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

Methods of Analysis of IVHS Safety Executive Summary

Anthony Hitchcock

PATH Research Report
UCB-ITS-PRR-92-13

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.

December 1992

ISSN 1055-1425

Methods of Analysis of IVHS Safety

Executive Summary

This report is part one of the final report of the PATH Program's project MOU (Memorandum of Understanding) 19 — "Methods of Analysis of IVHS Safety. " 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 principal individual tasks were:

- Specification and analysis of hazards in AVCS-2/3 systems (Automated Freeways)

  a) Development of techniques
  b) Investigation and demonstration of techniques: System #1
  c) Investigation and demonstration of techniques: System #2

- Methods of analysis of AVCS-1 Systems (Driver Aids and Copilots)

- Communication of results to industry, administration, etc.

- Final report.

Data collection was expressly excluded from the work.

In part two of this report, a number of recommendations regarding problems which need solution are made. Here, however, we refer only to recommendations affecting action now.

Safety Considerations for Automated Freeways

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 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 people killed and injured is likely to be large. Design must 'be such that accidents are very infrequent. It is of course impossible to design so that accidents will never occur. It will always be possible to imagine some combination of simultaneous unrelated faults which will cause a catastrophe.

A first, obvious 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.

Therefore, 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 must also 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, in theory, 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, it has been demonstrated, for two separate designs, that neither admits casualties, even if 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 used in other fields.

The first example system was chosen to have one automated lane on a freeway with other lanes devoted to ordinary traffic. It has most of the intelligence 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 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. It was judged that it would be easier to find a safe system if we started with infrastructure-based intelligence.

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 intended to maintain continued operation, with safety, in the presence of faults.

In the present work, therefore, the first step was to complete the design. Then safety could be tested. It turns out that it is possible to design a safe system with mainly vehicle-borne intelligence. A small amount of intelligence in the infrastructure is, however, necessary for both normal operation and safety.

Some special physical infrastructure is, however, necessary. We prove quite generally that it is necessary for safety that each automated lane be separated from any other automated lanes, and from the rest of the freeway, by a small barrier or "fence." If this is not done, then some 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 spin-offs. One has just been mentioned — there are designs for automated freeways which are safe. Another arises from the recognition that, when designing for real, it would be unwise 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, 1991a; 1991b; 1992a; 1992b) so that this project's work does conform to its own recommendations. Reference can be made to this very detailed material. It is not suitable for this summary or for part two of this report.

As a result of the work on automated freeways, 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.

What has not been shown is that the economic cost of conformity to a safety criterion is not excessive. The concern here is more about loss of performance (capacity) than about money. Some of the necessary features such as fences and gates will undoubtedly affect performance. This situation is basic to the whole development of automated freeways.

Investigation of the capacity ofproperly designed automated freeway systems should have the highest priority.

Safety Considerations for Driver Aids and Copilots

PATH is also concerned with other aspects of IVHS, and 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 assist the choice among different designs of the same concept. A further question which will arise is whether there is a need for governmental regulation, approval, or licensing of devices. Good evaluations will help to answer this question too. Then, if that is the decision, evaluations are 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 the U.S.A.

"In-Depth" Data. As used in Europe, 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. problems is not appropriate here. Accident patterns are very different in Europe and the U.S.A. There are three possible solutions to this problem:

(a) Other data, available in the U.S.A., can be sought. The data-sets can then 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 attempt. The line is promising. If Campbell's 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 foreseen which this data could uniquely satisfy. However, that is not yet the case. This possibility will not be discussed further.

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. The National Highway Traffic Safety Administration's (NHTSA) National Accident Sampling System (NASS) seemed a reasonable alternative, and access to the raw data was arranged. A method was proposed for determining whether this 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. The current work described in NHTSA (1991) has access to the data in NASS whose excision led to some of the difficulties encountered.

Management and Policy Issues

In part two we discuss the need for parallel design and verification/validation teams. The teams 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.

Furthermore, operation of automated freeways will require new laws to be made. Some will refer to system operation. They will affect design from the beginning. Others are yet more fundamental. Issues like responsibility for making standards, licensing, inspection, and type approval all arise.

In both areas there will be trade-offs among cost, capacity, and safety. In each there will be divisions of responsibilities among 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 lawyers), 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 relationship between the policy issues and the technical ones, and the multiplicity of ownership, give this problem its own flavour.

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.

Conclusions

Conclusions of the work are summarized here. This very brief section inevitably simplifies them somewhat.

A. Automated freeways

1. It is possible to design an automated freeway which meets rational safety criteria. However, it is not possible to design one which is injury free. Such injury accidents as may occur are likely to be spectacular and involve multiple casualties.

2. A technique (complete specification and fault tree analysis) has been demonstrated which makes it possible to ensure that a design meets the safety criterion chosen. This technique requires a particular organization of design work, and the participation of an independent verification and validation (V & V) team on an equal basis in the design work.

3. Safety considerations will constrain design very considerably. In particular, automated lanes will need to be separated by (perhaps calf-high) fences, with gaps ("gates") to permit lane-changing.

B. Safety-related autonomous devices

1. Techniques are described which enable an estimate to be made of the net safety impact of devices (e.g. "collision avoidance"). They require databanks of kinds not readily available in North America.

2. Some databases relevant to U.S.A. conditions have been examined for suitability for this purpose. Results were mixed. Other possibilities are identified.

3. The extent to which one or a group of such devices would cause accidents because of faults or poor design can be determined by techniques described. V & V procedures are necessary here.

Recommendations

1. Safety considerations should constrain the design of AHS systems. The extent to which research or development should proceed on systems which do not wholly meet the constraints, when known, should be considered. Research is needed on some topics, such as the design of fences, arising from this work.

2. Research is needed to decide if both economic capacity and driver acceptance is attainable within realistic constraints arising from safety and other considerations.

3. The present work should be extended to enable safety levels to be estimated quantitatively. It should also be extended to admit a satisfactory method of formal specification of modules and subsystems, and formal, computerized methods for analyzing conformity to specification.

4. All this implies an agreed procedure for V & V within the IVHS community.

References

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.

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

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

Hitchcock, A., 1991b. "Fault Tree Analysis of an Automated Freeway." PATH Research Report UCB-ITS-PRR-9 l-0808-3. University of California, Berkeley, CA., 199 1.

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

Hitchcock, A., 1992b. "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 D, P, 1991. "The Design of Platoon Maneuver Protocols for IVHS." PATH Research Report UCB-ITS-PRR-91-6. University of California, Berkeley, CA., 1992.

Marburger, E.A., Klöchner, J.H. and Stocker, U., 1990. "Estimation of the Potential Accident Reduction by Selected PROMETHEUS Functions." *in* "PRO-GEN Safety

Group Summary Report: Estimation of the Potential Safety Effects of Different Possible PROMETHEUS Functions", PROMETHEUS Office, Stuttgart, 1990.

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.

7000\7400