This paper has been mechanically scanned. Some errors may have been inadvertently introduced.
Fault Tree Analysis of an Automated Freeway with Vehicle-Borne Intelligence

Anthony Hitchcock

UCB-ITS-PRR-92-15

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 10551425
CONTENTS

1. Introduction 1
2. The System Considered 2
   2.1 Architecture 2
   2.2 Manoeuvres 4
3. Hazard Analysis 5
4. Fault Trees 6
5. Analysis and Results 8
6. Discussion 9
   6.1 Safety of Alternative Concepts 10
Acknowledgments 11
References 12

APPENDIXES

Hazard A A.3
   Line A A.3
   Line B A.7
   Line C A.9
   Line D A.12
   Line E A.16
   Line F A.22
Hazard B A.26
Hazard C A.28
Hazard D A.29
GLOSSARY OF TERMS

In the text and the appendixes some terms of art, previously defined, are employed. Below is a set of section references to the definitions. For other terms, reference should be made to Hitchcock (1992c).

<table>
<thead>
<tr>
<th>Term</th>
<th>Section</th>
</tr>
</thead>
<tbody>
<tr>
<td>AL — automated lane</td>
<td>2</td>
</tr>
<tr>
<td>CA — closed-ahead, mode (see Hitchcock, 1992c)</td>
<td>2</td>
</tr>
<tr>
<td>fence</td>
<td>2</td>
</tr>
<tr>
<td>follower</td>
<td>2.2</td>
</tr>
<tr>
<td>foreseen hazard</td>
<td>4</td>
</tr>
<tr>
<td>free agent</td>
<td>2.2</td>
</tr>
<tr>
<td>gate</td>
<td>2</td>
</tr>
<tr>
<td>lateral guidance reference</td>
<td>2</td>
</tr>
<tr>
<td>leader</td>
<td>2.2</td>
</tr>
<tr>
<td>manual spacing</td>
<td>2.2</td>
</tr>
<tr>
<td>NE — no-entry mode (see Hitchcock, 1992c)</td>
<td></td>
</tr>
<tr>
<td>platoon spacing</td>
<td>2.2</td>
</tr>
<tr>
<td>responder</td>
<td>2.1</td>
</tr>
<tr>
<td>SA — slow ahead mode (see Hitchcock, 1992c)</td>
<td></td>
</tr>
<tr>
<td>TL — transition lane</td>
<td>2.1</td>
</tr>
<tr>
<td>turning-point</td>
<td>2.1</td>
</tr>
<tr>
<td>UL — unconcerned lane</td>
<td>2.1</td>
</tr>
<tr>
<td>VPD — vehicle presence detector</td>
<td>2.1</td>
</tr>
<tr>
<td>V &amp; V — verification and validation</td>
<td>1</td>
</tr>
</tbody>
</table>
Fault Tree Analysis of an Automated Freeway with Vehicle-Borne Intelligence

1. INTRODUCTION

This paper is not complete in itself. The background is discussed in “Methods for Analysis of IVHS Safety: Final Report of MOU 19” (Hitchcock, 1992a). Readers not familiar with the area are strongly advised to read the other report first. Yet shorter accounts of the background are found in Hitchcock (1991a) and Hitchcock (1992b). Further, in this paper an automated freeway is the subject of a fault tree analysis. That automated freeway is specified in full in Hitchcock (1992c). As is made clear in Hitchcock (1992c), that design is a completion of a partial system design due to Hsu, et al. (1991).

It is explained in these other papers, notably Hitchcock (1992a), that the whole project has been devoted to the derivation of a method for designing automated freeways in a manner which conforms to pre-set safety criteria. Further the method goes on to provide means by which the design can be verified to conform to specification. Finally the method also makes it possible, to a degree, to validate the specification, showing that the specification does indeed conform to what is wanted. The process, in the whole work, by which the efficiency and practicality of the proposed method is demonstrated, is by example. Two very different designs of automated freeway have been specified, and the V & V (verification and validation) method has been applied to both. That V & V method is called fault tree analysis.

This paper describes the fault tree analysis of the second example design. This design is characterized by extreme emphasis on vehicle-borne intelligence, and by the presence of a multiplicity of automated lanes. It is a platooned system. At the end of this paper there is a brief discussion of the relative merits of vehicle-based and infrastructure-based intelligence, mainly from the viewpoint of safety.

The analysis starts with definition of the hazards to be avoided. Here a hazard is defined as a precursor to a condition in which one further failure could lead to a catastrophe. A catastrophe is a high-delta-V collision between platoons. In such a collision multiple deaths and injuries are likely. The qualitative safety criterion chosen is that two independent failures should have to occur before a catastrophic hazard arises. This means that three near-simultaneous independent failures are necessary to cause a high-delta-V collision.

In the end, such criteria should be quantitative. Estimates would be made of the frequency of catastrophes. Alternatively, estimates would be made of the reliability required to make this frequency small enough. This would require data on reliability of existing system components. These includes tires, automatic transmissions, and vehicle presence detectors. Such data is not immediately available. Research on this topic is planned. In the meantime the present qualitative analysis can reveal whether or not a design concept is basically sound. The analysis points the way to the critical items for quantitative analysis.
2. THE SYSTEM CONSIDERED

The system which has been put together to demonstrate a fault tree analysis in this example has many automated lanes (ALs). Down the centre of each AL runs a lateral guidance reference, which is used by the vehicle-borne lateral control system to maintain vehicles on track. The ALs are separated from each other by barriers called fences. In the fences there are gaps to enable vehicles to change lanes. These are called gates. At each gate there is a vehicle presence detector (VPD) on the lane to which the lane-change is made. The signal from the VPD is one of the influences on an active turning-point near the gate on the lane from which vehicles leave. (Two-way gates, if the system is designed that way, have VPDs and turning points, separately controlled, in both lanes.) The turning point, when activated, provides a reference for the start of the change-lane manoeuvre. If the turning-point is not activated, no vehicle will change lane.

For control purposes the system is divided into lengths of some 1 to 5 miles in length called blocks. As each AL enters a new block there is a reference point which enables a vehicle-borne odometer to be zeroed. The combination of odometer reading, block# and lane# define the position of vehicle on the system. We call this data record the vehicle’s loc. Entry and exit are from a lane, the transition lane or TL, running parallel to the ALs for part of their length. The VPD on the TL by an exit gate is unusually long, so that the system can distinguish the presence of vehicles here for some longer interval. In this discussion it is usually unnecessary to consider whether there are other unconcerned lanes (ULs) which contain manually controlled vehicles running parallel to ALs and TL. Occasionally we do mention this possibility, when it becomes important, as for example happens when one is concerned with the possibility that a vehicle bearing an external load may legally be present on the TL. If the TL is for access and egress to and from the ALs only, no such vehicle should be present, for external loads are not legally permitted on the ALs.

2.1 Architecture

Figure 1 presents a general diagram of the system architecture. This is based on an original proposal by Varaiya and Shladover (1991). The regulatory layer contains the basic vehicle-borne control systems which enable a vehicle to remain on track, keep position in a platoon, keep a record of its loc and communicate with other vehicles. The regulatory layer also contains sensors, and, in particular, a forward sensor. The forward sensor will detect the distance to a vehicle ahead in the same lane and its relative speed at a range greater than the normal separation of platoons as well as at the short in-platoon spacing. It is not clear in the specification whether this instrument requires an active element on the vehicle perceived. In the analysis, the point is left open. Where such an active element is discussed it is called a responder. The regulatory level also contains a self-monitor, which is continually testing the operation of the vehicle and its controls. If a fault is detected a fault flag is set.

The platoon layer is again largely on-vehicle. It includes a general supervisor, which organizes the protocols for the various manoeuvres, and a vehicle-borne state vector (VSV) which holds
Figure 1. IVHS Control Architecture (after Varaiya and Shladover) (9).
information relating to the vehicle, its lot, its destination and other data describing its current situation. Fault flags are held in the VSV. There is also, one per block, a roadside-based platoon-level controller, which keeps track of fault conditions, and occasionally enters into manoeuvres involving faulty vehicles.

The link layer is concerned to advise on the track to be followed through the system by each vehicle, in relation to its destination. This data is written to the VSV by a roadside-based link controller, which communicates with the vehicle at each gate it passes (including, of course, the entry gate). The higher levels in the architecture are not of concern here, except to note that we do assume that some laws are in force which cover operation on the ALs. These are discussed in detail in Hitchcock (1992c). The legal provisions include exclusion of non-equipped vehicles from the ALs and a ban on unequipped trailers and external loads. We do not assume, in the analysis discussed later, that the law is always obeyed. In the analysis, however, we do reckon up the number of simultaneous faults necessary to permit a hazard to arise by this or that route. An illegal action counts as one fault.

The platoon-level supervisor will carry out the manoeuvres required to keep the routing prescribed by the link layer if it is safe to do so. Thus link layer is outside the safety-critical subsystem. When not engaged in a manoeuvre the supervisor will either instruct a vehicle to maintain position in a platoon, or, to proceed at a given speed, keeping at least a suitable distance (platoon spacing) from the vehicle ahead in the same lane. In the former case the vehicle is a follower, in the latter it is a leader. The leader of a one-vehicle platoon is called a free agent. At suitable intervals vehicles not engaged in a manoeuvre will conduct probes, which are operations designed to check that the equipment is still working.

Here platoon spacing is derived by an argument following Shladover (1979). A leading vehicle reduces speed abruptly with a stated deceleration. After some defined reaction time the following one brakes with another deceleration. Platoon spacing is the distance which just avoids collision. Here the follower’s deceleration is that deceleration at which a platoon can maintain internal separations. It will be less than the maximum brake performance of a well-maintained vehicle. Clearly platoon spacing depends on, among other things, the weather. It is set, as a function of speed, by the system at run time. There is also manual spacing, which is a spacing at which a driver will feel able to control the vehicle when control is returned to him.

2.2 Manoeuvres

Three manoeuvres are sufficient for normal operation. In the merge manoeuvre, two platoons move together to join into a larger platoon. In the split manoeuvre, a platoon divides into two. In a change-lane manoeuvre a free agent (only) communicates with vehicles in other lanes, and, when it is safe to do so, moves over into an adjacent lane. The presence of fault flags will excite one of two other manoeuvres. These are forced-split and emergency-change. Their effect is the same as split and change-lane respectively, but the presence of faults makes different protocols necessary.
For a full description of the system, reference should be made to Hitchcock (1992c). This includes the ways in which operation in particular sections of some lanes may be degraded in fault conditions.

3. HAZARD ANALYSIS

There has been no formal analysis which arrived at the hazards. Part of the basis is a common-sense appreciation of how high-delta-V collisions can arise. Another part is a general understanding of the dynamics of platoons arising from Shladover (1979). They were promulgated in Hitchcock (1991) with an express invitation to readers to consider alternatives. In the twelve months since, no criticism has been forthcoming. The author is not aware of any other technique for proposing hazards at this level which can be carried out by one person. However, the literature abounds with examples of cases where catastrophes have occurred by routes which were obvious with hindsight.

Thus, in Hitchcock (1992a), a method of working is proposed in which hazards arise after examination of the basic requirement by a team of workers independent of the designers. That is not possible here. The arguments from which the current hazards are derived are set out in Hitchcock (1991) and Hitchcock (1992a).

The hazards are:

A. A platoon (or single controlled vehicle) is separated from one ahead of it, or from a massive stationary object in its path, by less than platoon spacing.

B. A vehicle, not under system control, is an unmeasured and unknown distance in front of a platoon (or single controlled vehicle).

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

D. 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 within a short period. Here we propose a period of two seconds.

There are other hazards related to (illegal) equipment that can pass false messages to the system controls, interference with the control computers, explosives, heavy weights dropped from bridges and other deliberate acts. One may wish to design to circumvent such activity. The features introduced for these reasons are unlikely to interact with the design of the system as a whole.

The course of a vehicle not under system control is not predictable. A driver's aberrant behaviour can always cause a collision. On the AL, the fences prevent this. An exception
arises if a vehicle enters the AL illegally by driving through a gate. This possibility will be discussed later. On the TL, however, all vehicles, whether controlled and uncontrolled, are exposed to the possibility of bad driving. This means that vehicles under system control are liable to be exposed to catastrophes. We argue that they would have equally been so exposed, had there been no automated system. Original safety levels are not augmented.

4. FAULT TREES

We have now to propose a technique to verify that the specification does not permit a hazard within the safety criterion. Fault tree analysis is here demonstrated to be appropriate. The criterion, it will be remembered, is that no hazard shall arise unless two independent and near-simultaneous faults occur. Fault trees have been described elsewhere (see Roberts, 1981). The technique has been applied in other fields. It is new to highway and automobile engineering.

The situation under which each hazard could occur is considered. The answer will be of the form “If this or that or both of those or...happens.” In the language of predicate logic, the answer is “If A happens or B happens or (C and D) happens,” where “A happens,” “B happens,” etc. are propositions. These propositions describe possible logical precursors to the hazard.

It may happen that one or more of these propositions can be shown to be impossible. For example, a proposition might imply reversal of gravity. Alternatively a proposition could imply that two simultaneous faults have occurred. In such cases this branch of the tree can be terminated. Otherwise, the question “How could A happen?” brings the answer “If AA or AB or...happens.” The process can be repeated. Sooner or later one of two possibilities will arise. A chain of events may be found which could indeed cause a hazard after only one fault. The alternative is that the chain peters out in double faults and impossibilities. In the former case a design fault has been discovered. In the latter case the safety criteria have been met. If there is a fault the designer, hopefully, can rectify it. However, it will still be necessary to repeat the whole fault tree analysis to verify the design.

The merit of fault tree analysis arises when the trees do terminate quickly in practice. A prime reason for this demonstration is to discover if this is true in the field of automated freeways. When the trees do terminate, working backwards in this way is practical. Working forwards is never practical. To consider the consequences of all conceivable vehicle configurations with all possible combinations of faults involves so many combinations that the analysis would last for years or even centuries.

In this example, some additional observations are necessary. That vehicles, communicators, and sensors fail is a matter of common observation. These failures are allowed in the design of fault tree analysis. Computers, vehicle-borne or at the roadside can also fail. With them can fail the platoon-level supervisors or regulatory-level controllers. We assume here that there is such redundancy in the computers that if a computer fails totally, all at once, this counts as two
simultaneous faults. Such system failures are therefore not usually proposed as reasons for the occurrence of a particular event. We thus also tacitly assume that if a level of redundancy is lost in any computer, this is detected by the self-monitor. A fault is declared.

Again, communicators can fail. For this or other reasons messages may be passed and not received. Both possibilities are allowed for in the design and admitted in the fault trees. However, we do assume that messages are not misinterpreted. There is supposed to be such redundancy in the message structure that a garbled message is recognized as such. It is ignored. A turning-point may fail in such a way as to close a gate that should be open, but not the reverse. VPDs are also duplicated, so that both parts do not fail simultaneously.

Further some hazards can be foreseen, and do not appear to be remediable. In all cases they are rare. Further research will be necessary to estimate their frequency and the severity of any resulting accidents. Then a decision can be made about the acceptability of these risks. We call these “foreseen hazards” in the analysis.

There are four kinds of foreseen hazards.

(a) Some malfunction of a vehicle in a platoon may cause vehicles in the platoon to crush together. This is not usually a catastrophe. The collisions occur at low relative speeds, and the fences ensure that the vehicles come to rest without striking anything else. If however, such an accident occurs at a gate, some wrecked vehicles, perhaps with occupants may trespass on to another lane. Another platoon can strike them. There have to be gates in the fences, for vehicles must change lane. This class of accident seems unavoidable. Equally it is rare. One can argue that the accident is one fault, that it protrudes through a gate is rare enough to count as a second, and that the platoon in the adjacent lane cannot stop is a third. But this may not convince. Certainly the occurrence of a collision is immediately signalled to the system, and both the lane affected and parallel ones are put into degraded modes which reduce speed. But this will often not be fast enough to avoid a second collision.

A parallel situation arises if debris from an accident between manually-controlled vehicles, on TL or ULs or a dropped load, protrudes on to the ALs. Alternatively, the debris from an accident on the TL or ULs can be so massive that it breaches the fence. In these cases there would have been an accident on the left-hand lanes even if there had been no automation. However, the greater density of traffic on the ALs can mean that the number of casualties is greater than it would have been.

(b) During the merge and split manoeuvres, hazard 1 — platoons on ALs separated by less than platoon spacing — is necessarily violated.

(c) If an object drops from above on to the ALs, we are again dealing with a situation where there would have been an accident in the absence of automation, but where increased density of traffic on the ALs means an increase in numbers of casualties.
(d) If a manually-controlled vehicle (illegally) enters the ALS, unpredictable behaviour by the driver can give rise to hazards. It is a weakness of any design where the intelligence is concentrated in the vehicles that a “rogue” cannot be tracked. In this case, the fact that it will not respond to messages means that it is undetectable by this means (trouble in change-lane). Further if the forward sensor requires a responder, this may be absent, which will mean that the vehicle might not be detected at full range by this means either. We have no easy means of predicting the frequency of this occurrence, or of its propensity to result in accidents.

5. ANALYSIS AND RESULTS

The analysis is set out in detail in the appendixes, and illustrated in Figures A.1 to A.6. All the branches in the trees are “or” branches. Thus, in Figure A.1, Hazard A divides into six mutually exclusive possibilities, A through F. A, in turn divides into two mutually exclusive possibilities, and so on. It will be appreciated that the figures merely illustrate the whole tree structure. The logic is found in the written appendix.

It is seen that no branch of the tree contains more than three divisions. This means that the fault tree analysis is practical. The alternative, of arguing forward from possible combinations of faults would have involved millions of times more cases, if indeed not billions or trillions.

It will be seen that some design faults were identified. One of these had been foreseen. The change-lane specification in Hsu et al. (1991) does contain a manoeuvre in which a free agent enters just ahead of a platoon. It is shown in Hitchcock (1991) that, with these hazards, this is not permitted. The fault could be remedied by requiring that the platoon in the receiving lane drop back a full platoon spacing.

The other design faults are errors. The fact that the fault tree picked them up does demonstrate that the method is effective. They also demonstrate that mistakes are easily made, and that the V & V process is indeed necessary to obtaining designs which meet the safety criteria.

The design errors detected follow.

1. If fault #1 — loss of the forward sensor — is present at entry, it will not be detected immediately. Hazards can follow. The fault can be corrected by including a check on the forward sensor as part of the entry procedure.

2. If a vehicle is moving slowly, and another wishes to change lane into the lane in which it is moving, the slow mover will not respond to the initial message (request-change-lane) because it is too far away. Nevertheless there is a possibility that the changer will catch up with it and change lane too close. A vehicle which cannot communicate laterally is already enclosed in a no-entry lane. Vehicles which are slow-moving should also be so treated.
3. (This is the foreseen error referred to above.) If a vehicle changing lanes does so at the head of the co-operating platoon and strikes the gate-post, there is immediate catastrophe. As noted above, this can be cured by requiring that the co-operating platoon drop back to full platoon spacing.

4. If two vehicles each wish to change lane into the same lane, but from opposite sides, and their speeds are ill-matched, it is possible that at the time that the messages request-change-lane are sent, they are too far apart to need to reply, but that at the time of change they are too close.

5. On exit, if a vehicle has a fault in its forward sensor, and there is a manually controlled vehicle ahead of it, the separation of the two is unknown. This violates hazard B. Any danger can be avoided by causing such a vehicle to leave at very low speed, and maintain such a low speed until manual control is resumed.

6. DISCUSSION

We have examined a particular design to demonstrate the techniques of complete specification and fault tree analysis. Elsewhere (Hitchcock, 1992a, b), we recommend them for general use. The particular design tested is not being put forward as a contender for construction. It is therefore not necessary to reiterate the cycle and attempt to correct the errors. Indeed the detection of the errors is evidence of the effectiveness of fault tree analysis. However, correction of the faults is readily done, as has been shown.

We may therefore conclude:

(a) A specification has been made of an automated freeway. A set of hazards and a safety criterion have also been specified. A number of foreseen hazards have been discounted.

(b) Fault tree analysis was practical. No branch of the tree had more than four elements. Faults were detected, but it is reasonably clear that they can be corrected.

(c) It is therefore possible to construct an automated freeway which meets these safety criteria.

It should be noted that there is some gap between the assertion that the design meets the safety criteria and an assertion of safety. The primary reason for this is the alleged acceptability of the foreseen hazards. During every merge and every split, situations arise which violate the hazards. If the leading platoon should lose speed more rapidly than the following one can brake there will be a high speed collision - a catastrophe. If it is said that such an accident is very unlikely, then the merits of platooning may also be questioned. In Shladover (1979), precisely this type of accident is the basis of the argument for platooning.
6.1 Safety of Alternative Concepts

We shall now speculate briefly about the relative merits, from a safety viewpoint, of alternative automated-freeway design concepts. The speculation is based on the experience gained in the work reported here plus the parallel study reported in Hitchcock (1991b, 1991c). That was a specification and fault tree analysis of a system with a single AL and intelligence concentrated in the infrastructure. There is some interest in the comparison between vehicle-borne and infrastructure-based intelligence. The most important point, however, reflects rather on the difference between a single AL and multiple ones.

In the multi-AL system discussed here, merging and splitting are frequent. There does not seem to be any way of avoiding these manoeuvres as regular occurrences on a multi-AL automated system. In the single-AL system considered in Hitchcock (1991b), merge and split on the AL are avoided, but only at the cost of transferring merge to the TL and the entry gate, and allowing vehicles to exit from the middle of a platoon, which must then close up. It may be safer, in fact, to have platoons formed on the TL, because speeds here can be reduced if that is desired. The advantage is not overwhelming. The procedure of forming platoons by merging of vehicles at the rear of a platoon as they enter the lane certainly is less liable to hazard than any alternative, and could be the only way used in a single-lane system.

The effect on capacity of these variations is unknown. It needs to be studied.

The infrastructure-based design of Hitchcock (1991b) relied heavily, perhaps too heavily, on the integrity of communications. This is an extreme in the infrastructure basis of intelligence. The control data are passed from vehicle to vehicle in a platoon via the roadside. Any interruption to communication lasting several seconds could produce large disturbances in platoon motion, though it does not seem likely that hazards would arise. But certainly, the more the intelligence is in the infrastructure the more important to safety does the integrity of road/vehicle communication become.

A minimum of vehicle-based intelligence is required to keep a vehicle hazard-free if communications (vehicle/vehicle or vehicle/road) are less than totally reliable. However, this is not the only need. The system discussed here relies heavily on the performance of the forward sensor. This device, as we have specified it can be relied on to detect the vehicle ahead of one in the same lane at distances of more than a platoon spacing - perhaps up to 200 m. Roads curve, both vertically and horizontally. They have obstacles to vision at their edges. Whether clear sight-lines can be guaranteed at this range, remembering that the sensor is unlikely to be above the level of the hood, can be doubted. Even more can one doubt the ability to guarantee that an image is one of a vehicle in the same lane. The forward sensor, as specified in this system concept, is not obviously readily implemented.

Alternatives are possible. In the system discussed in this report we steer a vehicle which has lost its forward sensor by using vehicle/vehicle communication. In Hitchcock (1991b), the same effect is achieved by the use of multiple VPDs and a good deal of roadside logic. However, we
have now turned full circle. This discussion started by an examination of alternatives to totally reliable communications.

There is not necessarily an impasse. A balance of integrity between sensors and communications, and a balance of intelligence between roadside and vehicle seems likely to offer ways forward. However, investigation of the safety of such systems would rely heavily on the ability to predict reliability in quantitative terms. One would also need to be able to predict the consequences of loss of reliability quantitatively, which would involve better understanding of the frequency with which critical configurations occurred in practical operation. We may conclude, extending the result here, that it is possible to design an automated freeway which meets a required standard of safety. The immediate result here, however, is that we can design one which satisfies safety criteria.

ACKNOWLEDGMENTS

The author wishes to acknowledge the technical support and encouragement of Dr. Steven E. Shladover, Technical Director, PATH, and Professor Pravin Varaiya. It has already been acknowledged (Hitchcock, 1992a) that much of the design of the system discussed here is due to Ms. A. Hsu, Mr. F. Eskafi, Ms. S. Sachs, and Professor P. Varaiya (Hsu, et al., 1991).
REFERENCES


APPENDIXES

On the succeeding pages the full arguments used in the fault tree analysis are displayed. The form of the fault tree is illustrated by the figures. In these, each box is labelled with capital letters and the corresponding argument can be found in the relevant Appendix.

The phrase “Foreseen Hazard” is discussed in the main text. The words “platoon” and “platoon leader,” import a free agent where the context permits this.

Full details of the system studied are contained in Hitchcock, 1992c.
Figure A. 1. Hazard A, line A.

A. 2
Hazard A.

Hazard A is “A platoon (or single controlled vehicle) is separated from one ahead of it, or from a massive stationary object in its path, by less than platoon spacing.”

A or B or C or D or E or F

A is “Platoon and object ahead are on an AL”
B is “Platoon and object ahead are on entry lane”
C is “Platoon and object ahead are on exit lane”
D is “Vehicle is changing lanes”
E is “Object is changing lanes”
F is “Both vehicle and object ahead are changing lanes”

A is “Platoon and object ahead are on an AL”

AA or AB

AA is “Object is preceding platoon”
AB is “Object is dropped load”

The case of objects arriving from above or below is in E

A is “Object is preceding platoon”

AAA or AAB or AAC or AAD or AAE or AAF

AAA is “Object visible to system: ranging wrong”
AAB is “Object visible to system: loss speed control”
AAC is “Object not visible: fault #1”
AAD is “Object not visible: hills, curves, etc”
AAE is “Object not visible • responder damaged or absent”
AAF is “Merge or split in progress”
AAA is “Object visible to system: ranging wrong”

That is, fault #1 is present and either has not been detected because fault #10 is also present and not detected by other means (three coincident faults) or has been detected, but control ineffective because of fault #10, undetected (three coincident faults)

THREE FAULTS

AAB is “Object visible to system: loss of speed control” (also BAB, CAB)

That is, fault in regulatory-level longitudinal control system. It has redundancy to make this:

TWO FAULTS

AAC is “Object not visible: fault #1”

There is a probing procedure expressly to avoid this. If it fails this is

TWO+ FAULTS

AAD is “Object not visible: hills, curves, etc” (also BAD, CAD)

This may be a real (and basic) system error. However the way the forward sensor works is not known. It is a basic assumption that this does not happen. Fault #1, AAC applies:

TWO+ FAULTS
AAE is “Object not visible - responder damaged or absent” (also BAE, CAE)

If the responder can be checked by MON (some kind of “looping”) this is an error in MON, which is redundant. If not, there will be a need to check this in motion and at entry. However the general basis of analysis here is that infrastructure-based checking is unnecessary - ie that MON can deal with this.

TWO+ FAULTS

-------------------------==---=-------=----

AAF is “Merge or split in progress”

FORESEENHAZARD

AB is “Object is dropped load”

If this is part of a trailer, etc, legally brought in, then its loss will have been recognized by MON, and Crashstopbehind will have been called. Also, since it bears a responder, it will be visible to a following platoon. This is therefore three faults.

If load is illegally brought in (one fault) and lost (second fault), it is likely not to be visible to a following platoon. Also, the frequency of these faults may be higher than would be wished.

FORESEENHAZARD

-------------------------==---=-------=----
Figure A.2. Hazard A, line B.
B is “Platoon and object ahead are on entry lane”

In this case the “platoon” is a free agent.

BA or BB

BA is “Object is preceding free agent”
BB is “Object is dropped load”

BA is “Object is preceding free agent”

BAA or BAB or BAC or BAD or BAE

BAA is “Object visible to system: ranging wrong”
BAB is “Object visible to system: loss of speed control”
BAC is “Object not visible: fault #1”
BAD is “Object not visible: hills, curves, etc”
BAE is “Object not visible - responder damaged or absent”

BAB, BAD, BAE are same as AAB, AAD, AAE, which see.

BAA is “Object visible to system: ranging wrong”

That is, fault #1#1 cannot be checked on by MON, and as the system is designed, is not checked at admission. It needs to be, as part of the Monsys (Figure 12) procedure. Desirably the responder could be checked at same time.

DESIGN ERROR

BAC is “Object not visible: fault #1”

This is same as BAA. Fault #1 is not checked for on entry. It should be.

DESIGN ERROR

A. 7
BB is “Object is dropped load”

If this is part of a trailer, etc, legally brought in, then its loss will have been recognized by MON, and Crashstopbehind will have been called. Also, since it bears a responder, it will be visible to a following platoon. This is therefore three faults.

On the entry lane, it is not wrong, at least in some configurations, for a vehicle with a poorly secured load to be present, and not seeking entry. However, it must have dropped off after the entering vehicle has called for admission, and therefore in a very brief interval of time. That it falls at all is one fault, that it does so at just the wrong time is TWO FAULTS
C is “Platoon and object ahead are on exit lane”

CA is “Object is preceding platoon”
CB is “Object is dropped load”

CA is "Object is preceding platoon”

CAA or CAB or CAC or CAD or CAE

CAA is “Object visible to system: ranging wrong”
CAB is “Object visible to system: loss speed control”
CAC is “Object not visible: fault #1”
CAD is “Object not visible: hills, curves, etc”
CAE is “Object not visible - responder damaged or absent”

CAB, CAD, CAE are same as AAB, AAD, AAE, which see.

CAA is “Object visible to system: ranging wrong”

That is, fault #1 is present and either has not been detected because fault #10 is also present and not detected by other means (three coincident faults) or has been detected, but control ineffective because of fault #10, undetected (three coincident faults)

THREE FAULTS

CAC is “Object not visible: fault #1”

There is a probing procedure expressly to avoid this. If it fails this is two faults. The slight additional delay caused by the final change-lane, and the fact that there is no probe after exit, does not make a significant difference.

TWO+ FAULTS

A. 9
Hazard A: Platoon too close to object ahead.

A. Platoon and object on an A L.
   See Figure A.1
   Three faults

B. Platoon and object on entry lane.
   See Figure A.2
   Two faults

C. Platoon and object on exit lane.
   Object is preceding Vehicle.
   See Figure A.3
   Fault #1: Object not visible.

D. Vehicle (*plat) is changing lanes.
   See Figure A.4
   Road Geometry: Object not visible.

E. Object is changing lanes.
   See Figure A.5
   Responder out: Object not visible.

F. Both vehicle and object changing lanes.
   See Figure A.6
   Object is dropped load
   Foreseen Hazard

CAR. Object visible: ranging error.

CAB. Object visible: loss of speed control.

CAB. Fault #1: Object not visible.

CAB. Foreseen Hazard

CAD. Two faults

CB. Two faults

Figure A.3. Hazard A, line C.

A. 10
CB is “Object is dropped load”

If this is part of a trailer, etc, legally brought in, then its loss will have been recognized by MON, and Crashstopbehind will have been called. Also, since it bears a responder, it will be visible to a following platoon. This is therefore three faults.

In some configurations, at least, it may not be illegal for a vehicle with a load to be present on the exit lane. If the load falls before the vehicle quits, the VPDs will detect the load, and exit will be denied. (If the VPDs do not detect the load we have two faults.) Therefore the vehicle has already quitted when the load falls. In this case, the vehicle must be some way away from the gate, or the following vehicle will not have exited. The load then falls at just the wrong moment. Further, even if this occurs a driver should have time to assume manual control and brake. However, we may not take account of this last. But even without the last, there are two faults here.

In some configurations, there is a possibility of crash debris from other, uncontrolled, lanes getting into the exit area. This is a known, foreseen hazard. However, as things stand, such debris does not create a warning - probably presence detectors should be provided. If load is illegally brought in (one fault) and lost (second fault), it is likely not to be visible to a following platoon. Also, the frequency of these faults may be higher than would be wished.

TWO FAULTS

=================================
D is “Vehicle is changing lanes"

DA or DB or DC or DD or DE or DF

DA is “Vehicle is changing between ALs; object is vehicle”
DB is “Vehicle is changing between ALs; object is debris, etc”
DC is “Vehicle is entering: object is vehicle”
DD is “Vehicle is entering: object is debris etc.”
DE is “Vehicle is exiting: object is vehicle”
DF is “Vehicle is exiting: object is debris etc.”

DA is “Vehicle is changing between ALs; object is vehicle”

A (non-faulty) vehicle entering a new lane may do so: at the head of a platoon, at the tail of a platoon, or into an empty space. The first case is not DA, unless the preceding platoon was too close before the change. In the second, hazard should be avoided by close spacing. The dangers therefore are:

DAA or DAB or DAC

DAA is “Entering vehicle side-swipes one on lane”
DAB is “Entering vehicle too far behind partner in Change-lane protocol”
DAC is “Vehicle enters too close to platoon not partner in change-lane”

DAA is “Entering vehicle side-swipes one on lane”

This implies that the turning-point setting procedure has failed. Also, either the struck vehicle (or platoon) was a partner in the change-lane, in which case there has been very great drop-back in this lane, and great reduction in speed since the original request-change was sent.

The latter case is treated in DAC. Apart from this:

TWO+ FAULTS


A. 12
Figure A.4. Hazard A, line D.
DAB is “Entering vehicle too far behind partner in Change-lane protocol”
If change-lane is carried out as designed, switch will not be made if both sides are not in agreed position. Further the one manoeuvring must send a gate-opening message. So it is two faults to here if it is the manoeuvring vehicle which gets it wrong or one for the other. If DAB occurs, possibilities are:
1. Undetected fault #10. Since a gate has just been passed by both, it seems impossible that it be undetected - two faults anyway.
2. Mistake in platoon length. Vehicle lengths are in license. This is not an unauthorized trailer which increases the length - does not seem possible.

TWO+ FAULTS

DAC is “Vehicle enters too close to platoon not partner in change-lane”
Possibilities are:
1. there has been an undetected communication fault (two faults)
2. the partner sent con_dropt, while too close to its predecessor. It should have fallen back, and would then not have been in position and so could not send con_dropt this
3. error in longitudinal control = two faults.
4. this was change to an empty lane, and the changer caught up with a slow-mover.
Last is a design error - Slowspeed should induce NE mode, and gates should check for NE mode before setting turning-point.

DESIGN ERROR.

DB is “Vehicle is changing between ALs: object is debris, etc.”
In lane #1, this may be accident debris projected through an exit- or entry-gate from an uncontrolled lane - this is a foreseen hazard. If the accident occurred on the AL, section should be in Stop Mode. This is a system failure - two+ faults. If this is a fallen illegal load, we have a slight variant on AB.

FORESEEN HAZARD or
TWO+ FAULTS

DC is “Vehicle is entering: object is vehicle”
Vehicles enter using the standard change-lane procedure: this case differs in no way from DA.
NOTHING NEW
DD is “Vehicle is entering: object is debris etc.”
This may be accident debris projected through the entry-gate from an uncontrolled lane - this is a foreseen hazard. If the accident occurred on the AL, section should be in Stop Mode. This is a system failure - two+ faults. If this is a fallen illegal load, we have a slight variant on AB.

FORESEEN HAZARD or TWO+ FAULTS

DE is “Vehicle is exiting: object is vehicle”

If vehicle is controlled, this differs slightly from DA, for while change-lane, emergency-change and gate-opening procedures are identical, increased length of detector pad on exit lane reduces, but does not eliminate the design error found there.

Consider therefore case of uncontrolled vehicle. If vehicle was formerly controlled, and there is only one off-gate, it has decelerated very violently. If exit lane is congested, or contains a breakdown, this is possible. Alternatively this is a vehicle which has just passed the gate before exit.

In either case the extended detector means that the vehicle cannot emerge very close, and if there is a slow vehicle close downstream of exit gate, exit lane will be in SA mode. So it looks as if one can say that this case is same as DA, with impact of design error reduced, or system failure, which is at least two faults.

TWO+ FAULTS

DF is “Vehicle is exiting: object is debris etc.”

The extended detector, and the arrangement for detecting slow moving vehicles on the exit lane (the lane is put into SA mode) will reduce the chances of collision here. There may be debris which has no responder. Even if a responder is required, the forward may offer some protection at close range.

On this lane, it is not illegal to have a load, and it might fall. If it falls at the gate, the VPDs will detect it (or there is a second fault). Otherwise this case is same as CB.

TWO+ FAULTS
E is “Object is changing lanes”

EA or EB or EC or ED or EE or EF

EA is “Platoon on AL, object changes from an AL”
EB is “Platoon on AL, object enters”
EC is “Platoon on AL, object from above or below”
ED is “Vehicle on exit or entry lane, object from AL”
EE is “Vehicle on exit or entry lane, object from UL”
EF is “Platoon on exit or entry lane, object from above or below”

EAA or EAB or EAC or EAD

EAA is “Object is vehicle”
EAB is “Object is vehicle which hits gate-post”
EAC is “Object is accident debris or non-mobile object through gate”
EAD is “Object is debris or other non-mobile object which surmounts or breaches fence”

EAA is “Object is vehicle”
(The first paragraph also covers EBA)

If the vehicle is properly under control, the platoon behind has sent confirm-dropt, and both vehicle and platoon have thus verified that they are “in position” before the change. If therefore they are not “in position,” one suffers undetected fault #10 (ie developed since the last gate). This must be the platoon, since the vehicle got a check just before it changed. This is two faults.

The other possibility is that the vehicle is a “rogue” - one which has entered illegally and is not under system control. As it stands, the system is vulnerable to such vehicles. It is necessary to modify the system concept, to suppose that this does not occur, or to institute a check on entry. Here we treat this as a

FORESEEN HAZARD

A. 16
Figure A.5. Hazard A, line E.
EAB is “Object is vehicle which hits gate-post”
EBB is same

If this can happen, and the platoon-decelerate option is being used to change lanes, there will be a catastrophe. Whether or not it can happen, or with what probability it can happen, is a matter for detailed examination. The problem can be avoided by requiring that a platoon drop back to full platoon spacing: and the words in the spec do not exclude this - but it would in fact be a change:

DESIGN ERROR

EAC is “Object is accident debris or non-mobile object through gate”

If this happens, the debris is detected by the pads at the gate, and Crashstop Mode is called. But there can well be a platoon within platoon spacing of the crush when it occurs.

The way in which a platoon will behave in an internal collision “crush” in a fenced lane with gates is not clearly understood. The idea is that intrusion of a crush on to adjacent lanes is reduced by:

a. Limited number of gates.
b. Limited size of gates.

We do not know how effective b is, or what size is needed for safe passage. But if at the size chosen intrusion of this kind is at all frequent, the concept of automation is in trouble. However it is a two-fault situation (accident on other lane (1), and occurs at gate (2)).

TWO+ FAULTS
EAD is “Object is debris or other non-mobile object which surmounts or breaches fence”
EBD is same.
(That part of EC which includes falling objects striking fence is also included here.)

The breach of the fence induces Crashstop mode. However a platoon can still strike this object. Had there been no automation there would still have been an accident. Its severity would be reduced by: - reduction in size of object penetrating because of fence - possible elimination because fence holds object. Its severity would be increased by: - increased number of vehicles involved because of platooning.

Arguably, this is two faults - accident that occurs in first place, plus breach of fence.

FORESEEN HAZARD

EB is “Platoon on AL, object enters”
EBA or EBB or EBC or EBD

EBA is “Object is vehicle”
EBB is “Object is vehicle which hits gate-post”
EBC is “Object is accident debris or non-mobile object through gate”
EBD is “Object is debris or other non-mobile object which surmounts or breaches fence”

EBB and EBD are same as EAB and EAD

If the vehicle is entering under normal control EAA applies.

It is more likely in this case that the vehicle is a “rogue” - a vehicle, not under control, entering illegally. As it stands, the system is vulnerable to such vehicles. It is necessary to modify the system concept, to suppose that this does not occur, or to institute a check on entry. Here we treat this as a

FORESEEN HAZARD
EBC is “Object is accident debris or non-mobile object through gate”

An accident on the ULs or the entry or exit lane can project debris through a gate. This is

FORESEENHAZARD

EC is “Platoon on AL, object from above or below”

Object from below requires an earthquake or some botched maintenance job. Dropped object from above can occur at bridges, etc. The fact of a resulting accident is independent of automation: the severity may be increased by platooning. As against this if warning is given and Crashstop called there may be a reduction in severity. This will happen: - if object hits fence (EAD) - if objects lands at gate, and excites detectors.

In any event:

FORESEENHAZARD

ED is “Vehicle on exit or entry lane, object from AL”

EDA or EDB or EDC or EDD

EDA is “Object is vehicle”
EDB is “Object is vehicle which hits gate-post”
EDC is “Object is accident debris or non-mobile object through gate”
EDD is “Object is debris or other non-mobile object which surmounts or breaches fence”

EDA is “Object is vehicle”

If all is well, the vehicle on the exit lane will have sent confirm-dropt and have verified its position before the change. If the error occurs the vehicle on the exit lane suffers undetected fault #10. (The other got a position check at the gate as it exited.)

If this vehicle too has just exited then this is an undetected fault (ie two faults). But if it is entering, there may have been no adequate check. If therefore the entry and exit lanes are combined (and this is not the standard) it is a design error. But, as it is,

TWO FAULTS

A. 20
EDB is “Object is vehicle which hits gate-post”

Here the exiting vehicle is not joining a platoon on the exit lane, so the change-to-void variant is used. So exit vehicle has time to stop, unless it is suffering fault #10. See EDA.

TWO FAULTS

EDC is “Object is accident debris or non-mobile object through gate”

If this happens, the debris is detected by the VPDs at the gate. Crashstop is called. If however, a vehicle on the exit/entrance lane is too close there will be a collision. See EAC.

TWO FAULTS

EDD is “Object is debris or other non-mobile object which surmounts or breaches fence”

That is, an accident on the ALs - a platoon crush or worse, goes over the fence. A platoon crush will not do this if the fence is properly designed. So this is a catastrophe, and the fence breach makes it worse. But the catastrophe is three faults, and this is, therefore:

TWO+ FAULTS

EE is “Vehicle on exit or entry lane, object from UL”

That is, a vehicle under manual control enters the entry/exit lane and strikes a controlled vehicle. An accident that could have occurred without automation, and a

FORESEENHAZARD

EF is “Platoon on exit or entry lane, object from above or below”

See EC. In this case the accident is to a single vehicle, since there are no platoons on the exit and entry lanes.

FORESEENHAZARD

A. 21
F is “Both vehicle and object ahead are changing lanes”

FA or FB or FC or FD or FE

FA is “Object and platoon each move to an AL from an AL”
FB is “Platoon to lane #1, object entering”
FC is “Platoon (vehicle) entering, object from lane #2”
FD is “Platoon (vehicle) exiting, object from UL”
FE is “Object from above or below”

FA is “Object and platoon each move to an AL from an AL”

FAA or FAB

FAA is “Object is vehicle”
FAB is “Object is accident debris or dropped load”

FAA is “Object is vehicle”

Two vehicles have entered an AL from opposite sides. For some reason the second did not hear the first send request-change-lane (for if it had it would have promised not to move) and either the first did not hear the second, or the second did not hear the \textit{ack\_request\_change\_lane}. One explanation is that the first vehicle has an undiagnosed (1 fault) fault \#6 (2 faults).

If there is a vast variation in speeds, then one may have fault \#10. In this case it will be making an \textit{emer\_change}. If there is a vehicle behind it in the lane to which it moves there will be a vehicle moving at the same speed as the changer. In this case the problem considered here cannot arise. But if the changer is moving slowly because of congestion, or because it is in SA mode, then this error can occur.

\textbf{DESIGN ERROR}
Figure A.6. Hazard A, line F.
FAB is “Object is accident debris or dropped load”

That is, part of a platoon crush pushes through a gate (2 faults - accident + occurrence at gate) within platoon spacing of a platoon on the other lane - or a dropped load protrudes into the other lane.

FORESEEN HAZARD and anyway TWO+ FAULTS

FB is “Platoon to lane #1, object entering”

FBA or FBB

FBA is “Object is vehicle”

FBB is “Object is accident debris or dropped load”

This is the same as FAA - a design error.

DESIGN ERROR

FBB is “Object is accident debris or dropped load”

This is the same as FAB, except that loads may not be illegal on the entry lane. Even so, that a load should fall (1) by the gate (2) is two faults. Same as CB.

TWO + FAULTS

FC is “Platoon (vehicle) entering, object from lane #2”

FCA or FCB

FCA is “Object is vehicle”

FCB is “Object is accident debris or dropped load”
FCA is “Object is vehicle”!

This is the same as FAA - a design error.

DESIGN ERROR

FAB is “Object is accident debris or dropped load”

This is the same as FAB.

TWO + FAULTS

FD is “Platoon (vehicle) exiting, object from UL”

That is, either a manually controlled car, or accident debris from an accident on the ULs enters a gate as a vehicle is leaving. The behaviour of manually controlled vehicles can cause accidents whether or not there is automation. Further, since only one vehicle is involved, this is not going to be a multi-vehicle catastrophe.

FORESEEN HAZARD

FE is “Object from above or below”

Object from below requires an earthquake or some botched maintenance. Object from above could occur at bridges, etc. In either case the event is independent of automation, and since, in this case, there is only one vehicle involved, there is no increase in severity. There may be a reduction of numbers, because the object will cause the gate to be closed, and, if the fence is struck, Crashstop is called.

Very rare event.

FORESEENHAZARD
Hazard B.

Hazard B is "A vehicle, not under system control, is an unmeasured and unknown distance in front of a platoon or single controlled vehicle."

A or B or C

A is “Platoon is on an AL”
B is “Platoon (vehicle) is on entry lane”
C is “Platoon (vehicle) is on exit lane”

A is “Platoon is on an AL”

In this case, the vehicle ahead is an intruder. If the platoon (vehicle, now) has fault #1, a collision is possible. But this is a two-fault condition. Otherwise, the forward sensor should detect a vehicle ahead, and stay clear behind it. This will not be the case if the probe relies on an active component on the vehicle ahead.

TWO FAULTS

Note. The system does not report the entry of an intruder. This is probably a design fault, for though there can be no mechanism for tracking an intruder, it is probably desirable that the supervisors are alerted to one’s presence.

B is “Platoon (vehicle) is on entry lane”

On entry, the vehicle has just declared itself fault-free. If it is, and there is a vehicle ahead, normal controls will keep it clear. If the controlled vehicle has fault #1, and it has not detected this, this is two faults. (Query - will fault #1 be infallibly detected at entry?)

TWO FAULTS

C is “Platoon (vehicle) is on exit lane”

If the exiting vehicle is fault-free, normal controls will keep it clear of the one ahead. If it has fault #1, the driver will be aware of this. He will not be permitted to exit unless the vehicle ahead is off the extended detector, so initially there is no difficulty. If he resumes control quickly enough, he can brake. But the system will not do this for him. It is disputable if this is two faults or not.

DESIGN ERROR
Figure A.7. Hazards B, C and D.
Hazard C.

Hazard C is “A vehicle is released to manual control before the driver has given a positive indication that he accepts it.”

This can only result from a fault in the on-vehicle controls, or a communication error. Both are sufficiently covered by redundancy.

NOT POSSIBLE
Hazard D.

Hazard D is “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 a spacing less than manual spacing will be realized within (say) two seconds.”

The extended detector on the exit lane will prevent a vehicle exiting with manual spacing of anything ahead of it. Thereafter, if it is not faulty, and it comes with platoon spacing of a slowly moving vehicle ahead of it, it will brake, and it will not be released to manual while braking.

The exception arises if it has fault #1. Now, if there is a stopped vehicle ahead the driver must regain control at once to prevent a collision. He can do so - but this is still a design error, the same one as that in hazard B, line C.

DESIGN ERROR