only in fault conditions. They are parts of the procedure by which a faulty vehicle leaves the system.

The five manoeuvres will now be described in general terms. These include formal specifications of every module. The listing which follows is given in order of priority, least significant first. If a vehicle receives two calls to take part in a manoeuvre simultaneously, it will prefer the later in the list that follows. “Simultaneously” here means “in the same cycle of the supervisor routine. "

The descriptions which follow are not complete: they ignore the procedures for ensuring continuity of operation if a fault arises during a manoeuvre. They also ignore the actions if some untoward event occurs. An example of the events ignored arises in the change-lane protocol. It is possible that alignments will be imperfect, and that the receiving side of a gate is occupied when a vehicle wishes to change lanes. In this case the turning-point will not be activated and there will be no change. The full protocol spells out what happens after that. Some of the untoward events, which affect other manoeuvres, are however touched on in the account of the forced-split manoeuvre.

The manoeuvres are all initiated by a message. If the message is a within-platoon one, its recipient is known to the sender, and stated in the message. For a message to another platoon, however, the initiating message is sent to a platoon whose identity is not known. However, the loc of the sender is given, and a recipient can determine if the message is relevant to it. If the recipient determines that the message is or may be relevant, it replies. The reply will give both the replier’s identity and its location. The original sender can now determine how to reply. In all subsequent messages, the addressee's identity is included.

The merge protocol is initiated by the leader of a small (less than optimum size) platoon, which perceives another ahead of it. The following platoon leader sends a message "request-merge" to the leading platoon. The message is received by the last vehicle in the leading platoon and is passed forward up the platoon to the leader. Other messages pass between leaders by the same route.

If the leader is not busy (engaged in another manoeuvre), and the leading platoon is not too large, the leader will reply favourably. Both the leader and the last vehicle in the platoon will set "busy" flags. The following leader now accelerates, and ultimately is following the leading platoon at the inter-platoon spacing. It then sends the message "confirm-merge. " On receipt of confirm-merge, the leader of the foremost platoon resets its busy flag. This leader modifies its VSV. The leader's following control data message refers to a larger platoon. On receiving a changed control message, vehicles with "busy" set are made aware that the manoeuvre is complete. They reset their "busy" flags. Each vehicle also updates its VSV and control data. Merge is complete.

The split protocol is initiated by a vehicle in a platoon which needs to become a free agent because its route requires it to change lanes. The procedure if a vehicle has become faulty is different. There are slight differences in the protocol if the vehicle wishing to become a free agent is the platoon leader. The differences are not discussed here.

A platoon member (the *splitter)* sends the message "request-split" to its leader. It sets its "busy" flag. If the leader is not busy, then it, too, sets "busy" and replies affirmatively. The vehicle ahead of the splitter, as the affirmation passes, also sets "busy." If a negation is returned, the would-be splitter resets its "busy" flag. Otherwise, however, the splitter declares itself a platoon leader, and transmits its own control data rearwards. The new leader also decelerates. Ultimately the new platoon reaches platoon spacing. The leader of the new platoon then resets its "busy" flag, and transmits "confirm-split." On receipt of "confirm-split," vehicles in the leading platoon reset "busy. " Split is complete.

The change-lane protocol can only be initiated by a free agent. It starts by sending a message "request_change_lane," indicating its location and the direction of the intended move. This will be responded to by vehicles in the receiving lane and, if there is one, in the lane adjacent to that. Any vehicle replying sets its "busy" flag. There are now two possibilities. Either there are relevant replies from the receiving lane, or there are none.

If there are relevant replies from the receiving lane, the lane-changer selects the nearest platoon with which to interact. Other repliers receive the message "thanx_but_-

no." On receipt of. this they reset their “busy” flags. Provided that the partner’s reply is positive, the partner now determines a strategy: the changer may enter ahead of it, behind it or at an intermediate point. Accordingly it advises the changer of the time at which it is to arrive at a specified gate. It may also decelerate to arrive at the gate just behind the changer. It may call on the other to decelerate, to arrive just behind its last vehicle. It may send the message "split_change_lane" to a specified member of its own platoon, thus initiating a “split” protocol. In this way a gap is opened into which the changer can move through the specified gate. The relevant message is overheard by the gate, which is so advised of the need to activate the turning-point. After a successful passage, the changer sends “confirm-change-lane.” A merge procedure is now entered. The changer becomes a member of a new platoon on the receiving lane. When the merge is complete, “busy” flags are reset. Change-lane is complete.

If there are no relevant replies from the receiving lane, the changer deduces that the lane is empty. Messages, if any, from the lane one over confirm that “busy” flags are set here, preventing another vehicle from entering the lane from the other side. The vehicle sends “change-to-void, " naming a gate. The gate overhears, and prepares to activate the turning point. After a successful change, the message “confirm-change-lane” enables any platoons in adjacent lanes to reset their “busy” flags. Change-lane is complete.

The emergency-change protocol is initiated by a faulty vehicle which is a free agent. It is similar to the change lane procedure. However, the change itself is always made into a gap of two or more platoon spacings in length. The platoons leading and following this gap on the receiving lane participate in the manoeuvre by keeping an appropriate relative position until the change has been made. This prevents the approach of any other vehicle from the receiving lane. In the same way, two other platoons on the lane adjacent to the receiving lane track the gap in the same way. This means that no vehicle can enter the gap from the other side. The fault may mean that the emergency-change vehicle cannot attain full speed, in which case a message is sent to the system and all the vehicles are slowed down.

The forced-split protocol is sometimes initiated by a faulty vehicle in a platoon. Usually it will call a forced-split ahead of itself, so that it becomes the platoon leader. If, however, the fault lies in its rearward communication, the faulty vehicle will start by causing forced-split behind itself. The protocol can also be initiated by the in-platoon probe (see Section 2.8.2.12). A vehicle in a platoon whose successor or predecessor ceases to communicate with it is caused by the probe to initiate a forced-split.

The effect of the forced split is the same as split. The differences are stated below.

(a) Although a confirm_forced_split message is sent, the protocol does not rely on its receipt to come to an end.

(b) The original platoon leader may be “busy” at the time the forced-split is started. For another manoeuvre, it would decline to take part. In forced-split, however, the leader may suspend other action, or may send a message breaking off the current manoeuvre. When the forced-split is complete, the leader will check to see if the previous activity needs to be resumed.

(c) Equally, the last vehicle in the rear platoon formed by the forced split will check at the end of the forced-split protocol to see if its “busy” flag is set. If it is, the original platoon was engaged in some manoeuvre before the forced-split, and the new leader needs to be advised of this.

2.8.4.12 Probes. The platoon leader probe serves to ensure that data are provided to MON by means of which a fault in the forward-looking sensor can be diagnosed. Whenever a platoon leader or free agent passes a gate and is not “busy” the probe is initiated. If the forward sensor detects one or more vehicles, it sends a message requesting a reply. The message gives the loc of the sender, which has just been updated at the gate. The reply should give the loc of the vehicle replying.

If a reply is received which agrees with what is seen, well and good. If no reply is received, a request for a reply from any vehicle within reasonable range is sent. If again no reply is received the forward sensor is adjudged faulty. An exception arises if only one vehicle is in sight. If the system advises that there is a vehicle that cannot communicate rearwards in the area, the testing vehicle is reprieved.

A similar procedure is gone through if no vehicle presence is reported by the forward sensor. If the probe elicits no reply, all is well. If a reply comes from a vehicle whose reported position is such that it ought to be perceived, the sensor is at fault.

A check on the odometer is carried out when a vehicle passes a gate. It is contained within the regulatory layer.

In platoon, whenever a control data message is passed backwards (upstream), an acknowledgement is sent forwards. This “acknowledge-control” message, alone of all messages passed in platoon, is not passed on. The in-platoon probe is a procedure within the vehicle controller. The probe checks that a control data message is received at least every other cycle of the supervisor. The in-platoon probe also checks that acknowledgments are received at least every other cycle. If appropriate data are not received, a vehicle starts acting as a new platoon leader. If, after a further delay, it does not receive data from a new leader ahead of itself, it will start the forced-split protocol. Equally, if a vehicle does not receive acknowledgments it will send forward an indication that a forced-split should start.

2.8.4.13 ***Entry and Exit***. There is little to add here. On entry, a driver should select a speed and position on the TL which will enable him/her to enter at a convenient gap.

The driver will request entry. Provided that MON on the vehicle indicates that all is well, the vehicle will be taken under automatic control. The first step is to call for a change-lane manoeuvre onto the first AL. As the vehicle enters it receives its route from link level.

At exit, a change-lane manoeuvre is called which leaves the vehicle on the TL. The driver is immediately invited to regain manual control. In this design, if manual control is not resumed, the vehicle is brought to rest at the end of the TL. The TL is made rather wide here, so as to leave room for this.

2.8.4.14 Design Choices. In Example II, the elements in terms of which the design is made are the manoeuvres and probes. The investigator was not aware of very many design choices. The decision to apply the full two-platoon-length gap to all emergency changes was one of them. Only one more choice is apparent. Vehicles which do not resume manual control at exit are "stranded" on the TL. Clearly it would be possible to readmit them onto the ALs. What should happen then is not clear. Probably they should be retained as free agents, operating as though they were faulty. There are other variations here, therefore.

The designers of the original subsystem probably did have more choices. Something like the "busy" feature is necessary to limit the number of interacting manoeuvres. In its present form it may be unnecessarily restrictive. There are probably several ways of designing an intermediate protocol. The choice among them could well produce marked effects on capacity. There would be some increased complexity in the design of the manoeuvres, but there is no reason to suppose that the safety criterion cannot still be met.

Again, it is to some extent possible to exchange the use of sensors to detect other vehicles with the use of messages from one to another saying where they are. This creates another set of design alternatives. However, it will be recollected that one of the determining factors in Example I was the desire to keep noise and signal overlap to a minimum. Whether the vehicle-borne intelligence designs can avoid excessive loss of information because of noise, etc., remains to be seen.

In Example I the number of satisfactory designs at this conceptual level was very small. In this case the constraints seem to be a little less restrictive. Certainly the physical layout is constrained. More work would be needed to establish the degree of variety. In Example I there were many requirement specifications for platoon level and regulatory level controllers and sensors. They could be met with a large variety of alternative technologies. Within each technology the requirement specifications could be met by many hardware designs. The same is clearly true for the vehicle-borne intelligence systems.

2.8.4.15 Fault Tree Analysis. As in the first example, a fault tree analysis has been carried out here. Once again, each hazard is considered in turn. First the places where the hazard might arise are distinguished. Then the nature of the objects involved is determined.

2.8.4.16 Results of the Fault Tree Analysis. This time, there were never more than three branches in the fault tree. Once again, the efficiency of fault tree analysis as a means for detecting faults is demonstrated. Once again, it was discovered that the designer had allowed faults to creep in, and these design faults were discovered. In this case, however, there is a fault which may be inherent in all systems in which the intelligence is primarily vehicle-borne.

This possibly inherent fault relates to the possible entry to the **ALs** of an intruder. An intruder is a manually-controlled vehicle, whose driver chooses to enter the **ALs.** This action is expected to be illegal. However, people do not always obey the law. An intruder can neither communicate with other vehicles, nor with the system. Other vehicles, and the system, will therefore often be unaware of the intruder's existence. A vehicle may be able to detect an intruder with the forward sensor. The system can detect the vehicle at entry and exit. Hazards can arise when an intruder is too close to the platoon ahead of it, and also if a vehicle changes lane close to an intruder.

It is a fault in the present design that the system does not warn of the presence of an intruder when one is detected at entry. If at that point stop mode were called by the system, it would be possible for the intruder to be detected by the Highway Patrol. This is a drastic solution. However, the difficulty arises here because it is not possible to track an intruder through the system.

Five other faults were detected by the fault tree analysis:

1. If a vehicle, on entry, has a fault in its forward sensor, this may not be detected until the vehicle is enabled to attempt the forward probe. A hazard can arise.

2. A vehicle is moving very slowly. Another vehicle changes lanes behind it. A message warning of the change will have been sent by the changer. But the slow vehicle will not, as the design stands, recognize the relevance, because it is more than platoon spacing ahead at the time of sending the message. Indeed the slow vehicle may even be out of reception range. At the time of the change, however, the two vehicles may be too close and a hazard can arise.

   A variant arises when a slow vehicle and a faster one are both wishing to enter the same lane. In this case, the hazard does not arise if the slow vehicle is faulty, because of the extra protection given by the emergency-change protocol. However, a vehicle may be slow-moving for other reasons.

3. A vehicle changing lanes, in one of the variations, enters at the head of a platoon in the next lane. If the vehicle strikes the gatepost there is immediate catastrophe. This point is discussed in Section 2.7.2. The solution is to arrange that in this variation of the change-lane protocol, the platoon in the receiving lane drops back a full platoon spacing.

4. If entry and exit lanes are combined, an entering vehicle may contain an undetected ‘fault in its odometer, since this can only be checked at a gate. In this case, the vehicle on the TL may not be sufficiently far away from an exiting vehicle.

5. A vehicle with a faulty forward sensor is protected from the consequences of the fault while being shepherded out of the system. Once the faulty vehicle has exited, there may be a slow-moving manually-controlled vehicle ahead of it on the TL. The fault prevents the vehicle control system from detecting the vehicle ahead. There will be no response to a message. The driver will have time to regain manual control and brake. Otherwise a hazard will arise.

Errors in design have been detected. Just as in the first example, in a real case there would be an intention to proceed further. In the end a system would be built. It would then be necessary to repeat the conceptual design to correct the errors. One would then repeat the fault tree analysis. The lines on which design could be corrected for most of the faults above are clear. However, some vehicle presence detectors plus a good deal of infrastructure intelligence would be needed to overcome the problem set out in 5 above.

It is less clear that it is possible to deal with the problem of an intruder. It is, indeed, part of the underlying basis of the use of vehicle-borne intelligence that it can be relied on, with the exception of rare faults in components. An intruder contradicts this completely. The investigator can conceive of only one satisfactory protection against an intruder within the system. Protection can be achieved by calling stop mode if an intruder is detected. This is a very high price to pay. It may be that some people would be tempted to intrude in order to provoke the nuisance of stop mode. An alternative would be to rely on legal sanctions against intruders.

2.9 Design Concepts for Automated Freeways

Designs satisfying the safety criterion can be achieved with the intelligence concentrated in either vehicles or the infrastructure. A proviso is that components with the assumed performance (or equivalents) can be instantiated as reliable engineering devices. It is also possible (with the same proviso) to have one or multiple ALs. No doubt there are also safe designs with the location of intelligence more mixed.

Current research in PATH suggests strongly that most devices with the required performance can be made, although the research required to specify the reliability required has not yet been done. The possibilities for such research are discussed in Section 4. However, all the designs require a vehicle-borne means of measuring the distance between two vehicles and the relative speeds. Devices with the range and flexibility required have yet to be demonstrated conclusively.

For in-platoon control only short range devices are required. Current research does suggest that this problem is soluble (Chang, 1991). However, the long-range forward sensor of Example II may not be possible. At the required ranges (say 150 m) vertical curvatures in the roads may mean that line-of-sight detection cannot be guaranteed. Equally, horizontal curvatures may preclude certainty about which lane a vehicle occupies.

Example II does appear to rely on such a long-range sensor. The design of Example II covers the fault where this device does not function. The communication equipment and odometer provide a way of furnishing the required data. A safe system with vehicle-borne intelligence which does not rely on the long-range sensor can therefore probably be designed.

However, the choice between intelligence in the infrastructure and in the vehicles should not be made on safety grounds alone. Cost and capacity are also very relevant. Capacity is dependent on the design of link level controllers. This is a topic which has not been studied. It would therefore be unwise to press for one location of intelligence rather than the other now.

2.10 Summary

In this section, an approach to the safety of automated freeways has been described. It operates at the conceptual level. The descriptions are mainly at the level of the architecture called "platoon level" by Varaiya and Shladover (1991). The steps are:

(a) Define safety criteria. No design is perfectly safe, and indeed, without definition, it is not possible to attempt a rational approach to safety. Here, the definitions chosen are in terms of the number of near-simultaneous faults which can be tolerated.

(b) Define hazards. These are the precursors of a catastrophic event. The term "catastrophic" also needs to be defined. Here it refers to a high-delta-V collision. Such a collision will often lead to multiple deaths or injuries. These, therefore, rather than all crashes, are what we seek to avoid.

(c) Define the general requirement. Here we considered both a single lane and a multi-lane freeway. The former shared a freeway with manually-controlled traffic.

(d) It is now found that the hazards and the requirement constrain the physical layout almost completely. The design team goes on to specify normal operation, and then to complete the specification, allowing for fault conditions. The paper shows how such a complete specification may be achieved.

(e) Simultaneously, a team of engineers, equal in status with the designers, verify that the design satisfies the specification. They also verify that the specification is complete, and that the safety criterion is met. Further, it is checked, to some degree, that the design is a design of what is wanted. It is possible that what was specified falls short of what is wanted. This is validation of the conceptual design. The last step is a complete fault tree analysis.

The section goes on to demonstrate the practicality of this prescription by working two examples. Both examples contained points where the safety criterion was not met, but it is clear that a second iteration would remove these faults. Thus it is possible to design an automated freeway which meets the safety criterion chosen.

The result can be generalized without being excessively tentative. It is possible to design an automated freeway which meets any safety criterion of the kind considered, and any reasonable requirement specification.

It seems likely that the imposition of a more rigorous safety criterion will impose significant additional costs. Cost here refers not only to money costs, but to reduction of the operating efficiency of the system. Because little is known of the capacity effects of differing modes of operation, it is not possible to draw conclusions about optimality of designs.

SECTION 3. SAFETY CONSIDERATIONS FOR DRIVER AIDS AND COPILOTS

3.1 Overview of Research Achievements

PATH is also concerned with other aspects of IVHS, in particular with so-called AVCS-1 devices (see Mobility 2000, 1990). These are vehicle-mounted devices which warn drivers of potential dangers ("copilots") or take control in dangerous situations ("driver aids"). In some advanced cases they may communicate with other vehicles or the infrastructure to achieve these goals.

The research problem here is to predict the performance of such devices, in terms of the number of casualties saved per vehicle-mile or per year. Evaluation in these terms will enable a choice to be made from the devices to be developed. If evaluation has sufficient relative accuracy, it will aid the choice among different designs of the same concept. Further, the question will arise whether there is a need for governmental regulation, approval or licensing of devices. Good evaluations will help to answer this question as well. Then, if that is the decision, evaluations will be necessary to determine which devices should be licensed, etc.

A method of evaluation has been proposed within the PROMETHEUS project in Europe (Hitchcock, 1987; 1988). It has subsequently been worked on and extended by others (Broughton, 1988; Fontaine, et al., 1989; Marburger, et al., 1990). This method was the only one available at the time. It has been applied and is practical, provided data of the appropriate kind are available. Regrettably such data are not available in U.S.A.

3.1.1 "In-Depth" Data

In the European applications, Hitchcock's method used "in-depth" accident databanks. There are no up-to-date in-depth databanks in North America. The use of European data for resolving U.S.A. problems is not appropriate here. Accident patterns are very different in Europe and the U.S.A. There are three possible solutions to this difficulty:

(a) Other data, available in the U.S.A., can be sought. They can be evaluated to see if they are effective when used with Hitchcock's method. That is the approach here.

(b) Alternative methods of analysis can be sought. Campbell, et al. (1991) report such an approach, which is promising. If this approach can be made to work it is likely to be the best solution. Its originators, however, recognize that this point has not been reached. Some comment on this unresolved issue is made later.

(c) One can collect new data of the kind originally used by Hitchcock. This would be very expensive. This approach would have merit if other uses were perceived for this data. However, that is not yet the case. This possibility will not be discussed further.

3.1.2 Approach to the Problem

Two questions seem to arise:

A. Is the Hitchcock method acceptable as an evaluation technique in the U.S.A.?

B. Can relevant data be made available for use with it?

The first question requires that the method be generally understood in IVHS circles in the U.S.A. Papers at technical conferences have been prepared which discussed the method and the European applications of it. These were compared, and found to be tolerably consistent.

Investigations were made into the availability of data having the right general characteristics in North America. One possibility was the use of Police Accident Records. These are regarded as sensitive data, and it was decided not to attempt this first. NHTSA's National Accident Sampling System seemed a reasonable alternative, and access to the raw data was arranged. A method was proposed for determining whether these data could be used with Hitchcock's evaluation technique for evaluating each of seven different devices.

The results were mixed. There has been very heavy editing of some data felt to be sensitive. As a result, the accuracy of any evaluation would be low. If the missing data were made available results would be attainable for many devices, but not all.

3.2 Structure of Section 3

All of the work reported here has already been published (Hitchcock, 1991b; 1991e; 1992b). Therefore we shall review only what is relevant to the general conclusions to be discussed in Section 4:

(a) A brief account will be given of Hitchcock's method for evaluation of AVCS-1 devices. Limitations of the method will be pointed out.

(b) The European applications, within PROMETHEUS, will be referred to and compared.

(c) Possible approaches to the problem of obtaining U.S. data suitable for use with the method will be discussed.

(d) Work on the evaluation, for the purpose of use with Hitchcock's method, of the NASS (National Accident Sampling System) data will be discussed.

(e) Alternative approaches to the problem will be discussed and compared with this one.

At the end of this section, we shall go on to draw conclusions about possible alternative lines of research.

3.3 The Evaluation Method

As proposed originally (Hitchcock, 1987; 1988), the evaluation method depends on the availability of "in-depth" accident data. Such data have been reviewed world-wide by OECD (OECD, 1988). No two such data-sets are identical. They have the following common features.

(a) A specialized team visits the scene of each accident. Maps are prepared, showing the paths of each vehicle. Photographs are taken. This visit may be contemporaneous with the accident, or may take place later. The maps usually incorporate the results of the other inquiries.

(b) Interviews are held (or at least, sought) with each participant driver in the accident.

(c) An examination is usually made of damage to vehicles. Some attempt is made to correlate this with the data in (d) below.

(d) Information is collected on the location and severity of injuries. This is done either by interview with casualties or by obtaining data direct from medical people.

In-depth databases are multi-purpose. The injury data, correlated with vehicle damage data, for example, are used to deduce the effects of different design features in-car, on patterns and severity of injury. Light can be cast on such psychological features as distraction, and so on. The full range of uses is not foreseen at the time of collection. However, no demand has been expressed for in-depth data in North America for any purpose except evaluation of IVHS.

Databases vary in the basis for sampling. All are restricted to one or more small areas. Some are restricted to a particular manufacturer's vehicles. Others concentrate on fatal accidents. Further, the method by which the team is alerted to the occurrence of an accident introduces sampling bias. For example, very few in-depth databases contain very many pedestrian accidents.

The information used in the method discussed here mainly derives from the map and the interviews. From these it is usually possible to deduce just what happened. The course of the accident can be traced. The account of the accident begins with what each driver believed was the situation. The account continues with what each driver attempted to do, as well as what he/she did do. There may be some uncertainty here, and usually this will be reflected in a probabilistic final evaluation.

In the method, the investigator now supposes that one or more vehicles involved in the accident was equipped with the AVCS device being evaluated. In the original, simplest form of the method a judgment is now made as to whether the device would have affected the course of the accident. Alternatively, the accident is modelled and a more precise determination is made. If the device gives a warning, it will also be necessary to make assumptions about the driver. The model must include statements about how he/she would react to the warning. This means not only reaction time, but also the nature of the action (brake, accelerate, swerve to left or right, etc.).

The next step is to total successes and failures for the device. Alternatively, probabilities are totalled. One can thus arrive at an estimate of the potential effect of the device for eliminating or affecting accidents belonging to the population sampled by the database.

The interview data are important here because it casts light on the intentions and so the nature of the errors made by drivers. A device can affect or correct some errors only. Of course, some drivers refuse to be interviewed, and no doubt some tell lies or have imperfect recollection. To a degree these factors can be corrected by using other interview data. With good interview data, it is possible, in half to three-quarters of the cases, to form a reliable view of the course of the accident.

3.3.1 Limitations of the Method

The quantity estimated by this method is the proportional reduction in accidents in the population sampled by the device on the basis that:

(a) the device operates correctly in all relevant cases;
(b) there are no effects of the presence of the device on driver behaviour;
(c) the device generates no accidents, in normal operation or in fault conditions;
(d) if there is partial penetration of the market, the drivers who purchase the equipment make up a random sample of all drivers.

In practice, too, it may not be possible to determine how a driver will react to a warning device. Some reactions may be inappropriate. The effectiveness of the device then needs to be reduced by the unknown fraction of mistaken reactions.

Assumption (b) above is almost certainly false. The evidence about the phenomenon known as risk compensation has been summarized by Evans (1985). There are many examples of changes made in the driving situation in order to increase safety. Most of these generate some change in driver behaviour which modifies the effect on safety. Usually the effect of these changes in behaviour is to reduce, but not eliminate, the safety gain. The difficulty is that the magnitude of these effects varies in different cases from 0 to 100%, and apparently, even more in some paradoxical cases.

A further possibility is that a driver who has become habituated to the effects of a particular AVCS-1 device may carry a changed behaviour into a vehicle which is not equipped. This, too, may reduce any overall positive effects.

Again, it is most likely to be those people who value safety highly who will be early purchasers of a device. It is at least plausible that such people drive in such a way that they are less likely to need rescue by the device. However, if such people bought the device dominantly for their teenaged male children, for example, the effect at partial penetration of the market could be enlarged.

For all these reasons the total effect of any device as estimated by the method is likely to be overestimated. The same is true for the same reasons for all other methods currently proposed. There does not seem to be any way in which a correction could be made on the basis of scientific evidence. In particular there is not any theoretical basis for estimating risk compensation. There is not likely to be such a theory soon. Thus there can be no basis for extrapolating from one measured effect to an unmeasured one.

Nevertheless, for many purposes this method has value. In practice the method will be used for:

(a) estimating a total cost-benefit ratio, in order to prioritize developments. In the early stages at least, no development of devices whose ratio is marginal is likely. More dubiously, there is no reason to suppose that the magnitudes of the risk compensation effects will vary wildly from device to device. Thus, to use the result of this method is unlikely to produce bad decisions.

(b) choosing between two alternative instantiations of a device. If the difference relates to the mode of warning then this method cannot help. The same is true if the difference relates to some other human-factor aspect. If, however, the difference is in sensor technology or logic, the relative effect of the corrections is likely to be negligible. The method then has merit.

There remain some unresolved questions here. They are discussed further in Section 4.

3.4 Application of the Method

The method described is recommended by the PRO-GEN group for use within PROMETHEUS for evaluation of safety effects. (Dryselius, 1990). There have been four separate applications, to similar but not identical devices, using three different databases (Hitchcock, 1987, 1988; Broughton, 1988; Fontaine, et al., 1989; Marburger, et al., 1990). Two of the databases were "in-depth" ones, and were of very similar design. Hitchcock and Broughton used the UK "at-the-scene" series (Sabey, 1983), which dates from 1981. Marburger and his colleagues used the Hanover database (Otte and Schlichtung, 1988). Fontaine and her collaborators made use of certain very full and elaborate French police accident reports (*procès-verbals*).

None of these workers apparently found any difficulty in using the data to produce results. Hitchcock (1991b) has compared the results of the UK and French workers. The results were corrected for differences in the assumptions. As good agreement as could reasonably be expected was found. The work of Marburger, et al. was not available at the time Hitchcock (1991b) was written, and is not discussed there, but the same general agreement is found there. Thus, although the method appears to have subjective elements, they do not appear to produce major effects in practice. The method is practical and effective when suitable data are available.

3.5 In-Depth Data in North America

The OECD report refers to only two "in-depth" databases in North America. Neither is up-to-date. The 1974-5 Indiana tri-level study (Treat, 1979), moreover, contains less than 500 cases at the deepest level. This is the "in-depth" level. The present author is advised that there is a somewhat more recent (-1979) database, modelled on the tri-level set, available in Canada. It is thought to be a little larger.

Both of these databases, and probably also the well known collection of accident reports held at the University of North Carolina, Chapel Hill, may well be suitable for use with Hitchcock's method. The earlier ones may fail to carry as much conviction as they would have done, had they been more recent. Further there are difficulties in accessing all save the tri-level study, which is almost certainly too small for many purposes.

Another possibility would be to follow the example of Fontaine, and investigate the use of Police Accident Reports (PARs). However, while the French ***pro&-verbal*** is a public document, PARs are regarded as sensitive in the U.S.A. It was felt that the need here was to have a method of telling whether or not a database would be useful for evaluation of a wide range of devices. If such a method could be established, perhaps a fairly brief study would be sufficient to establish whether a data source was worth the trouble of access.

The National Accident Sampling System (NASS) is a large data-set compiled by the National Highway Traffic Safety Administration (NHTSA). Its coverage is not fully representative of U.S. conditions, though there are methods of weighting it to reduce biases from this cause. It is a derivative of the old tri-level study.

An initial visit to one of the local collection agencies revealed that in the early stages, NASS collection procedures are not unlike those used in the UK in-depth work (of which the investigator had hands-on experience). The primary difference was the use of telephone interviews instead of home interviews. These observations were very encouraging. One possibility had been that the influence of U.S. legal procedures would create a marked increase in refusals to give interviews. However many of the NASS respondents gave similarly open interviews to the ones on which the UK in-depth database was based. A numerical comparison is not possible. PARs are also collected at this stage.

Accordingly, arrangements were made to access the NASS raw data files, with a view to determining their suitability for use with the evaluation method discussed here. This work is discussed in a following section.

It was found that the method selected did enable a view of the value of the NASS database to be formed. To this extent the result is helpful, since it sets a pattern for similar evaluations of other databases. However, it was regrettably concluded that the value was slight. In the form in which the data are available to external researchers the data originally collected have been heavily edited. The PARs and the interviews are absent, and replaced with a brief executive summary. The summary is not concerned with intentions.

An attempt was made to imagine that good interview data were available. A view was taken about the effectiveness of the NASS data for evaluation of AVCS devices in these circumstances. As would be expected, results were very much better. However, some lacunas remained. NASS says very little relevant to possible faults in road signing, layout or surface friction. The two vehicle faults most frequently associated with accidents are poor brakes and smooth tires. NASS reports on neither.

3.6 Evaluation of the NASS Database

The method used to evaluate the database will now be described. The problem was to examine the effectiveness of the NASS database when used with the method under discussion as an evaluation tool. The method requires that each record of a vehicle involved in an accident be examined. One then imagines that the vehicle is equipped with the IVHS device (device X) under study. The basic question then is:

(a) would the presence of device X have affected or eliminated this accident? or

(b) what is the probability that the presence of device X would have affected or eliminated this accident?

By counting hits and misses, or summing probabilities, an estimate of the reduction in accidents can be arrived at. If, however, the answer to the questions is "I do not know," a separate count must be made. Including this total gives a measure of the accuracy of the evaluation.

To evaluate the database, therefore, one needs to compare the fraction of "I do not knows" with the number of relevant cases where a judgment can be made about (a) or (b) above. The merit of this approach, compared with actually performing an evaluation and measuring the uncertainty, is that very many fewer cases need to be examined to obtain good statistics.

It is often easy to judge that device X could not have affected the accident. A night vision aid cannot affect a daylight accident. It is not relevant. The certainty of this judgment is also not relevant to the efficiency with which the database can evaluate the device.

The database evaluation therefore proceeded as follows. Seven different devices of diverse function were defined rigorously. After this, each vehicle record in the sample of accidents selected was examined. The same sample was used for all seven devices. For each device, and each record, the following questions were asked:

(a) Is the device *relevant* to this case?

(b) Is it possible to judge whether the device would have *functioned*? (Devices were defined with realistic limitations.)

(c) Is it possible to judge whether the device would have been *noticed* by the driver? (This question is relevant only if the device gives a warning. All the ones considered did. But each has an "intervention" analogue, to which driver reaction was irrelevant.)

(d) Is it possible to form a judgment about the probability that the device would have been *effective*?

After this, it was assumed:

(a) that the editing of the interviews had not taken place.

(b) that where an interview had been given it did give the sort of detail that had been collected in the interviews that had been witnessed.

The last three questions (b through d) were then repeated.

The results of this evaluation have been expressed in general terms in the preceding section.

3.7 Other Approaches

The situation described above is less than satisfactory. We have a method of doing what we want, provided we can obtain the right data. The most obvious source of such data is only available in heavily edited form. In this form its value is slight. If the data could be made available in unedited form (and this presents considerable difficulties) it would still not be suitable for every purpose.

One solution is to seek another data source. Probably the best would be PARs. This, too, however, presents real problems of confidentiality and propriety. Another solution is to seek an alternative method of evaluation. Another method has been proposed. We call it the method of types. It will now be explained.

3.7.1 Method of Accident Types

Clearly, many accidents have features in common with other accidents. Suppose we have a group of accidents defined by features which are obtained in the ordinary course of accident data collection. Suppose we can show that nearly all of these accidents have other features in common. Then it becomes reasonable to characterize this group as a type. This means that we can induce that they have features in common that are not observed. In particular they will have common causes. The driver errors that generated them were similar errors arising in similar circumstances. The effect of a particular device will be the same in all circumstances.

There is still a need for in-depth data related to a few ***type specimens.*** These can be used to determine what the common effect of a device is. It will not usually be sufficient to hypothesize, on the basis of the type characteristics, what the driver error is. There will be individual variations within a type, relating to varying speeds, road surface friction coefficients, curvatures, etc. These can well effect the efficiency of a device. But the quantity of such expensive data needed is now greatly reduced. The statistical reliability of the evaluation no longer depends on the size of the in-depth database.

If, therefore, types can be identified, the evaluation task may be greatly simplified. The number of types needed to cover most relevant accidents needs to be small. The volume of expensive in-depth data needed is then greatly reduced.

The restriction that the number of types covering most relevant accidents must be small is important. As the Michigan team (Campbell, et al., 1990; Massie, et al., 1991) has shown, the work needed to identify a type is significant. It may be nearly impossible to demonstrate, in practice, that an elementary type has been found. (A elementary type is one not compounded of several types.) Different kinds of searches for types may be needed for different devices. If one finishes up with many types, and for each an in-depth analysis is needed, the saving of data collection may be small. Indeed if the number of types is very large, the method of types and the in-depth-based approach studied above become the same.

In practice, therefore, one may use compound types, deliberately or accidentally. This will particularly be the case where a full in-depth analysis has been done in one set of circumstances. This might, for example, be the effect of device X on a kind of accident, which is sensitive to road surface condition in Michigan where it snows). If one then wishes to know the efficiency of the device in California, some kind of loose typing will be convenient, and probably not very inaccurate.

Another use of the word “type” is found in the work of Fontaine, et al. (1989). Here, in-depth data are used. But the author found that the majority of cases where a positive effect of some device was found were characterized by a few pre-crash situations. Naming these situations “types,” Fontaine proposed to restrict her in-depth analyses to these types. This would increase the speed of evaluation. There would be a small loss in accuracy, which would probably be dwarfed by other effects.

The approach in current work by NHTSA contractors (NHTSA, 1991) has not been fully published. It seems to be very similar to that of Fontaine, just described. One first specifies the device to be considered. One then uses the descriptors in the databases that are being used to define a class or classes of accident which can be selected by the terms in the computer index. These descriptors produce a limited class or “type. " Obviously the selection is made so that all accidents which a device may affect are in the type. After this, the NHTSA technique seems to be basically the same as the one described here. The NHTSA contractors are using the successor data to NASS, whose efficiency is discussed earlier. However they do have access to the **PARs** and interview data. The work described here suggests that there will be some success here for most devices.

SECTION 4. APPLICATIONS AND CONSEQUENCES

4.1 Overview

This brief section reviews the primary results of the work. We consider how the results may be applied. Improvement is always possible, however. We point the directions of further possible technical developments which will complement or enhance what has been done already. We indicate priorities here.

However, the results also point to the need to achieve some new departures in non-technical fields. There are managerial and institutional consequences of the need for safety in IVHS. These problems can be illuminated by what has been done. However, technical results alone cannot solve them. Here the problems are expounded in a preliminary way, but no solutions are offered.

4.2 Automated Freeways

As a result of the work reported in Section 2, we can say:

(a) It is possible to design an automated freeway which conforms to a reasonable safety criterion. Absolute safety, however is a pipe-dream. There will always be a trade-off between safety and economic performance.

(b) A method has been produced which can both assure conformity of design to a safety criterion and enable this conformity to be verified. It is practical. Validation — the assurance that what has been asked for is what is wanted — cannot be so readily assured in theory. In practice, the method should do this also.

(c) Methods similar to the one proposed are in use and are found to be practical in other industries. The managerial organization and techniques required are not in current use in highway and automobile engineering.

The cost in performance (capacity) terms of conformity to a safety criterion has not been examined. It is possible that it is large. Some of the necessary features such as fences and gates will undoubtedly affect performance. There is not likely to be a black-and-white choice, but a trade-off range. It is possible, however, that economic operation and an acceptable safety level are not compatible. No work is presently in progress in this area.

Investigation of the capacity of properly designed automated freeway systems has the highest priority.

Further, there are two directions in which further development of the methods already demonstrated would be valuable. First, the method provides a way of developing a complete specification. As it stands the completeness of the specification has not been verified. In the work of Hsu, et al. (1991), a demonstration of completeness for a subsystem was achieved. Hsu and her colleagues used computer methods to prove logically that the subsystem considered conformed to specification. Extension of their method to the whole problem will need development, which might not succeed. There are other approaches, however, and the area is in which there is a good deal of computer science development. A successful approach can probably be found.

Development of the use of "formal methods" for verification of conformity of both hardware and software systems to specification would be of great value to IVHS.

A second extension of what has already been done would make the safety criteria used more policy-oriented. At present, the methods specify a minimum number of contemporaneous, co-located independent faults which must occur before a hazard arises. A major advantage of this approach is that it points clearly to the components where reliability is important. It is a designer's aid. There is another approach, more suited to the policy problems which arise. It is to express the safety criteria in terms of casualties per year or per vehicle-mile.

This requires data not readily available. It is not just that the reliability of equipment not yet existing must be estimated. Similar equipment has been used for many years in non-highway contexts where reliability is vital. It is probable that good judgments can be made about reliability of new equipment. It is the reliability of the vehicles, used in the ways in which vehicles are used by private owners, which is the unknown factor.

This is one instance of the way in which automated freeways differ from all other large-system safety-critical technologies. A chemical complex, a nuclear power station or an aeroplane is under one professional control. One institution or person is responsible. Highways, automated or not, are multi-owner, multi-responsibility systems. Further, casualties do occur on them regularly. The accidents are scattered. The usual way of reducing casualties at the moment is by local non-systematic actions. Thus the ideas of system safety are not present in the minds of many traffic safety professionals.

With automation, however, the effects of driver errors are almost completely eliminated. Component failures loom large. Vehicle faults, which are of little consequence in accident avoidance now, become of prime importance.

There are other problems which can be foreseen in trying to use a safety criterion based on casualties per vehicle-mile. Probably there are yet others not yet foreseen. This is, however, a desirable research objective. It would aid policy decisions about management goals.

Development of methods of handling a safety criterion expressed in terms of casualties per vehicle-mile would be advantageous.

4.3 Driver Aids and Copilots

The work in Section 3 also shows that an evaluation method for AVCS-1 devices does exist. If appropriate data are available, it is practical. In North America appropriate data have not yet been found. One database (NASS) has been examined and found wanting, at least in the form in which it is available now. The current work described in NHTSA (1991) has access to the data in NASS whose excision led to some of the difficulties encountered. Some difficulties with this data will remain. Alternative methods of approach are, however, open to criticism. If the method of accident types can be developed successfully, it may well be better than the method discussed here. However, it is at best doubtful that such success can be demonstrated. It seems best to continue to try to find data.

In the author's judgment, the best approach would be to attempt to collect the required data as an extension of the present Police Accident Report system. There are alternatives including the use of some existing databases. These databases, however, are not easily reached physically from California. Any approach would need to be piloted. A method of piloting has been developed.

Several approaches, both within and without California, should be made to discover or develop appropriate crash data. The data must be oriented towards accident avoidance. (Much national crash data are currently oriented towards injury amelioration.) The data must also be sufficiently detailed to enable conclusions to be drawn about driver intentions.

Also, further development of the method of types would be very useful. This is in fact in progress at the University of Michigan by researchers experienced in the area. The work is of high priority. There is no need to try to duplicate it in California.

Both of these methods can be made more quantitative. This is desirable, since it would then become possible to make a relative evaluation of two competing instantiations of similar specifications. This could be done by development of some large computer modelling shells, which would be costly. The need is not immediate, and it would not be appropriate to give it high priority at the moment. This view would be modified if an equipment manufacturer expressed interest. It is possible that such interest will arise, for the output could be used as a design tool.

4.4 Specification of Devices and Components

Another relevant line of development would be to try to draw up achievable requirement specifications for particular AVCS-1 functions. The device may be a copilot (warning) or a driver aid (overriding). In either case we must avoid false alarms. We must also ensure that there are only very few (like one in a billion) traffic situations where the device could generate an accident. Specification of the more elaborate components of a fully-automated system is a similar problem. We have in mind here components like the longitudinal and lateral control systems on-vehicle.

In both cases, the methods which would have to be developed seem likely to combine the results found here for AVCS-1 with the results for AVCS-2. Such work could be applied in one of two ways. In the first place, any agency adopting a proactive approach in the application of AVCS needs such results. Secondly, the results will illuminate the policy debates we refer to shortly.

Development of techniques to specify components of filly automated systems is an important area. It needs to be linked with development of techniques to verify conformity to specification. Actual specifications should be one output. The methods need equally to be applied to autonomous functions like obstacle detection. Specifications should be developed here too.

4.5 Management and Policy

In Section 2.7 a description is given of parallel design and verification/validation teams. They communicate in formalized ways, which are documented. Such design methods exist in other sectors. They are complicated, slow, laborious, and costly. They are less complicated and costly than the alternative. That is to kill a lot of people before going back to the drawing board.

The introduction of this way of thinking into an existing executive organization will be a difficult managerial problem. But, in this case, who are the managers? Which is the organization? The system will have no one owner, no one operator, no one responsible institution.

Operation of automated freeway systems of this kind will require laws to be made. Some, discussed in Section 2.4, refer to system operation. Such laws affect design in a fundamental way. Others also referred to in Section 2.4, where issues like responsibility for making standards, licensing, inspection, type approval, all arise.

In both areas, there will be trade-offs between cost, capacity, safety and division of responsibilities between sectors and institutions. Existing legislators and existing officials are not experts here. A mechanism has to be found for revealing the issues.

The mechanism must also achieve equity among governmental and professional institutions, (e.g., the judiciary and the bar), a multiplicity of private-sector bodies, and travellers.

One issue that will permeate all this debate will be the issue of performance versus safety. This is reflected as the technical problem of selection of a safety criterion. Another issue will relate to the division of costs between sectors. In part this is reflected in the technical problem of the balance between vehicle-borne and infrastructure intelligence. Not every policy compromise will be achievable.

All this is not unprecedented in general terms. But every case is different. The very close relation between the policy issues and the technical ones, and the multiplicity of ownership, give this problem its own flavour.

No recommendations are offered here. The technicians are not the only party in this area. To strike a position would be counter-productive.

IVHS's ability to achieve increased safety and capacity will be limited until this set of problems has been grappled with. A final resolution is not needed today. But the questions will not go away. The clock runs.

ACKNOWLEDGMENTS

The author has received assistance, technical and otherwise from many colleagues at PATH, the University of California, and elsewhere. The support and guidance of Dr. Steven E. Shladover, Technical Director, PATH, and of Professor Pravin Varaiya, University of California, Berkeley, however, has been unfailing throughout.

REFERENCES

API 1990. "Management of Process Hazards." API Recommended Practice 750, first edition, Jan 1990. American Petroleum Institute, Washington D.C., 1990.

Broughton, J., 1988. "The Possible Effects of Future Technological Developments on Road Accidents in Great Britain. " Transport and Road Research Laboratory Report TRRL WP/RS/80. Crowthorne, England, 1988. ***Reprinted in*** Dryselius 1990, qv.

Campbell, K. L., et al., 1990. "Accident Data Analysis in Support of Collision Avoidance Technologies. " University of Michigan Transport Research Institute Report UMTRI 90-31. Ann Arbor, MI, 1990.

Chang, K-S., 1991. "Implementation of Platoon Control System." Presented at SAE Future Transportation Technology Conference. Portland, OR, Aug 1991.

Dryselius, B., (ed), 1990. "PRO-GEN Safety Group Summary Report: Estimation of the Potential Safety Effects of Different Possible PROMETHEUS Functions. " PROMETHEUS Office, Stuttgart, Germany, 1990.

Evans, L., 1985. "Risk Homeostasis Theory and Traffic Accident Data." General Motors Research Laboratories Research Publication GMR-4910. Warren, MI, 1985.

FAA 1988. "System Design and Analysis." Federal Aviation Administration Advisory Circular 25.1309-1A. Washington, D.C., 1988.

Fontaine, H., Malaterre, G. and van Elsande, P., 1989. "Evaluation de l'Efficacité des Aides à la Conduite. " Rapport Institut National des Etudes des Transports et Securité no. 85. Paris France, 1989.

Hitchcock, A., 1987. "Potential Safety Implications of the PROMETHEUS Project." Transport and Road Research Laboratory Report TRRL WP/S&T/3. Crowthome, England, 1987.

Hitchcock, A., 1988. "Road User Safety - Possible European Research Cooperation. " ***in*** "Proceedings of Roads and Traffic Safety on Two Continents in Gothenberg, Sweden, 9-l 1 September 1987." Statens Väg- och Trafik- Instituet Report VTI 328A, pp. 188-201. Linköping, Sweden 1988.

Hitchcock, A., 1991a. "Intelligent Vehicle Highway System Safety: Problems of Requirement Specification and Hazard Analysis." Transportation Research Board Annual Meeting, paper 910206. Washington, D.C., 1991.

Hitchcock, A., 1991b. "Intelligent Vehicle Highway System Safety: Approaches for Driver Aids and Copilots. " Transportation Research Board Annual Meeting, paper 910058. Washington, D.C., 1991.

Hitchcock, A., 1991c. "A Specification of an Automated Freeway. " PATH Research Report UCB-ITS-PRR-91-0808-2. University of California, Berkeley, CA., 1991.

Hitchcock, A., 1991d. "Fault Tree Analysis of an Automated Free-way." PATH Research Report UCB-ITS-PRR-91-0808-3. University of California, Berkeley, CA., 1991.

Hitchcock, A., 1991e. "Use of NASS Data for Evaluation of AVCS Devices. " PATH Research Report UCB-ITS-PRR-91-8. University of California, Berkeley, CA., 1991.

Hitchcock, A., 1991f. "Notes for a Talk on Standards and IVHS Safety." PATH Working Paper UCB-ITS-PWP-91-3. University of California, Berkeley, CA., 1991.

Hitchcock, A., 1991g. "Safety of IVHS: Methods for Determination of Accident Levels for AVCS- 1 Devices. " in Proceedings of Conference on Applications of Advanced Technologies in Transport Engineering, Minneapolis MN. American Society of Civil Engineers, New York, NY, 1991.

Hitchcock, A., 1992a. "Intelligent Vehicle Highway System Safety: A Demonstration Specification and Hazard Analysis." Transportation Research Board Annual Meeting, paper 920184. Washington, D.C., 1992.

Hitchcock, A., 1992b. "Intelligent Vehicle Highway System Safety: Use of NASS Data for Evaluation. " Transportation Research Board Annual Meeting, paper 920473. Washington, D.C., 1992.

Hitchcock, A., 1992c. "A Specification of an Automated Freeway with Vehicle-Borne Intelligence. " PATH Research Report to be published. University of California, Berkeley, CA., 1992.

Hitchcock, A., 1992d. "Fault Tree Analysis of an Automated Freeway with Vehicle-Borne Intelligence. " PATH Research Report to be published. University of California, Berkeley, CA., 1992.

HSU, A., Eskafi, F., Sachs, S., and Varaiya, P, 1991. "The Design of Platoon Maneuver Protocols for IVHS. " PATH Research Report UCB-ITS-PRR-91-6. University of California, Berkeley, CA., 1991.

Jovanis, P., Anwar, M. and Hitchcock, A., 1992. “Effect of Non-automated Accidents on Automated Median Lane Operations. " Transportation Research Board Annual Meeting. Washington, D.C., 1992.

Kletz, T. A., 1986. “Hazop and Hazan: Notes on the Identification and Assessment of Hazards. " Institution of Chemical Engineers Loss Prevention Information Exchange Scheme: Hazard Workshop Modules, 2nd ed. Rugby, England, c1986.

Marburger, E.A., Klöchner, J.H. and Stocker, U., 1990. “Estimation of the Potential Accident Reduction by Selected PROMETHEUS Functions.” *in* Dryselius 1990, qv.

Massie, D. et al., 1991. “Development of a Collision Typology for Evaluation of Collision Avoidance Strategies." Proceedings of Conference of Association for Advancement of Automotive Medicine, 38th Annual Meeting, Toronto, 1991.

Mobility 2000, 1990. “Intelligent Vehicle/Highway Systems: Report of the Working Group on Operational Benefits. " Mobility 2000, Dallas, TX, 1990.

NHTSA, 1991. “Crash Avoidance Problem Definitions/Countermeasure Technology Assessments. " National Highway Traffic Safety Administration Request for Proposals, Washington, D.C., 1991.

OECD, 1988. “Road Accidents: On-Site Investigations.” Organization for Economic Cooperation and Development Road Research Programme Report. Paris, France, 1988.

Otte, D, and Schlichtung, K.-D., 1988. “Auswertung von Ehrebungen am Unfallort im Rahmen von PROMETHEUS. " [Medical School Report], Universität Hannover, Hanover, Germany, 1988.

RTCA, 1985. “Software Considerations in Airborne Systems and Equipment Certification . " Radio Technical Commission for Aeronautics Document no. RTCA/DO-178A, Washington, D.C., 1985

Sabey, B. E., 1983. “Road Safety In the 80’s. " *in* Report of Symposium on Recent Developments in Road Safety and Remedial Measures, University of Salford, Sal ford, England, 1983.

Shladover, S. E., 1979. “Operation of Automated Guideway Transit Vehicles in Dynamically Reconfigured Platoons. " Urban Mass Trans-it Administration Report UMTA-MA-06-0085-79-1, 2 &3. Springfield, VA, 1979.

Treat, J.R., et al., 1979. “Tri-level Study of the Causes of Traffic Accidents.” Indiana University Institute for Research in Public Safety Report. Bloomington, IN, 1979

Varaiya, P., and Shladover, S. E., 1991. “A Sketch of an IVHS System Architecture.” PATH Research Report UCB-ITS-PRR-9 l-3, University of California, Berkeley, CA, 1991.

Appendix

Safety of IVHS Systems — A Bibliography

Introduction

‘The bibliography contained in this appendix was prepared as the first stage of the study of methods for the investigation of safety of Intelligent Highway/Vehicle Systems reported in the main text. The specification was narrowly interpreted. As far as possible, references which do not expressly deal with safety in some form have been excluded, although some leading papers on the safety of large distributed computer-dependent systems (especially standards) have been included.

As explained in the main report, there were, in the spring of 1990, professional librarians preparing the PATH data base. This bibliography was made available in draft. The references quoted here have been incorporated in the database. The database has been updated regularly by those responsible. This bibliography has not been updated subsequently.

Methods

Searches of computerized databases were carried out in both the USA and Europe. The primary ones were:

MELVYL — the online catalog of the University of California libraries

GLADIS — the online catalog of the libraries of the University of California at Berkeley

COMPENDEX PLUS

TRIS, Transportation Research Information System, DOT, Washington, D.C.

IRRD, International Road Research Documentation Scheme, Organization for Economic Cooperation and Development (OECD), Paris, France

British Library Technical Index

In addition, the author has included other references which he has found useful in the course of the primary study. Most of the references listed here have been viewed, and an attempt has been made to exclude material which does not refer directly to the technicalities of safety of distributed computerized systems in general, or of IVHS systems in particular. There is, for example, a large literature on the safety of (tracked) automatic guideway transit, most of which has been excluded.

Acknowledgements

This work has been very much aided by the Librarians, Catherine Cortelyou (Public Services, ITS Library) and Seyem Deus Petrites (PATH Database Coordinator).

1. Anon. ***Vehicle Automation - Principles of Automatic Systems.*** Transport and Road Research Laboratory Leaflet TRRL-LF-265, Crowthorne, 1971.

2. Anon. Taking the human error out of driving. ***Commercial Motor.*** London, 1974.

3. Anon. Antilock Brakes: The European Experience. ***The Private Carrier.*** Vol. 25, No. 10. October 1988, pp. 24-27.

4. Battelle Institute. *Independent* ***Assessment*** *of* ***Safety Aspects of an Automated Mixed Traffic Transit System: Final Report.*** UMTA-OH-06-0030-82- 1. Springfield, Va., 1982.

5. Bateman, W. ***Vehicle On-Board Navigation Systems.*** Institute of Electrical Engineers, Colloquium on Vehicle Route Guidance, IEE 1985/11, London, 1985.

6. Bernstein, H., & Schnitt, A. Emergency Strategies for Safe Close-Headway Operation of PRT Vehicles. ***Personal Rapid Transit.*** University of Minnesota, Minneapolis, 1972, pp. 352-360.

7. Blikman, G. A New Method for Traffic Safety Research on Driver Distraction. ***Traffic Safety Theory and Research Methods.*** Amsterdam 88, SWOV, Leidschendam, 1988.

8. British Standards Institute. ***Draft British Standard: Functional Safety*** *of* ***Programmable Electronic Systems: Generic Aspects.*** BSI 89133005 DC, London, 1989.

9. British Standards Institute. ***Draft British Standard: Software*** *for* ***Computers in the Application of Industrial Safety-Related Systems.*** BSI 89133006 DC, London, 1989.

10. Broughton, ***J. Possible Effects*** *of* ***Future Technical Developments on Road Accidents in Great Britain,*** Transport and Road Research Laboratory, TRRL-WP/RS/80, Crowthorne, 1989.

11. Brus, E. Vehicular Radar - The Ultimate Aid for Defensive Driving. ***Microwaves and RF.*** Vol. 26, 1987, pp. 53-54.

12. Cardew, K.H.F. ***The Automatic Steering*** *of* ***Vehicles - An Experimental System Fitted to a DS 19 Citroen Car.*** Transport and Road Research Laboratory, TRRL-LR-340, Crowthorne, 1970.

13. Chipperfield, J.L. Inductive Loop Based Guidance System. ***Znstitute*** *of* ***Electrical Engineers Colloquium: Vehicle Route Guidance.*** IEE 1985/1 1, London, 1985.

14. Colson, C.W., Shroder, R.J., & Chapman, W.B. ***Advanced Group Rapid Transit Odometer Data Downlink Collision Avoidance System Design Summary.*** UMTA-CA-06-0088-80-1, Springfield, Va., 1979.

15. Courage, K., & Hauer, C. ***Integration of Systems Under Development.*** DOT-FH- 1 l-6373, Springfield, Va., 1973.

16. Dacker, D. ***Development of an On-Line National Route Guidance System.*** Institute of Electrical Engineers, Colloquium on Vehicle Route Guidance, IEE 1985/11, London, 1985.

17. Dauber, R.L. ***Passenger and Convenience Services in Automated Guideway Transit.*** DOT-TSC-UMTA-79-48-I and -11, Springfield, Va., 1979.

18. Dewar, R.E. In-Vehicle Information and Driver Overload. ***International Journal of Vehicle Design.*** Vol. 9, Geneva, 1988, pp. 557-564.

19. Dhalluin, J.F., Gabillard, R., & Koursi, M.E. Microprocessors Applied to the Control of Safety Processes. ***Récherches Transports Securité,*** English issue, No. 2, September 1987, Paris, pp. 13-18.

20. Dobias, G. La Voiture Intelligente: Un Plus pour la Securité Routière? ***Recherches Transports Securité, No.*** 15, September 1987, Paris, pp. 13-18.

21. Dobson, J.S., Penoyre, S., & Stoneman, B.G. Automatically Controlled Vehicles. ***Control of Guided Land Transport.*** Institute of Electrical Engineers, Conference Publication 117, London, 1974, pp. 138-145.

22. Dobson, J.S. ***Improvements in Vehicle Guidance Systems.*** UK Patent Specification 1 459 788. London, 1973.

23. Dobson, J.S., Allard, R., & Ford, R.L. An Automatic Headway Control System Based on the Use of a Microwave Telemetry Link. ***Institute of Electrical Engineers International Conference on Automobile Electronics*** IEE Conference Publication 141, London, 1976, pp. 96-159.

24. Domann, H. An Automatic Guidance System for Road Vehicles. ***Institute of Electrical Engineers International Conference on Automobile Electronics*** IEE Conference Publication 141, London, 1976, pp. 96-159.

25. Ervin, R.D., & Chen, K. Toward Motoring Smart. ***National Academy of Science, Issues in Science and Technology, Vol 5.*** Washington, D.C., 1988, pp. 92-97.

26. Farber, B.C., Farber, B.A., & Popp, M. Evaluation Methods for Traffic Safety Aspects of New Technologies in Vehicles. ***Traffic Safety Theory and Research Methods.*** SWOV, Leidschendam, 1988.

27. Fancher, P.S. ***European/Australian Experience With Antilock Braking Systems in Fleet Service.*** DOT-HS-807-269, Springfield, Va., 1988.

28. Finnie, B.W. Design for Safety. ***Safety-Critical Software in Vehicle and Traffic Control.*** Institute of Electrical Engineers, IEE 1990/031, London, 1990.

29. Finnie, B.W. The Introduction of New Methods for Assuring Safety into the Software Development Process. ***Safety-Critical Software in Vehicle and Traffic Control.*** Institute of Electrical Engineers, IEE 1990/031, London, 1990.

30. Foote, R.S. Automatic Vehicle Identification. ***Traffic Engineering and Control.*** Vol. 15, 6, London, 1973.

31. Frank, L.H., Gasall, J.S., & Wierville, W.W. Effects of Visual Display and Motion System Delays on Operator Performance and Uneasiness in a Driving Simulator. ***Human Factors.*** Vol. 30, 1988, pp. 201-217.

32. Frobose, H.J., & Kuchenbecker, A. Verkehrssicherrheit und Massenmedien. ***Verne Congrès - L'Insecurité Routière.*** Atec, Paris, 1986.

33. Garrard, W.L. State-of-the-Art of Longitudinal Control of Automated Guideway Transit Vehicles. ***High Speed Ground Transportation Journal.*** Vol. 12, 2, New York, 1978, pp. 35-67.

34. Glauz, W.D. ***An Ice and Snow Detection and Warning Feasibility Study.*** FH-11-7428, Springfield, Va., 1971.

35. Goode, A.P. Some Research Towards Automation in Traffic Control. ***Traffic Engineering and Road Safety, A Special Issue*** *of* ***Traffic Engineering and Control.*** London, 1979, pp. 46-50.

36. Gullstrand, T.R. PROMETHEUS. ***International Journal*** *of* ***Vehicle Design.*** Vol. 10, 4, Geneva, 1989, pp. 428-431.

37. Hahlganss, G. Headway Radar Using Pulse Techniques. ***Institute*** *of* ***Electrical Engineers International Conference on Automobile Electronics.*** IEE Conference Publication 141, London, 1976, pp. 96-159.

38. Han, L.D., & May, A.D. ***Artificial Intelligence Approaches for Urban Network Incident Detection and Control.*** Institute of Transportation Studies, University of California, Berkeley, CA, 1989.

39. Harms, P.L., & Johanessen, R. Radiating Cable Performance for Use With a Driver Information System. ***Institute of Electrical Engineers International Conference on Automobile Electronics.*** IEE Conference Publication 141, London, 1976, pp 96-159.

40. Harris, W.J., & Bridges, ***G.S. (Eds.). Proceedings of a Workshop on Intelligent Vehicle/Highway Systems by Mobility 2000.*** Texas A&M University, Austin, Texas, 1989.

41. Hathaway, W.T. ***Development of a Graphics Based Automated Emergency Response System (AERS) for Rail Transit Systems.*** UMTA-MA-06-0178-89-1, Springfield, Va., 1989.

42. Hinman, E.J., & Pitts, G.L. Practical Safety Considerations for Short-Headway Automated Transit Systems. ***Personal Rapid Transit II.*** University of Minnesota, Minneapolis, 1974, pp. 375-380.

43. Hitchcock, A., & Sedgfield, H.B. Guided Buses on Segregated Ways. ***Conference on Rapid Transit vehicles for City Services.*** Paper No. 5. Institute of Mechanical Engineers, London, 1972.

44. Hitchcock, A. ***Potential Safety Implications of the PROMETHEUS Project.*** Transport and Road Research Laboratory Report TRRL WP/S&T/3, Crowthorne, 1987.

45. Hitchcock, A. Road User Safety - Possible European Cooperation. ***Roads and Traffic Safety on Two Continents.*** VTI, 328A Linköping, 1988, pp. 188-201.

46. Hodgson, D.B. Time Compressed Aural Communication Links to Moving Vehicles. ***Institute of Electrical Engineers International Conference on Automobile Electronics.*** IEE Conference Publication 141, London, 1976, pp. 96-159.

47. Holscher, H. & Rader, J. ***Microcomputers in Safety Techniques.*** Verlag TÜV Bayern, Munich, 1986.

48. International Electrotechnical Commission. ***Draft - Functional Safety of Programmable Electronic Systems: Generic Aspects.*** IEC SC65A WG10, Geneva, 1990.

49. International Electrotechnical Commission. ***Draft - Software for Computers in the Application of Industrial Safety-Related Systems.*** IEC SC65A WG9, Geneva, 1989.

50. Imbaeu, D.; Wierwille, W.W., & Wolf, L.D. Effects of Instrument Panel Luminance and Chromaticity on Reading Performance and Preference in Simulated Driving. Human ***Factors.*** Vol. 31, No. 2, April 1989, pp. 147-160.

51. Institute of Electrical Engineers. ***The Car and Its Environment - What DRIVE and PROMETHEUS Have to Offer.*** Colloquium programme presentations. IEE 1990/20, London.

52. International Road Federation. Electronic Route Guidance System Tested Successfully in Tokyo. ***World Highways,*** Vol. 30, p. 2. Washington, D.C., 1987.

53. Jeffrey, D.J. ***Potential Benefits of Route Guidance.*** TRRL LR-997, Crowthome, 1981.

54. Jeffrey, D.J. Road/Vehicle Electronic Communication. ***15th International Study Week - Traffic Engineering and Safety,*** Venice World Touring & Automobile Association, London, 1985.

55. Jeffrey, D.J., Russam, K., & Robertson, D.I. Electronic Route Guidance by Autoguide: The Research Background. ***Traffic Engineering & Control,*** Vol. 28, No. 10, 1987, pp. 525-529.

56. Jesty, P.H., Buckley, T.F., & Hobley, K.M. DRIVE Project V1051 - Procedure for Safety Submissions for Road Transport Informatics. ***Safety-critical Software in Vehicle and Traffic Control.*** IEE 1990/03 1, London, 1990.

57. Koboyashi, T. Human Factors in Driving. ***International Journal of Vehicle Design,*** Vol. 9, Geneva, 1988, pp. 586-599.

58. Koh, K.H., & Lew, S.C. Drives - A Low Cost Retrofittable Module for Enhanced Vehicular Safety and Driver Information. ***International Journal of Vehicle Design,*** Vol. 10, No. 5, Geneva, 1989, pp. 553-559.

59. Levenson, N. Software Safety: Why, What, and How. ***Computing Surveys,*** Vol. 10, 1988, pp. 125-163.

60. Lobsinger, D. An Analysis of Minimum Safe Headway for No Collisions. ***Personal Rapid Transit ZZ,*** Minneapolis, Minnesota: University of Minnesota, 1974, pp. 391-398.

61. Lum, L., Kinney, L.L., & Kumar, K.S.P. Feasibility of a Distributed Computer Traffic Control System. ***Fourth IFAC/IFIP/IFORS Conference,*** Baden-Baden, DBR. Oxford: Pergamon Press, 1983.

62. McGean, T:J. Headway Limitations for Short-Term People Mover Programs. ***Personal Rapid Transit II***, University of Minnesota, Minneapolis, 1974, pp. 349-354.

63. Malaterre, M., Fontaine, H., & van Elstande, W. ***Evaluation de l'efficacité potentielle des aides à la conduite.*** INRETS 85, Paris, 1989.

64. Milward, J. System Architectures for Safety-Critical-Automotive Applications. ***Safety-Critical Software in Vehicle & Traffic Control.*** IEE 1990/031, London, 1990.

65. Moody, R.L. Automatic Control Speed System for Vehicles. ***International Conference on Automobile Electronics.*** IEE Conference Publication 141, London, 1976, pp. 96-159.

66. Moon, A. Vehicle Control Systems - Reliability through Simplicity. ***Safety-Critical Software in Vehicle & Traffic Control.*** IEE 1990/031, London, 1990.

67. Mounce, M. ***Summary of Traffic Control Guidelines for Major Incident Response.*** Texas Transportation Institute (Texas A&M University), Research Report 410-7F, College Station, Texas, 1986.

68. NATO. ***NATO Materiel Configuration Management Policy.*** Report No. STANAG 4159, Brussels, 1984.

69. Nissan Motor Company. ***Nissan Installed Head-up Display on the New Silvia.*** Nissan Motor Company Ltd., Tokyo, 1988.

70. Noy, Y.I. Human Factor Considerations in the Design of Intelligent Automobile Displays. (Project due for completion in 1988, Transport Canada). ***Index of Research in Progress,*** International Road Research Documentation Scheme (IRRD) OECD, Paris, 1985.

71. Olsen, C.L., Fuller, G.H., & Fling, R.B. Some Reliability, Dependability and Safety Considerations for High-Capacity PRT Systems. ***Personal Rapid Transit III.*** University of Minnesota, Minneapolis, 1976, pp. 465-473.

72. Panizza, E. New Concepts for Body Electronics. ***XXI FISITA Congress, Yugoslav Society of Auto Engineering.*** Vol. 3, Belgrade, 1986, pp. 113-115.

73. Papageorgiou, M., & Schmidt, G. Freeway Traffic Modelling and Control. ***Fourth IFAC/IFIP/IFORS Conference, Baden-Baden, DBR.*** Pergamon Press, Oxford, 1983.

74. Papp, I. Safety Messages and Information Consumption. ***Vème Congrès - L'Insecurité Routiere.*** Atec, Paris, 1986.

75. Parey, C., & Lauer, A. La Voiture Intelligente. ***La Récherche,*** Vol. 190, pp. 46-*55* Paris, 1987.

76. Parsons, R.E. Program on Advanced Technology for the Highway (PATH). ***ASCE Conference, San Francisco 1989.*** ASCE, New York, NY, 1989.

77. Penoyre, S., Feaver, J.L., & Stoneman, B. A Drive-by-Wire Vehicle Control System for Severely Disabled Drivers. ***International Conference on Automobile Electronics, ZEE.*** Conference Publication 141, London, 1976, pp. 96-159.

78. Penoyre, S. A Robot in the Driver's Seat. ***New Scientist and Science Journal,*** Vol. 50, London, 1971, pp. 371-372.

79. Pfafferott, I. Fahrzeugwerbung in den Medien - ein Problem für die Verkehrssicherrheit? ***Vème Congrès - L'Insecurité Routière.*** Atec, Paris, 1986.

80. Posch, B., & Schmidt, G. A Comprehensive Control Concept for Merging of Automated Vehicles under a Broad Class of Traffic Conditions. ***Fourth IFAC/IFIP/IFORS Conference, Baden-Baden, DBR.*** Pergamon Press, Oxford, 1983.

81. PROMETHEUS Secretariat. ***PROMETHEUS: Programme for a European Traffic with Highest Efficiency and Unprecedented Safety: A Concentrated Program*** *of* ***Basic and Product-Oriented Research in the Areas*** *of* ***the Eureka Research Programme.*** Stuttgart, 1987.

82. Pue, A.J. Implementation Trade-Offs for a Short-Headway Vehicle-Follower Automated Transit System. ***IEEE Transactions on Vehicle Technology,*** Vol. VT-*28,* 1, pp. 46-55, New York, NY, 1979.

83. Queree, C. Toepassingen van Informatie-en Telecommunicationtietechnologie op Verkeers-veiligheid (Applications of Information and Telecommunication Technology to Road Safety). ***Colloquium Vervoersplanologisch Speurwerk, Vol. 2,*** pp. 617-636. Delft, 1986.

84. Radio-Technical Commission on Aeronautics. ***Procedures*** *for* ***Safety-Critical*** *Software.* D-0178A, Washington, D.C., 1986.

85. Reed, W. Safety-Critical Software in Traffic Control Systems. ***Safety-Critical Software in Vehicle & Traffic Control.*** IEE 1990/031, London, 1990.

86. Rémy, C. Quand l'Automobile Devient Intelligente. ***Micro Systèmes,*** Vol. 82, Paris, 1988, pp. 111-112.

87. Richardson, D.J., & Clarke, L.A. Partition Analysis: A Method Combining Testing and Verification. ***Transactions on Software Engineering.*** IEE Publication SE-11, pp. 1477-1490, IEE, London, 1985.

88. Roberts, N.H., et ***al. Fault Tree Handbook.*** U.S. Nuclear Regulatory Commission, NUREG-0492, Washington, D.C., 1981.

89. Rockwell, T.H. Spare Visual Capacity in Driving Revisited: New Empirical Results for ***an*** Old Idea. ***Second Conference on Vision in Vehicles, Nottingham, Vol*** 2. pp. 317-324. Elsevier Science, Amsterdam, 1988.

90. Rodwell, J. Driverless Bus Nears Reality. ***Commercial Motor,*** London, 1974.

91. Ross, G.F., Cronson, H.M., & Rama Rao, B. New Collision Avoidance System Using Baseband Reflectometry. ***Proceedings of the 8th European Microwave Conference, Paris*** pp. 594-597. Microwave Publications, Sevenoaks, 1978.

92. Rouse, W.B., & Morris, N.M. Conceptual Design of a Human-Error-Tolerant Interface for Complex Engineering Systems. ***Analysis, Design and Evaluation of Man-Machine Systems - IFAC/IFIP/IFORS Conference,*** pp. 281-286. Pergamon Press, Oxford, 1985.

93. Rumar, K. PROMETHEUS Man-Machine Interface. (Project due for completion in 1991, VTI, Linköping). ***Index of Research in Progress,*** International Road Research Documentation Scheme (IRRD) OECD, Paris, 1988.

94. Rumar, K. In-Vehicle Information Systems. ***International Journal of Vehicle Design,*** Vol 9, pp. 548-556, Geneva 1988.

95. Schumacher, P. Vehicle Longitudinal Control and Reliability Project. ***Vol. 3 - Longitudinal Control Analysis and Design. Parts A and B.*** UMTA-IT-06-0148-79-7 & 8. Springfield, VA, 1979.

96. Schuesler, R. Looking without Seeing. ***Traffic Safety,*** Vol. 90, 1990, pp. 16-17.

97. Shladover, S.E. Dynamic Entrainment of Automated Guideway Transit Vehicles. ***High Speed Ground Transportation Journal,*** Vol. 12, 3, New York, NY, 1978, pp. l-27.

98. Shladover, ***S.E. Operation of Automated Guideway Transit Vehicles in Dynamically Reconfigured Trains and Platoons.*** UMTA-MA-0085-06-79- 1, 2 & 3. Springfield, VA, 1979.

99. Shladover, S.E., & Parsons, R.E. ***Safety Issues for Intelligent Vehicle/Roadway Systems.*** Paper presented at ASME Winter Annual Meeting, ASME, San Francisco, 1989.

100. Spreitzer, D.A. ***Technology, Vehicles, Highways and Future Transportation.*** GMR-6878, General Motors, Warren, MI, 1989.

101. Thibault, H.B., & Dhalluin, J.F. On Safety Regulations for New Transport Modes by Means of Quantified Objectives. ***Récherches Transports Securité,*** English Issue, No. 3, Paris, 1988.

102. Thompson, R.E. ***Safety and Reliability of Automated Guideway Transit Systems: Final Report.*** UMTA-OH-06-0028-82-l. Springfield, VA, 1982.

103. Thompson, R.E. Safety Considerations for Automated Mixed Traffic Transit (AMTT) Systems. ***Journal of Advanced Transportation,*** Vol. 17, 2, New York, NY, 1983, pp. 103-118.

104. Tran, S., Marks, K., & Cullyer, W.J. On the Development of High Quality Software Design Methodology for Automotive Applications. ***Safety-Critical Software in Vehicle & Traffic Control.*** IEE 1990/031, London, 1990.

105. UK Health and Safety Executive. ***Programmable Electronic Systems in Safety-Related Applications - Parts 1 & 2: Generic Aspects.*** HMSO, London, 1987.

106. UK Ministry of Defence. ***Requirements for the Analysis of Safety-Critical Hazards.*** Interim Defence Standard DEFSTAN 00-56, Glasgow, 1988.

107. UK Ministry of Defence. ***Requirements for the Procurement of Safety-Critical Software in Defence Equipment.*** Interim Defence Standard DEFSTAN 00-55, Glasgow, 1988.

108. UK Ministry of Defence. ***Configuration Management Policy and Procedures for Defence Materiel.*** DEFSTAN 05-57 Issue 2, Glasgow, 1985.

109. U.S. Congress Office of Technology Assessment. ***Advanced Vehicle/Highway Systems and Urban Traffic Problems,*** Washington, D.C., 1989.

110. U.S. Department of Defense. ***Procedures for Performing a Failure Mode, Effects and Criticality Analysis.*** MIL-STD-1629A, Washington, D.C., 1980.

111. Verwey, W.B., & Janssen, W.H. Driving Behaviour with In-Car Navigation Aids. ***Road Safety in Europe,*** Vol. 1, VTI, Linköping, 1988, pp. 85-97.

112. Willis, D.K. IVHS Technologies: Promising Palliatives or Popular Poppycock? ***Transportation Quarterly,*** Vol. 44, No. 1, Westport, Ct., 1990, pp. 73-84.

113. van Winsum, W. ***Mental Workload of Car Driving,*** Report No. NVK-8, U. Grönigen, 1987.

114. Wootton, J. The Benefits from Improving the Quality of Information Given to Drivers. ***15th International Study Week - Traffic Engineering and Safety, Venice.*** World Touring Association and Automobile Association, London, 1985.

115. Zemlin, H., Dauper, H., Fricke, H., & Schild, G.H. Safety Requirements for Automated Guideway Transit Systems I, II. ***High Speed Ground Transportation Journal,*** Vol. 12, No. 2, New York, 1978, pp. 69-91.

116. Zwahlen, H.T., Adams, C.C., & Debald, D.P. Safety Aspects of CRT Touch Panel Controls in Automobiles. ***2nd Conference on Vision in Vehicles.*** Vo12. pp. 335-344. Elsevier Science, Amsterdam, 1988.