CALIFORNIA'PATH PROGRAM
INSTITUTE OF TRANSPORTATION STUDIES
UNIVERSITY OF CALIFORNIA AT BERKELEY

Fault Tree Analysis of a First Example Automated Freeway

A. Hitchcock

PATH Research Report
UCB-ITS-PRR-91-14

This work was performed as part of the California PATH Program of the University of California, in cooperation with the State of California, Business and Transportation Agency, Department of Transportation, and the United States Department of Transportation, Federal Highway Administration.

June 1991

ISSN 1055-1425

Fault Tree Analysis of a First Example Automated Freeway

by

A. Hitchcock

Partners for Advanced Transit and Highways
Institute of Transportation Studies
University of California (Berkeley)

TABLE OF CONTENTS

Fault Tree Analysis of a First Example Automated Freeway

INTRODUCTION

This paper is not complete in itself. The background to it 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 1991b. It is a system with one automated lane, on which vehicles move in platoons. Its conforms to the constraints derived in Hitchcock 1991a.

The specification of Hitchcock 1991b was created in order to provide an example of the way specifications should be constructed if a safety analysis should carry conviction. The way in which such a specification should be recorded was also demonstrated. Finally the specification provides a basis for a demonstration of how conformity to safety criteria can be demonstrated by fault tree analysis. This paper describes the fault tree analysis as demonstrated in one example. The conclusion is that the technique described for specification and safety analysis in the earlier papers is practical and valid through its qualitative stages.

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, when platoons are involved, 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 sensors. This data is not immediately available. A ‘report on this topic is planned for later. 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 cases for quantitative analysis.

THE SYSTEM EXAMINED

Fig 1 shows the physical layout of the system considered here. There is one automated lane (AL). The Al is separated from a transition lane (TL) by a barrier, which we call the fence. There are other uncontrolled lanes (UL) to the right of the TL. The system is divided into blocks, each about a mile long. Each block contains one logical on-ramp (LONR) and one logical off-ramp (LOFR). At the LONR and the LOFR there are gaps in the fence. These are called on-gates and off-gates. Here vehicles or platoons formed on the TL may enter the AL. The AL is continuous. The TL is not continuous. It runs beside the gates and for some distance upstream of them. There are vehicle position detectors ("VPDs") on the full length of the TL and on that part of the AL which parallels the TL’s downstream end.

A general diagram of the system architecture is shown in Fig 2. The names used for the different layers were first proposed by Varaiya and Shladover 1991. The regulatory layer contains all the on-vehicle controls and some roadside ones. The platoon layer is off-vehicle.

This analysis is principally concerned with the platoon layer. The link layer controls the target speeds of vehicles and platoons. It directs platoon formation and organizes entry to and exit from the AL at the points requested by drivers. It thus optimizes capacity. Link control is outside the safety-critical subsystem. All the lower layers are safety-critical. As required by sound safety practice, the safety-critical subsystem is modular in design. Communication between the modules is controlled by defined protocols.

Control and operation are complex. There are twelve relevant modes in which vehicles operate as they pass through the system and seven possible system modes in which each block may operate.

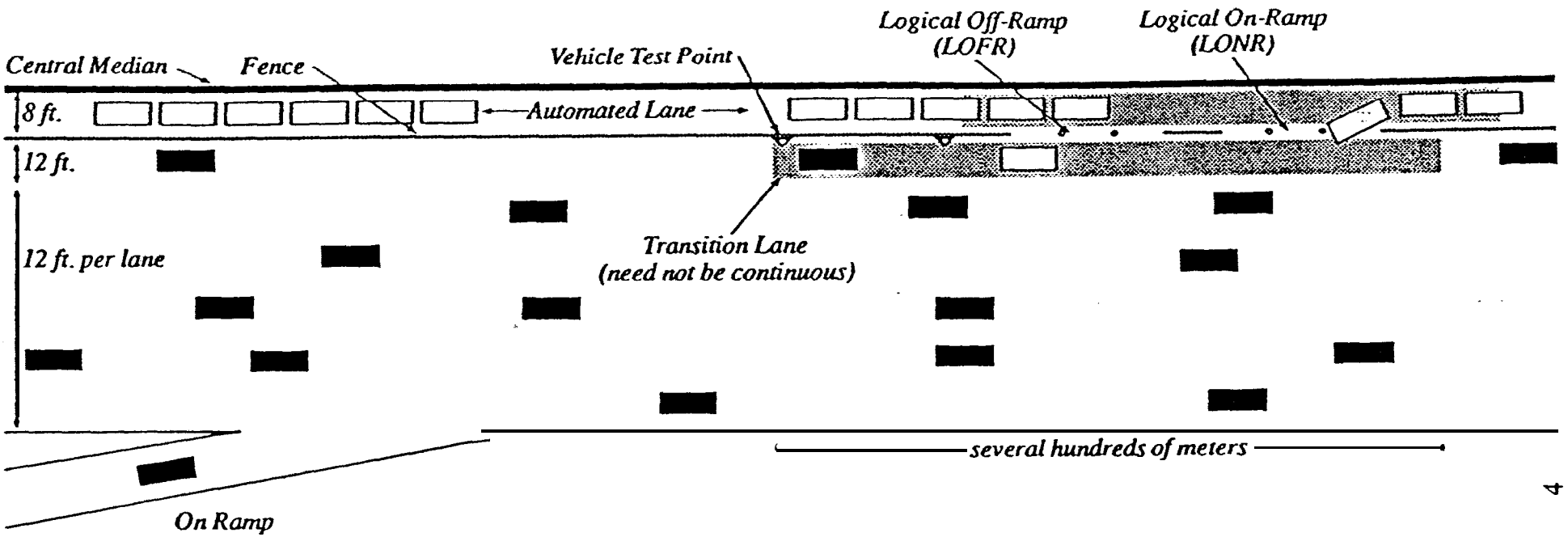
For a full description of the system, including the ways in which block operations are degraded in fault conditions, reference should be made to Hitchcock 1991a.

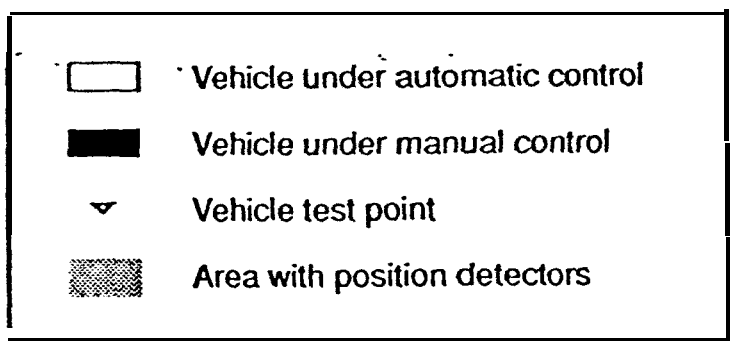
HAZARD ANALYSIS

A set of hazards has been proposed in Hitchcock 1991a. It is repeated below. Some of the terms of art used in the definitions are defined precisely in that paper.

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 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. The hazards are:

1. 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.

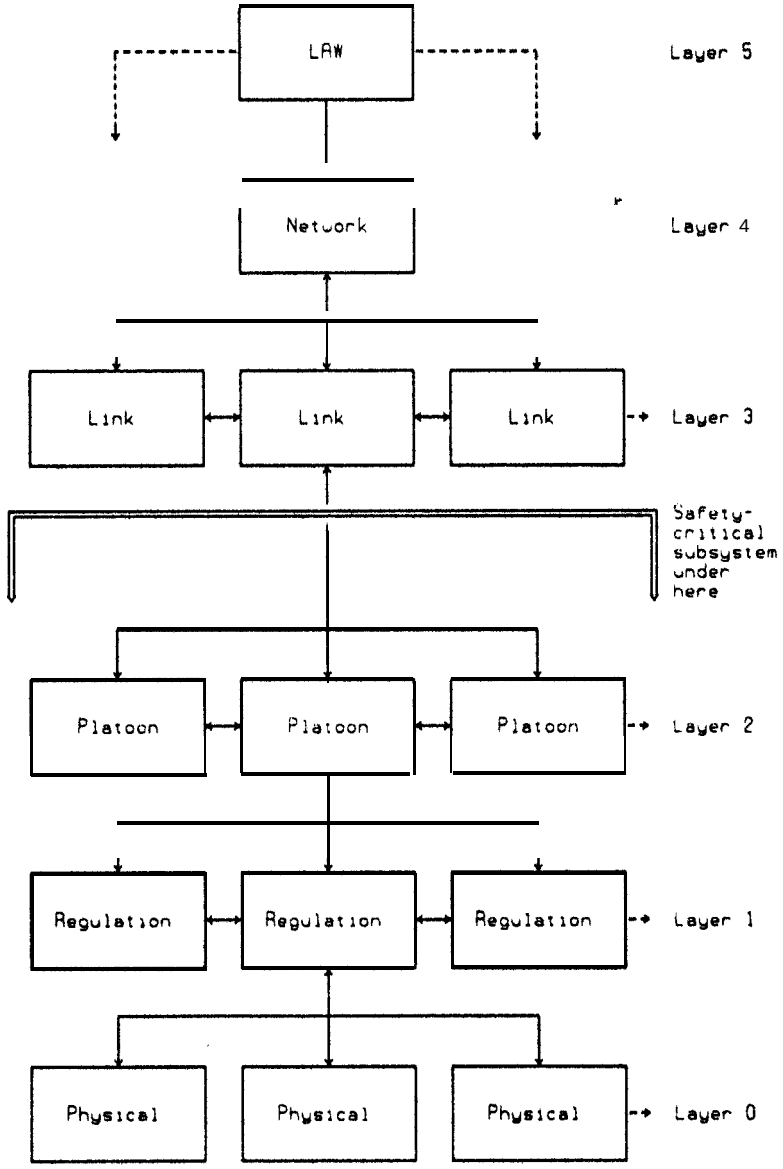




Layout of One-Automated-Lane Freeway

Figure 2. IVHS Control Architecture

After Varaiya and Shladover (1991)



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

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

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 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 is allowed for in the design. On the TL, however, all vehicles, both 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 diminished.

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.

We consider each hazard in turn. We ask "How could this hazard arise?". 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. Alternative a proposition could imply that two simultaneous faults have occurred. In such cases this branch of 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 the case of our example some additional observations are necessary. That vehicles and sensors fail is a matter of common observation. Computers can also fail, but it is possible to provide sufficient redundancy to ensure that such failures involve two

independent faults. Two-out-of-three voting is one way of doing this. We shall assume that this has been done. The computers used are therefore reliable. A quantitative analysis based on computer failure rates would rule out computer faults as a source of hazard. The phrase "computer error" in the appendix therefore means - "computer is multiply redundant - this implies sufficient simultaneous faults to satisfy the safety criterion".

Great care has been taken in the design to rule out noise, interference or misinterpretation. The message protocols are supposed to be again multiply redundant. We shall assume that the communication system and protocols are multiply redundant. Errors in the passage of messages are again dismissed in the appendix as "computer error". The interpretation is as before.

It will appear that efficient working of the VPDs is vital to safety. There have to be a great many VPDs close together. If one fails, we arrange that the adjacent ones are on separate circuits. A common cause of failure is thus eliminated. We also arranged that the computer logic ignores a failed VPD, except to report it as in need of repair. Provided therefore that maintenance is carried out promptly and effectively, VPD failure can be disregarded as a source of hazard. This issue arises in numerous cases in the appendix. It is always combined with a possible computer error. The comment is shortened to "Multiple VPD failure - cannot occur". If, however, management were insensitive to the potential risk of delaying maintenance of VPDs multiple failure could occur. Similarly, in a number of cases, safety depends on a piece of equipment only used to avoid a particular danger. There is possible that because the equipment operates so rarely it is not adequately self-monitored. In the appendix, such cases are pointed out with the phrase "Maintenance failure".

We have already observed that, on the TL, aberrant driving can cause dangers to controlled vehicles. Such behaviour would be equally likely to cause an accident if the control system were absent. Because of platooning, however, it is possible that the number

of vehicles involved is greater than it otherwise would be. This needs separate assessment: here all such cases are referred to as “foreseen hazards” and are not reckoned as design failures.

Finally there is one condition, foreseen, which can cause a hazard on the AL with one fault. This arises if an accident (one fault) on the ULs, or even the TL, causes a piece of debris to pass through the gate on to the AL. Since the gates are a small fraction of the length of the fence the occurrence of an accident at precisely the wrong location can be reckoned as equivalent to two faults. The fault tree, however, will reveal it as a single one. This case is also described as a “foreseen hazard”.

THE ANALYSIS AND ITS RESULTS

The analysis is set out in detail in the figures and the appendixes. All the tree branches are “or” branches. For example, in Fig Al the box C divides into CA, CB and CC. This means that C may arise from any one of three mutually exclusive possibilities. (The author is aware that the conventional symbols for fault trees are not being used - he has no access to relevant software.)

It will be seen that four design faults were identified. Care was taken in the design to avoid such errors, but they crept in nevertheless. This demonstrates that the fault tree technique is an effective method for verifying conformity of specification to safety criteria for AVCS-2 systems. Some other weaknesses were also detected. The most important of these was an error detected in the hazard specification. Hazard D should also require that a vehicle is not released to manual control while the brakes are being applied. Another weakness was that the detailed specification did not expressly define messages which cause the vehicle to turn the manual function off and on.

The four design errors are:

1. No mechanism was provided for correcting any catching-up of one platoon on its predecessor during its passage on the uninstrumented part of the AL. 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 on the vehicle's speed when it enters the AL. If the speed is grossly mismatched with the platoon speeds, a hazard can arise.

3. If a vehicle develops a fault, it is detected, and invited to resume manual control as soon as possible. No special precautions, however, are taken before it does so to keep other vehicles away from the danger a faulty vehicle presents. This can lead to hazards.

4. When a vehicle is released from a platoon, care is taken that it is not too close to the vehicle in front. Also the vehicle is not moving much faster than the one ahead. This also happens when a vehicle joins the TL on its way out. Thereafter its distance from preceding vehicles is controlled to a safe spacing. An unconcerned 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.

The fault tree analysis also drew attention to the fact that there are a few functions and sensors which come into use only in rare emergencies. There would be a need to test these periodically as part of routine maintenance.

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 1, 2 and 4 would be trivial.

Fault 3 can be corrected. Correction would require us to identify separately vehicles which are being excluded because of a fault detected after entry. Essentially another vehicle mode would be introduced. New variants of modules would have to be specified. This is clearly all possible.

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.

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 principal reason for this is that it has been assumed that a within-platoon accident cannot of itself be a catastrophe. This is the assumption usually made by those working on platooned systems. It is in fact not obvious that it is valid in all cases. If an accident which occurs while vehicles are joining or leaving a platoon, the consequences can be serious. This case is not really covered in the basic work of Shladover 1979. More research is desirable here.

Another deficiency would require more basic research advances. The specification here has been neither verified or validated. The system specified is supposed to be complete. There should be no conditions in which the specification does not say what happens next. The system specified is supposed to fulfil its primary function. This should mean that all drivers can exit if they wish. This must exclude those caught in Crashstop or Stop modes. Equally, the analysis is supposed to have detected all ways in which each element of the fault tree can arise.

The method by which the specification was drawn up (Hitchcock 1992a) should have ensured its completeness. At present the only way of verifying this is to take care. Nor can we presently validate the hazard specifications or the fault tree.

The system is closed. In principle it would be possible to determine the truth of these assertions by a logical process. This is not presently practical and will be a topic for further research. The “formal specifications” of the appendixes are not in the right form for logical verifications. They contain many necessary elements for this. The language employed is not however grounded in the axioms of a logical meta-system. It is not known how to remedy this.

It would have been possible, had a team of workers been available, to subject the work to a standard V & V (verification and validation) process. This would be standard practice in many industrial sectors. In these sectors standards exist. The standards differ slightly between sectors. Their essence is that a designer must justify his design to independent scrutineers. To do this the designer must record his claims precisely. The independent scrutineers also record what they find and how. The author considers that some such standard practice is desirable in IVHS. In the present case, however, the work is the work of one person. An independent check is not available.

ACKNOWLEDGMENTS

This work was performed as part of the programme of Partners for Advanced Transit and Highways (PATH) 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, and National Highway Traffic Safety 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. The report does not constitute a standard, specification or regulation.

The author would wish to acknowledge the technical support and encouragement of Dr S. E. Shladover, Technical Director, PATH. The author experienced some difficulty in writing this paper as clearly understood prose. The comments of Ms. Anna Bozzini, Editor, PATH and Mr Sompol Chatusripitak, Caltrans were very helpful.

REFERENCES

Hitchcock, A. "Intelligent Vehicle/Highway System Safety: Problems of Requirement Specification and Hazard Analysis", TRB Annual Meeting, Washington D.C., 1991(a).

Hitchcock, A., "A First Example Specification of an Automated Freeway", PATH Research UCB-ITS-PRR-91-13, Berkeley, CA, June 1991(b).

Hitchcock, A. "Methods for Analysis of IVHS Safety: Final Report of PATH MOU 19", PATH Research Report to be published, Berkeley, CA, 1992(a).

Hitchcock, A. "Intelligent Vehicle/Highway System Safety: A Demonstration Specification and Hazard Analysis", TRB Annual Meeting, Washington, D.C., 1992(b).

Roberts, N., "Fault Tree Handbook." NUREG-0492, Nuclear Regulatory Commission, Springfield, VA, 198 1

Shladover, S. E., "Operation of Automated Guideway Transit vehicles in Dynamically Reconfigured Platoons." UMTA-MA-06-008.5-79-1. UMTA, Springfield, VA, 1979.

Varaiya, P., and S.E. Shladover, "Sketch of an IVHS Systems Architecture." PATH Research Report UCB-ITS-PRR-91-3, Berkeley, CA, 1991.

APPENDIXES

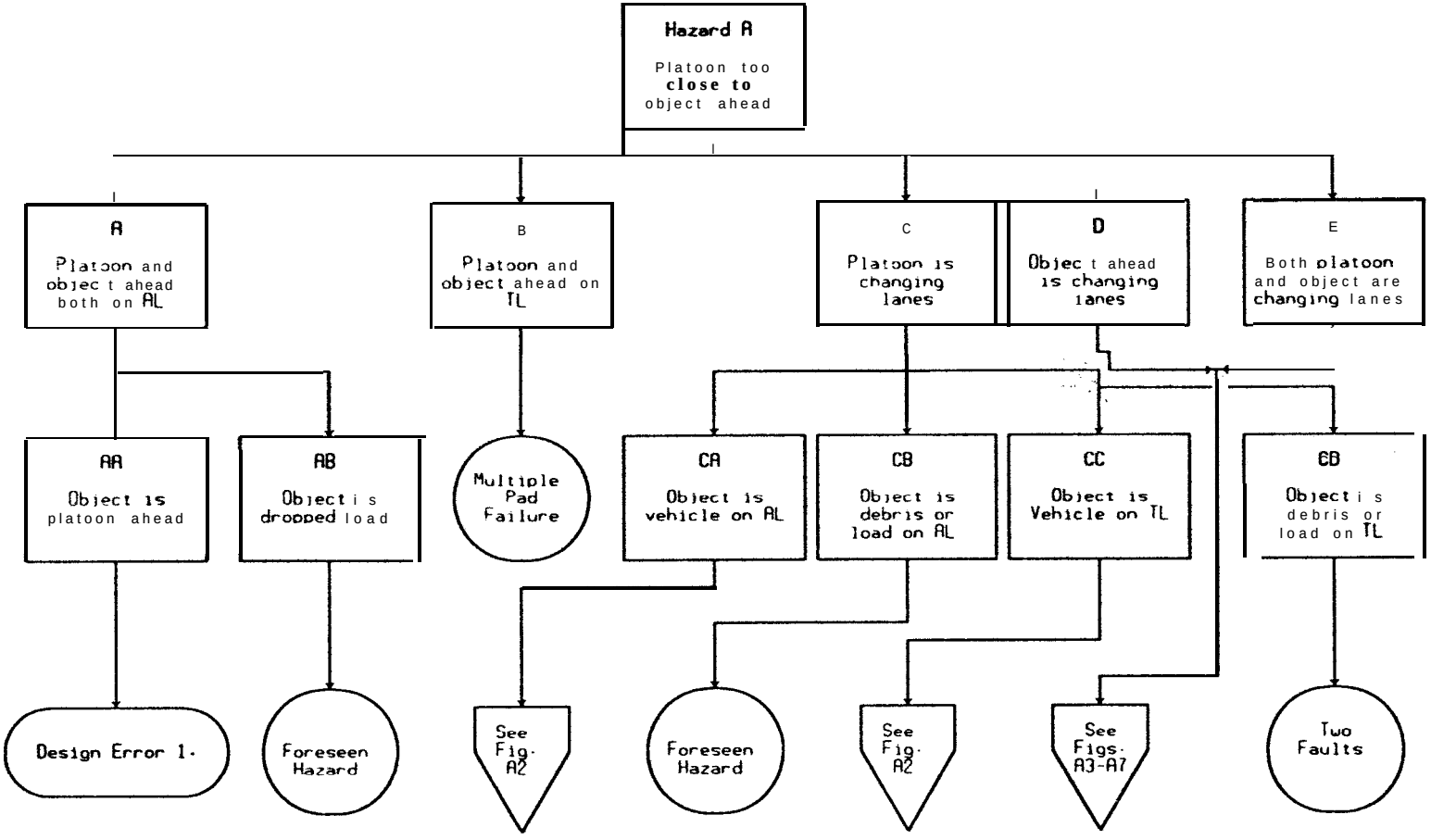
On the succeeding pages the arguments for the fault tree analysis are set out. Reference is freely made to the modules described in Hitchcock 1991b. The general form of the fault tree is given in the figures. Each box bears a reference of one to four capital letters, and the corresponding definitive argument can be found in the relevant appendix (labelled A, B, C, D and referring to the corresponding hazard.)

The phrases “Computer Error”, Multiple VPD Failure”, “Maintainance Error” are discussed on page 4 of the main text. In what follows the word “platoon” includes a solo vehicle under automatic control.

Module names are *italicised*. For details of modules, see Hitchcock 1991b.

The phrase “critical condition” refers to an accident falling short of a catastrophe. The most common of these is a within-platoon collision. A critical condition does not violate the safety criterion. Some other terms of art are defined in Hitchcock 1991a and 1991b.

Fig A. 1. Hazard A - Lines A, B and C(part).
(For full descriptions see text)
(See also Figs A2 through A7)



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

A is "Platoon and object ahead are on AL".
B is "Platoon and object ahead are on TL".
C is "Platoon is changing lanes".
D is "Object is changing lanes".
E is "Both platoon and object ahead are changing lanes".

Lines A and B are shown in Fig Al

A is "Platoon and object ahead are on 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 dealt with in D.

AA is "Object is preceding platoon".

Interval between platoons is measured by *Newspeed*. Speed is set so that this does not occur. Some allowance for variations is made. If the preceding platoon, or part thereof, loses speed, *Allospeed* is sent, which generates SRC, avoiding hazard.

However if platoon arrives at counter too close to its predecessor there is no technique for correcting it quickly. Small variations are inevitable, especially if there are hills. This may may be quite frequent. The error is not as serious as may appear, since the platoons will not be very close. Nevertheless:

DESIGN ERROR - One fault.

AA (continued).

Other possibilities are that:

a. the platoon sets off with the wrong maximum speed,

b. the platoon exceeds maximum speed,

c. the platoon does not respond to ***Speedset,***

d. the preceding platoon fails to send *Allospeed*.

All of a - d are:

COMPUTER ERROR.

AB is "Object is dropped load"

Carrying an external load and seeking entry to the system is illegal. The measurement at the chicane should exclude most cases of external loads. Thus in this case we have:

Three faults.

However, this appears to be a much more likely event than many others in this category. There is also the case where the load is internal, but badly secured. An ill-secured load is illegal on all roads, but the offence is detected only by failure. There will be no large trucks on AL, but nevertheless this may be a real worry. It does not however violate the hazards within our assumptions.

FORESEEN HAZARD.

B is "Platoon and object ahead are on TL".

Procedures designed to prevent this hazard are ***Dropback-c,*** *-p*, *-s* and *-x*. The failure Failure of any one requires computer error, multiple failure of presence detectors or vehicle controller error.

The only likely one of these three reasons is vehicle controller error, if the condition arises before testing at the chicane. The vehicle must have declared itself fit here.

MULTIPLE VPD FAILURE or COMPUTER ERROR.

Line C is shown in Figs Al, A2

C is “Platoon is changing lanes”.

CA or CB or CC or CD
CA is “Object is vehicle on AL”.
CB is “Object is debris, load, etc on AL”.
CC is “Object is vehicle on TL".
CD is “Object is debris, load, etc on TL".

CA is “Object is vehicle on AL”.

A platoon entering the AL should do so just after a platoon on AL has passed - this is ensured by the message *Onok*. If this has failed:

CAA or CAB or CAC

CAA is “Entering vehicle strikes rear of platoon on AL”.
CAB is “Entering vehicle side-swipes platoon on AL”.
CAC is “Entering Vehicle is struck from rear by platoon on AL”.

CAA is “Entering vehicle strikes rear of platoon on AL”.

This means that the speed of the entering vehicle is greater than that of platoon it is joining. There is no check that a vehicle which has received *Comeinc* or *Comeinp* and *Onok* is not travelling too fast (or too slow) for the platoon it is joining. Link control should take this into account, but link control is not part of the safety-critical system.

DESIGN ERROR.

If this error were corrected (eg by modifying the spec of *Onok*), there would be these possibilities:

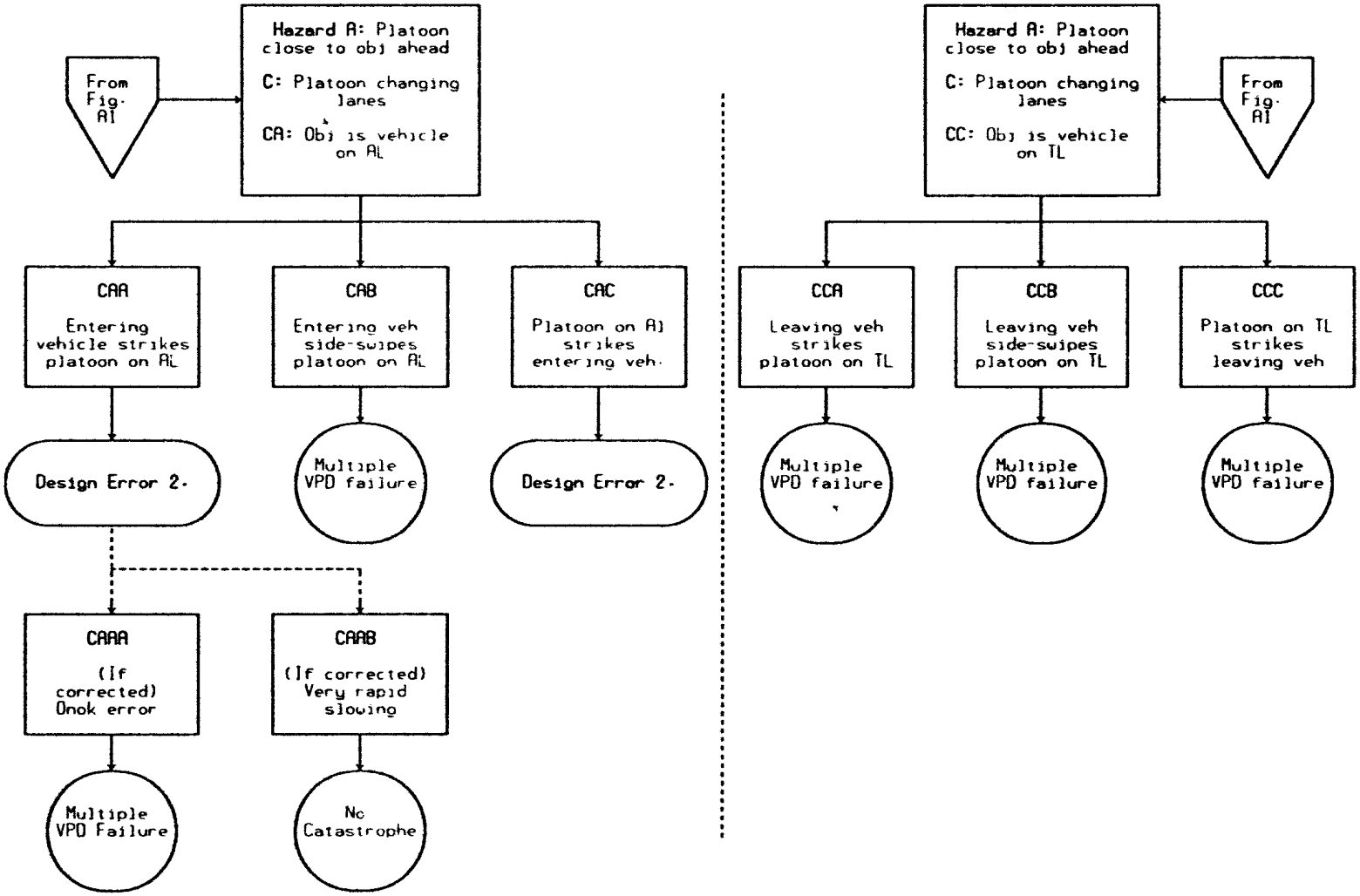
CAAA or CAAB

CAAA is "*Onok* wrongly set or vehicle enters in spite of *Onok* reset”.

CAAB is “Platoon on AL has decelerated very quickly”.

Fig A. 2. Hazard A - line C (Continued)

(for full descriptions see text)
(See also fig A1)



CAAA is "*Onok* wrongly set or vehicle enters in spite of *Onok* reset".

MULTIPLE VPD FAILURE.

CAAB is "Platoon on AL has decelerated very quickly".

That is, a platoon has stopped or crashed just after after a platoon joining its rear has entered E mode. This is a very brief interval. Velocity reduction cannot be very large. This is analogous to the stopping of a preplatoon while a vehicle is joining, but less serious. It is, to all intents and purposes a within-platoon collision.

Critical condition.

CAR is "Entering vehicle side-swipes platoon on AL".

This results from failure of reset of *Onok* to prevent entry.

MULTIPLE VPD FAILURE.

CAC is "Entering Vehicle is struck from rear by platoon on AL".

This means that the speed of the entering vehicle is much less than that of following platoon it is joining.

There is no check that a vehicle which has received *Comeinc* or *Comeinp* and *Onok* is not travelling too slow (or too fast) for the platoon it is joining. Link control should take this into account, but link control is not part of the safety-critical system.

DESIGN ERROR.

If this error were corrected (eg by modifying the spec of *Onok*), there would be the possibility that *Onok* is wrongly set or vehicle enters in spite of *Onok* reset.

MULTIPLE VPD FAILURE.

CB is "Object is debris, load, etc. on AL".

This may be accident debris projected through the gate. Otherwise it is a load dropped from a vehicle on the AL. The case that this is an accident which occurred on AL is covered in CA. In either case *Onok* should be reset. Therefore entry should be denied. Also *Helplonr* should have been sent, which would induced *Onclose*. The gate should therefore be closed.

Accident debris from, which has arrived too recently to stop the entry, is just another case of material from UL arriving too late for protection to operate. This case is a rare combination:

FORESEEN HAZARD.

Debris from an accident on TL is part of a within-platoon collision.

If an illegal load has fallen from a vehicle on the AL, just before the entering vehicle comes in (and therefore too late for *Onclose*, etc. to be effective) this is:

TWO FAULTS.

CC is "Object is vehicle on TL".

A platoon entering the TL should do so into a safe gap. This is ensured by the module *Outok*. If this has failed:-

CCA or CCB or CCC

CCA is "Leaving vehicle strikes rear of platoon on TL".
CCB is "Leaving vehicle side-swipes platoon on TL".
CCC is "Leaving Vehicle is struck from rear by platoon on TL".

CCA is "Leaving vehicle strikes rear of platoon on TL".

This means that speed of leaving vehicle is greater than that of platoon which has just passed and either *Onok* or *Dropbacks* has failed. Both require a computer error, a vehicle controller error or repeated detector errors.

While there is no check that a vehicle which has received *Ugo* or *Ugop* and *Outok* is not travelling too fast (or too slow) for the platoon it is joining (link control should take this into account, but link control is not part of the safety-critical system) this does not lead to an unacceptable condition.

COMPUTER ERROR or MULTIPLE VPD FAILURE.

CCB is "Leaving vehicle side-swipes platoon on TL".

This results from failure of reset of *Outok* to prevent exit. This implies a computer error, an error in the vehicle controller, or that the multiple detectors which deliver the *Outok* message are faulty.

COMPUTER ERROR or MULTIPLE VPD FAILURE

CCC is "Leaving Vehicle is struck from rear by platoon on TL".

The following platoon on the TL must be moving faster than the leaving vehicle. Either of (*Outok* and *Dropbackc)* or *Dropbackp,* as applicable, should stop this. The alternative is Computer error or loss of many presence detectors.

(There is no check on the leaving vehicles speed in *Outok,* but this does not matter.)

MULTIPLE VPD FAILURE

CD is "Object is debris, load, etc on TL".

If the debris is very close to gate, *Outok* should prevent exit. This will not be so if the object is debris from the preceding vehicle in a postplatoon. In this case we have a within-platoon collision.

Critical condition.

C D (c o n t i n u e d)

If the object is a dropped load or a stationary vehicle, or accident debris, *Stoptl* should have caused slowing to rest immediately on exit. *Stoptl*, however, does not close gate, It cannot be modified to do so, because of likelihood that postplatoons will come to rest. More design thinking and analysis is needed here.

Two faults, but design may need improvement.

POSSIBLE DESIGN CHANGE.

If *Stoptl* is not sent this is:

COMPUTER ERROR.

Line D is shown In Figs A3 through A6

D is "Object is changing lanes".

DA or DB or DC or DD or DE

DA is "Platoon on AL: Object from TL".
DB is "Platoon on AL: Object from above or below".
DC is "Platoon on TL: Object from AL".
DD is "Platoon in TL: Object from UL".
DE is "Platoon on TL: Object from above or below".

DA is "Platoon on AL: Object from TL".

DAA or DAB or DAC or DAD or DAE

DAA is "Object is Platoon or vehicle entering properly".
DAB is "Object is vehicle entering improperly".
DAC is "Object is entering vehicle which hits gate-post".
DAD is "Object is accident debris or other non-mobile object".
DAE is "Object is debris or other immobile object surmounting or breaching fence".

DAA is "Object is Platoon or vehicle entering properly".

"Properly" here means that *Comeinc* or *Comeinp* has been received and that *Onok* is set, so that the vehicle, whether in platoon or not, can enter without hazard. If this sequence is followed there is no hazard. Therefore there is a computer error, or Onok has failed.

MULTIPLE VPD FAILURE.

Fig A. 3. Hazard A - Line D(part)

(For full descriptions see text)
(See also figs A1, A4, A4 and A6)

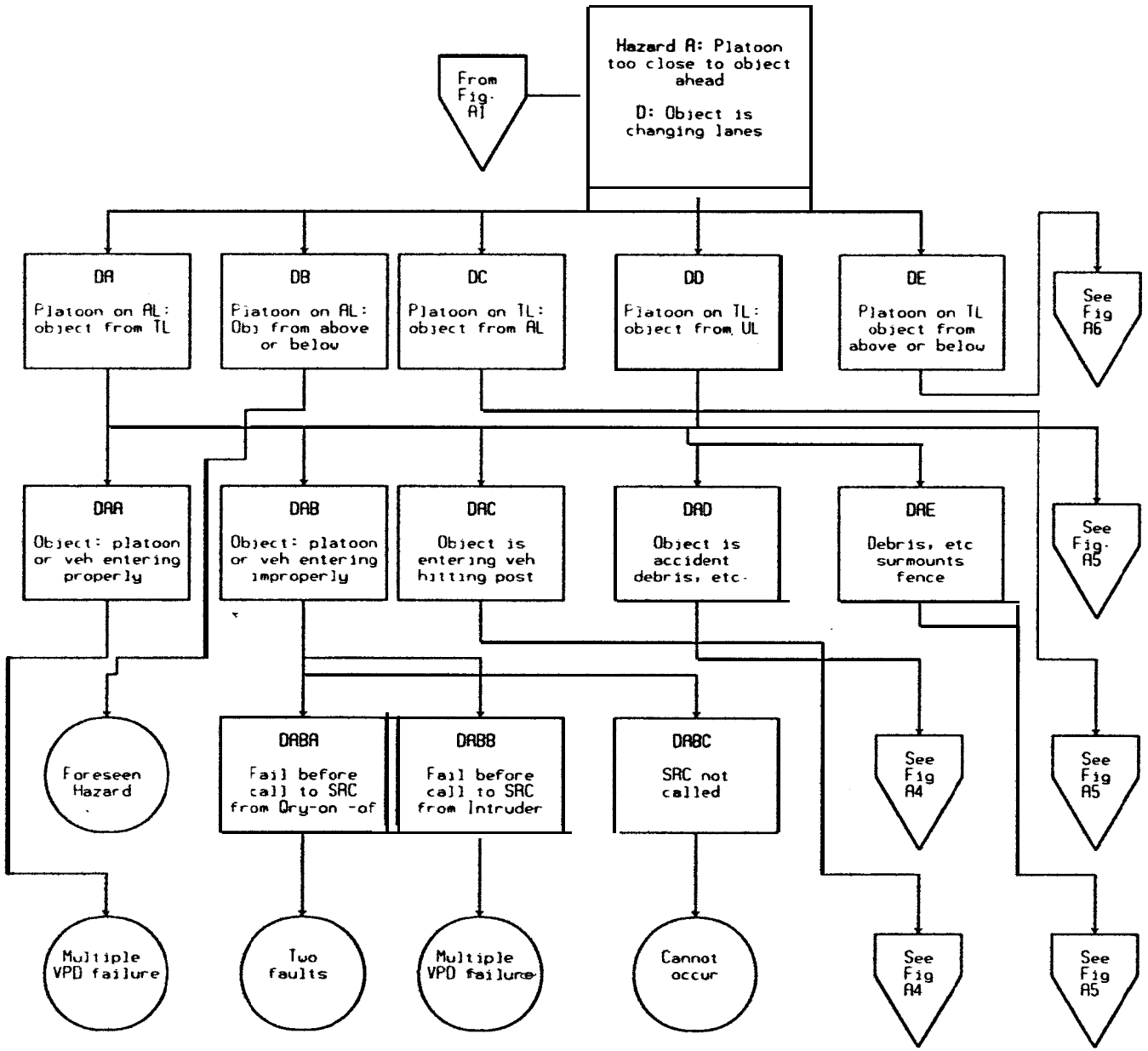


Fig A. 4. Hazard A - Line D(Part)

(For full descriptions see text)
(See also Fig A3)

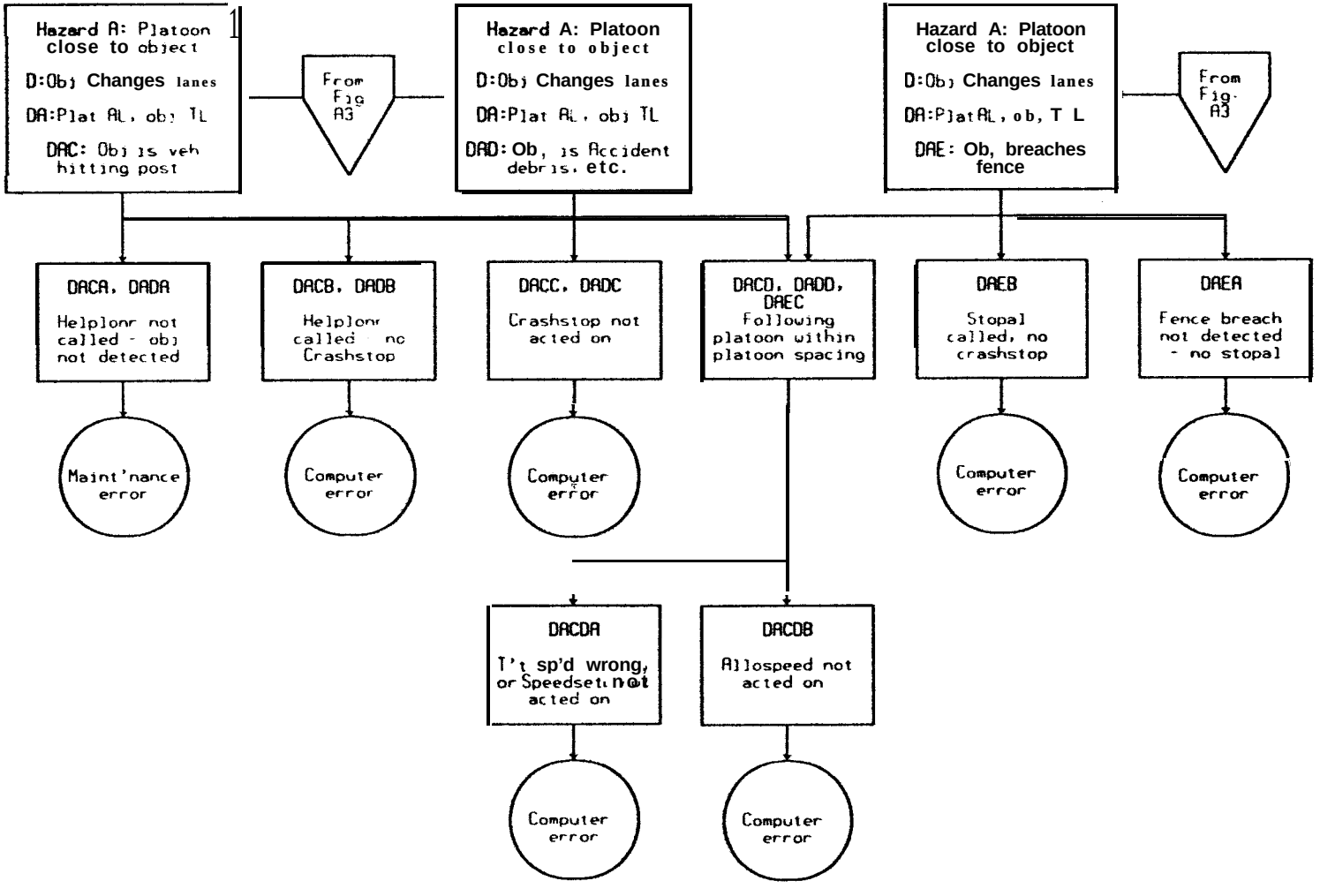


Fig A. 5. Hazard A - Line D(part)

(For full descriptions see text)
(See also fig A3)

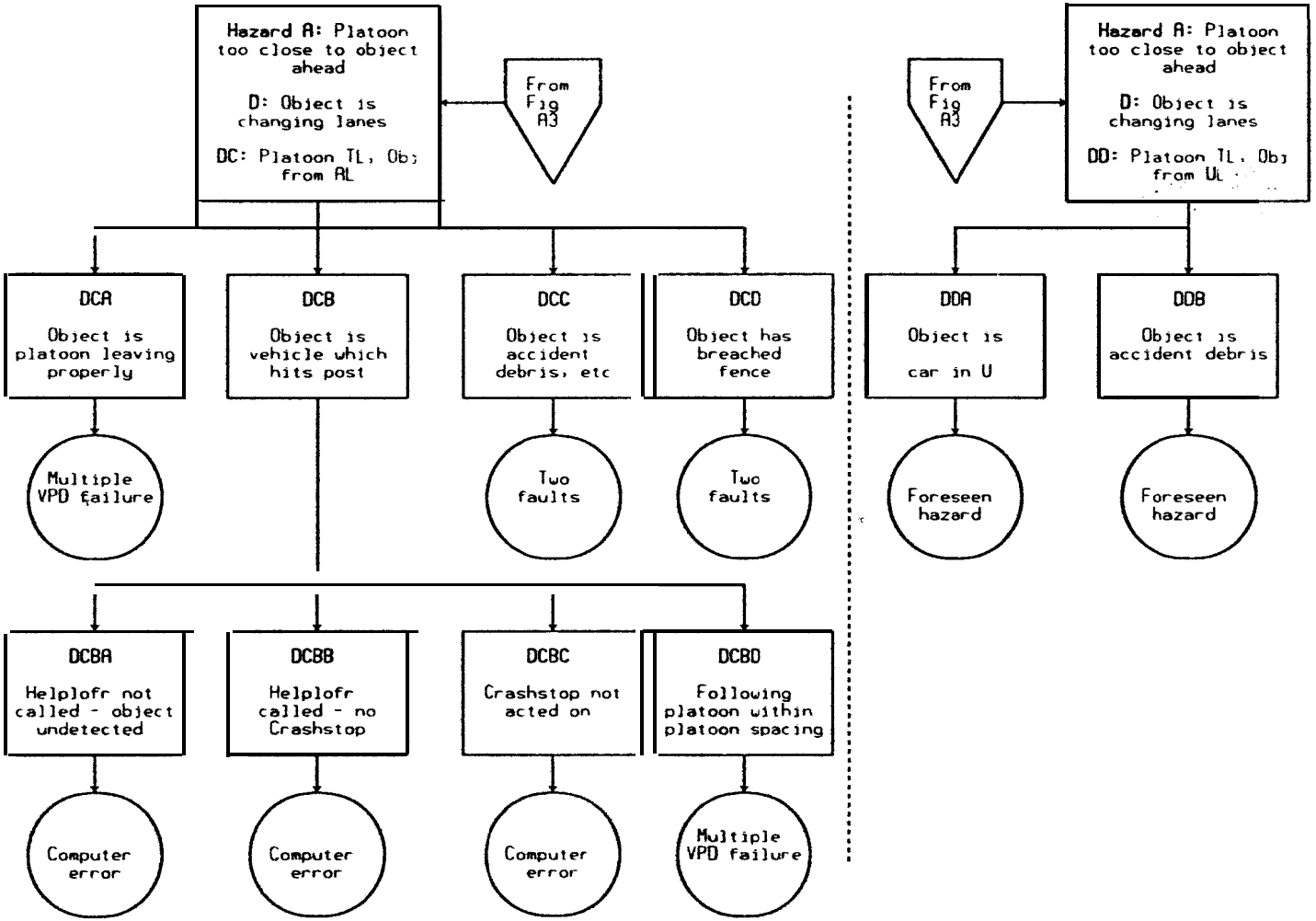
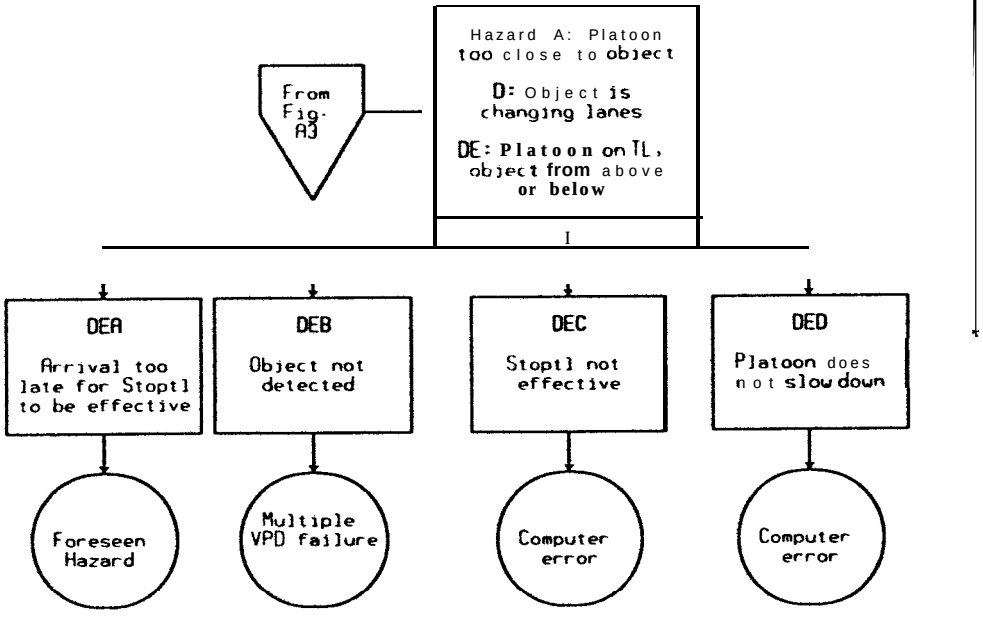


Fig A. 6. Hazard A - tine D (part)
(for full descriptions see text)
(See also Fig A3)



DAB is "Object is vehicle entering improperly".

This is illegal. If it occurs *Queryinton* or *Queryintoff* should be called. This should be followed by *Intruder* (even if *Queryinton* or *Queryintoff* is not called). Any of these calls SRC, which removes hazard quickly. Further action is up to HP.

DABA or DABB or DABC

DABA is "Hazard arises before call to SRC from *Queryinton* or *Queryintoff* is effective".

DABB is "*Queryinton* or *Quetyintoff* not called: hazard arises before SRC called from *Intruder"*.

DABC is "SRC not called".

DABA is "Failure before call to SRC from *Queryinton* or *Queryintoff* is effective".

This implies that the illegally entering vehicle did so closely in front of a platoon, and was travelling more slowly than the platoon. The platoon hit it. This is a known hazard - counts as two faults, since action is illegal, and occurred at just thewrong time.

FORESEEN HAZARD and TWO FAULTS.

DABB is "*Queryinton* or *Queryintoff* not called: failure before SRC called from *Intruder"*.

MULTIPLE VPD FAILURE.

DABC is "SRC not called'.

Double Computer error, or maintenance failure plus computer error.

CANNOT OCCUR.

DAC is “Object is entering vehicle which hits gate-post”.

If there are following vehicles in platoon behind the entering vehicle there will be a within-platoon collision. This is a

Critical Condition.

Otherwise, *Helplonr* is called, and also *Stoptl*. The former will cause Crashstop on AL, while the latter will cause vehicles on TL to brake to sensor-range. On AL, the spacing should be full platoon spacing. *Helplonr* causes braking soon enough to stop further collisions. On TL, similarly, any controlled vehicle is a full platoon spacing behind and will be warned to stop in time. An manually controlled vehicle can, however, ram the crashed platoon from behind. This is a foreseen hazard. Otherwise:

DACA or DACB or DACC or DACD

DACA is "*Helplonr* not called - stationary vehicle not detected”.
DACB is "*Helplonr* called but no Crashstop”.
DACC is “Crashstop not received or acted on - vehicle continues”.
DACD is “Following platoon is within platoon spacing”.

DACA is "*Helplonr* not called - stationary vehicle not detected”.
DADA is same.

This is either a computer error or failure of the mechanism in the post that detects its being rammed. The latter is a maintenance failure. However the device is one which will come into play very rarely, and only in situations of potential catastrophe. It is possible that routine self-monitoring is inadequate here. There is a need for routine inspection.

Critical condition.

MAINTENANCE ERROR.

DACB is "*Helplonr* called but no Crashstop”.
DADB is same.

COMPUTER ERROR.

DACC is “Crashstop not received or acted on - vehicle continues”.
DADC is same.

COMPUTER ERROR.

DACD is “Following platoon is within platoon spacing”.
DADD is same.
DAEC is same.

Critical condition.

DACDA or DACDB

DACDA is “Target speed wrongly calculated initially, or *Speedset* not acted on”.
DACDB is "*Allospeed* not sent or acted on”.

DACDA is “Target speed wrongly calculated initially, or Speedset not acted on”.

COMPUTER ERROR.

DACDB is "*Allospeed* not sent or acted on”.

COMPUTER ERROR.

DAD is “Object is accident debris or other non-mobile object”.

This is a foreseen danger. Debris has to enter through the gate, which makes this a two fault case. *Helplonr* or *Helplofr* should be sent, and the platoon approaching the object should Crashstop. It may still strike, though at reduced speed. This case is covered in DAC, though DAC has other cases also.

DADA or DADB or DADC or DADD

DAD* identical with DAC*, * = A, B, C, D.
TWO FAULTS.

DAE is “Object is debris or other immobile object surmounting or breaching fence”. (DB, with falling object striking fence, is included here).

Breach of the fence should call *Stopal*, sending block to Crashstop mode. It should also call *Stoptl*. Collisions may still occur. Usually speed will be reduced. If, however the fence is struck immediately by a running platoon the accident will occur at high speed. This is a foreseen hazard. The accident that would have occurred without AVCS. Its severity may be increased by platooning, since this may mean more casualties. If things proceed in this way, we count one fault because there has been an accident on the UL or TL which has sent debris to the fence and a second because it has breached the wall. Thus he “normal condition is both:

FORESEEN HAZARD and TWO FAULTS.

Further collisions should be avoided because *Allospeed* is called.

However, the sequence above may not occur:

DAEA or DAEB or DAEC

DAEA is "*Stopal* not called - fence breach not detected”.
DAEB is "*Stopal* called but no Crashstop”.
DAEC is “Following platoon is within platoon spacing”.

DAEC is same as DACD (qv).

DAEA is "*Stopal* not called - fence breach not detected”.

This may be failure in a component not used in normal operation. Self-monitoring may not be valid here. Routine inspection is needed. Alternatively it is a computer error.

COMPUTER ERROR or MAINTENANCE ERROR.

DAEB is "*Stopal* called but no Crashstop”.

COMPUTER ERROR.

DB is "Platoon on AL: Object from above or below"

There is no direct warning unless the object falls at a gate, in which case EA applies. If the object strikes the fence in falling, DAE applies, and consequences may be reduced. Otherwise, if the fence is missed or the object falls very close to platoon, this is a foreseen hazard. The potential for an accident is not increased by automation, but platooning may increase the potential number of casualties.

FORESEEN HAZARD.

DC is "Platoon on TL: Object from AL".

DCA or DCB or DCC or DCD

DCA is "Object is platoon or vehicle leaving properly."
DCB is "Object is leaving vehicle which hits post".
DCC is "Object is accident debris or other non-mobile object".
DCD is "Object is debris or other immobile object surmounting or breaching fence".

DCA is "Object is Platoon or veh leaving properly".

"Properly" here means that *Ugo* or *Ugop* has been received and that *Outok* is set, so that vehicle (in platoon or not) can leave without hazard. If this sequence is followed there is no hazard.

MULTIPLE VPD FAILURE.

DCB is "Object is leaving vehicle which hits post".

If there are vehicles following the leaving vehicle in platoon, they will collide with it. This is a within-platoon collision:

Critical Condition.

DCB (continued)

Thereafter *Helplofr* is called, and also *Stoptl*. Former will cause Crashstop on AL, latter will cause vehicles on TL to brake to sensor-range. On AL, the spacing should be full platoon spacing. *HeZpZofr* causes braking soon enough to stop further collisions. On TL, similarly, any controlled vehicle is a full platoon spacing behind and will be warned to stop in time. A manually controlled vehicle can, however, ram the crashed platoon from behind. This is a foreseen hazard. Otherwise:

DCBA or DCBB or DCBC or DCBD

DCBA is "*Helplofr* not called - stationary veh not detected".
DCBB is "*HeZpZofr* called but no Crashstop".
DCBC is "Crashstop not received or acted on - vehicle continues".
DCBD is "Following platoon is within platoon spacing".

DCBA is "*HeZpZofr* not called - stationary vehicle not detected".

This is either a computer error or failure of the mechanism in the post that detects its being rammed. The latter is a maintenance failure. However the device is one which will come into play very rarely, and only in situations of potential catastrophe. It is possible that routine self-monitoring is inadequate here. There is a need for routine inspection.

MAINTENANCE ERROR.

DCBB is "*HeZpZofr* called but no Crashstop".

COMPUTER ERROR.

DCBC is "Crashstop not received or acted on - vehicle continues".

COMPUTER ERROR

DCBD is “Following platoon is within platoon spacing”.

This may mean that *Dropbackc, -p, -s, -p* has not functioned. This is computer error or multiple VPD failure. Alternatively the vehicle controller has not functioned.

MULTIPLE VPD FAILURE or COMPUTER ERROR.

DCC is “Object is accident debris or other non-mobile object”.

An accident has occurred on the AL, and debris has passed through the gate. The accident is therefore at the gate. The accident is one fault; thast it is near the gate is a second. *Helplonr* or *Helplofr* and *Stoptl* should be called. The platoon should be slowing when any impact occurs. Impact is, however possible

Critical Condition.

FORESEEN HAZARD and TWO FAULTS,

DCD is “Object is debris or other immobile object surmounting or breaching fence”.

Accident debris or a fallen load (illegal) has crossed the fence from *AL* to *TL*. *Stoptl* and *Stopal* should be called. The speed of any colliding vehicle will be reduced. This is an accident that could have occurred in the absence of IVHS, and because of the ameliorating effect of the fence, is less serious than it would have been. Thus, this is a foreseen hazard. Further, an accident on the AL is one fault. The breach of the fence is a second fault.

FORESEEN HAZARD and TWO FAULTS.

DD is “Platoon in TL: Object from UL".

There are no problems here which arise because of IVHS except that if a platoon leader collides with an object, the number of vehicles involved is increased because of platooning.

DDA or DDB

DDA is “Object is car in U (U = *Unconcerned mode* - see Hitchcock 1991c)".
DDB is “Object is accident debris, etc”.

DDA is "Object is car in. U".

This means that a car in U sideswipes a platoon. Aberrant of cars in U is a foreseen hazard. The accident would have occurred without automation. Under some circumstances there will have been some slowing, so IVHS gives a plus as well as the minus due to platooning.

FORESEEN HAZARD.

DDB is "Object is accident debris, etc".

An accident between vehicles on the ULs has thrown debris on to the TL. This is a foreseen hazard. However, ***Stoptl*** will be called. Speeds will be reduced. IVHS gives a plus as well as the minus due the increased number of vehicles involved.

FORESEEN HAZARD.

DE is "Platoon on TL: Object from above or below".

By definition, object falls on to detectors, and ***Stoptl*** (plus, if relevant, *Offclose*, etc) will be sent. The platoon should therefore be at sensor-range speed. No collision will occur, except as below:

DEA or DEB or DEC or DED

DEA is "Object arrives too late for ***Stoptl*** to be effective".
DEB is "Detector fails to register presence of object".
DEC is ***"Stoptl*** not called for computer failure, or lofiter fails to send signal to reduce speed".
DED is "Platoon fails to respond to signal to reduce speed".

DEA is "Object arrives too late for ***Stoptl*** to be effective".

FORESEEN HAZARD.

DEB is “Detector fails to register presence of object”.

MULTIPLE VPD FAILURE.

DEC is "*Stoptl* not called for computer failure, or lofiter (loniter) fails to send signal to reduce speed".

COMPUTER ERROR.

DED is “Platoon fails to respond to signal to reduce speed”.

Vehicle controller failure.

COMPUTER ERROR.

Line E is shown in Fig A7

E. “Both platoon and object ahead are changing lanes”.

If both are moving from the same lane to the same lane the hazard existed before the move. Therefore this can be disregarded. Otherwise platoon is moving from AL to TL (XA, EX or PX mode) and other object is moving from ULs or above to TL.

EA or EB or EC

EA is “Object falls from above or comes up through road”.
EB is “Object is accident debris or shed load from ULs".
EC is “Object is vehicle in U”.

EA is “Object falls from above or comes up through road”.

DB, with object falling or rising at a gate, is included here.

These mishaps should induce *Stoptl*, or, if object falls very close to off-gate, *Outok* reset as well. Platoon should therefore be at sensor-range speed, or fail to exit, and will stop without mishap except as in cases below.

EAA or EAB or EAC or EAD

EAA is “Object arrives too late for *Stoptl* or *Outok* to be effective”.
EAB is “Detector fails to register presence of object”.
EAC is “*Stoptl* not called for computer failure, or lofiter fails to send signal to reduce speed”.
EAD is “Platoon fails to respond to signal to reduce speed”.

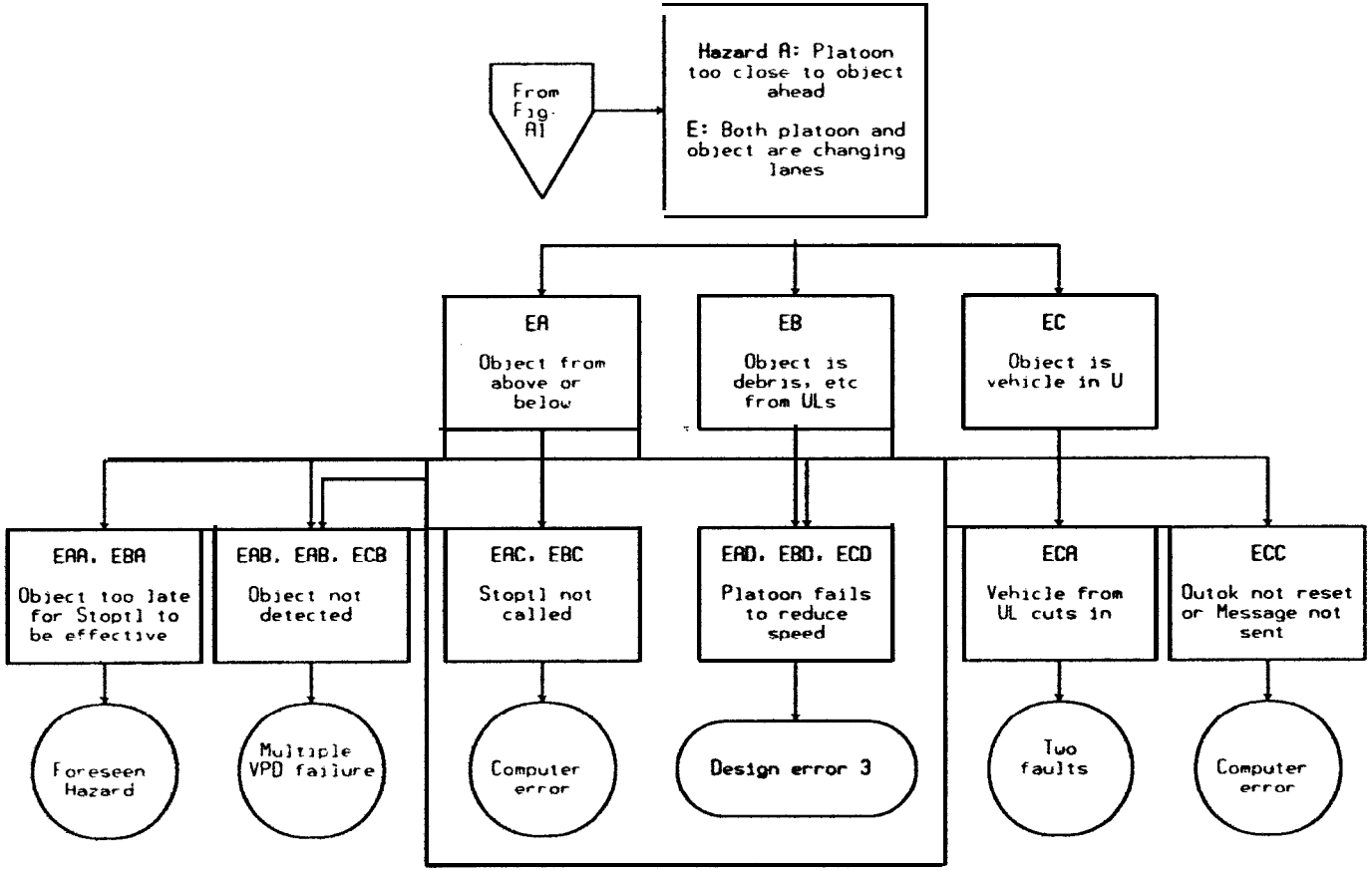
EAA is “Object arrives too late for *Outok* or *Stoptl* to be effective”.

This means that malice, an accident on overpass, or a natural disaster causes obstacle to arrive vertically immediately in front of platoon, as it leaves *AL*. *Stoptl* should be called. Thismay reduce severity of collision.

FORESEEN HAZARD.

Fig A. 7. Hazard A - Line E

(For full descriptions see text)
(See also Figs A1)



EAB is "Detector fails to register presence of object".

MULTIPLE VPD FAILURE.

EAC is "*Stoptl* not called for computer failure, or lofiter fails to send signal to reduce speed".

COMPUTER ERROR.

EAD is "Platoon fails to respond to signal to reduce speed".

Vehicle controller failure exists at exit from AL. The failure occurred after vehicle has entered system. The failure has not been detected while vehicle was on TL before entry to AL. If it has also not been detected on AL this is a multifault case. However, if the fault had been detected on the AL, the vehicle will be in EX or PX. However, this is still faults. The mechanism for passing maxspeed to the vehicle is expressly redundant, and so are the on-vehicle controllers and communicators. Nevertheless the failure to keep other vehicles away from a faulty vehicle is a fault.

DESIGN ERROR - ONE FAULT.

EB is "Object is accident debris or shed load from ULs".

If object is just by off-gate *Outok* should be reset, and vehicle (platoon) should not emerge. Otherwise, *Stoptl* should be sent, and vehicle (platoon) should be at sensor-range speed, should perceive stopped vehicle, and come to rest.

EBA or EBB or EBC or EBD

EBA is "Object appears so close to vehicle (platoon) that it cannot be avoided".
EBB is "Object is not detected by VPDs".
EBC is "Failure to send *Stoptl* (or reset *Outok*)".
EBD is "Platoon receives message, does not slow down".

EBA is "Object appears so close to vehicle (platoon) that it cannot be avoided".

Object, (debris from accident on ULs), appears just at wrong moment. A similar accident would have occurred in absence of IVHS.

FORESEEN HAZARD.

EBB is "Object (debris or load from ULs) is not detected by sensors in roadway".

MULTIPLE VPD FAILURE.

EBC is "Failure to send *Stoptl* (or reset *Outok*), following debris or load from accident in ULs to TL".

COMPUTER ERROR.

EBD is "Platoon receives message, but does not slow down to avoid debris from accident in UL.

Vehicle controller failure exists at exit from AL. Therefore the fault has occurred after vehicle has entered system, and had not been detected while vehicle was on TL before entry to AL. If it has also not been detected on AL this a multifault case.

However, if the vehicle was in EX or PX, following detection of fault on AL, this is one fault only.

DESIGN ERROR - ONE FAULT.

EC is "Object is vehicle in U".

In this case object is moving. It must be arrested by a fault before there can be a catastrophe. Its presence should have been detected by the VPDs. If the too close approach occurred just beyond off-gate, *Outok* should have been reset. Exit should not then occur. On the main TL, away from the gate the small spacing should have caused *Dropbackx* or *Dropbacks* to call *Slipbackx* or *Slipbacks*. The following vehicle platoon should have braked to a platoon spacing. If this has not happened:

ECA or ECB or ECC or ECD

ECA is "Vehicle (in U) from UL cuts in ahead of platoon".
ECB is "VPDs do not register presence of vehicle for *Outok*".
ECC is "*Outok* not reset or *Dropback*- or *Slipback*- not sent".
ECD is "Platoon receives speed message and does not reduce speed.

ECA is "Vehicle (in U) from UL cuts in ahead of platoon".

The off-gate would be giving warning of imminent exit of controlled vehicle(s). Thus this arises from failure to obey traffic signal or failure of signal. Signal lights should be redundant. Thus the vehicle in U has both side-swiped and disobeyed a signal.

If vehicle precedes exitting vehicles, then unless it is very close *Outok* will prevent exit. Otherwise, very quickly, *Dropbackx* or *Dropbacks* should call *Slipbackx* or *Slipbacks*. For collision to occur the vehicle in U must either decelerate very quickly or be moving much more slowly than the vehicle it cuts in on. Both of these are aberrant driving, which is a foreseen hazard.

TWO FAULTS or FORESEEN HAZARD.

ECB is "VPDs do not register presence of vehicle for *Outok"*.

MULTIPLE VPD FAILURE.

ECC is *Outok* not reset or *Dropback-* or *Slipback-* not sent.

COMPUTER ERROR.

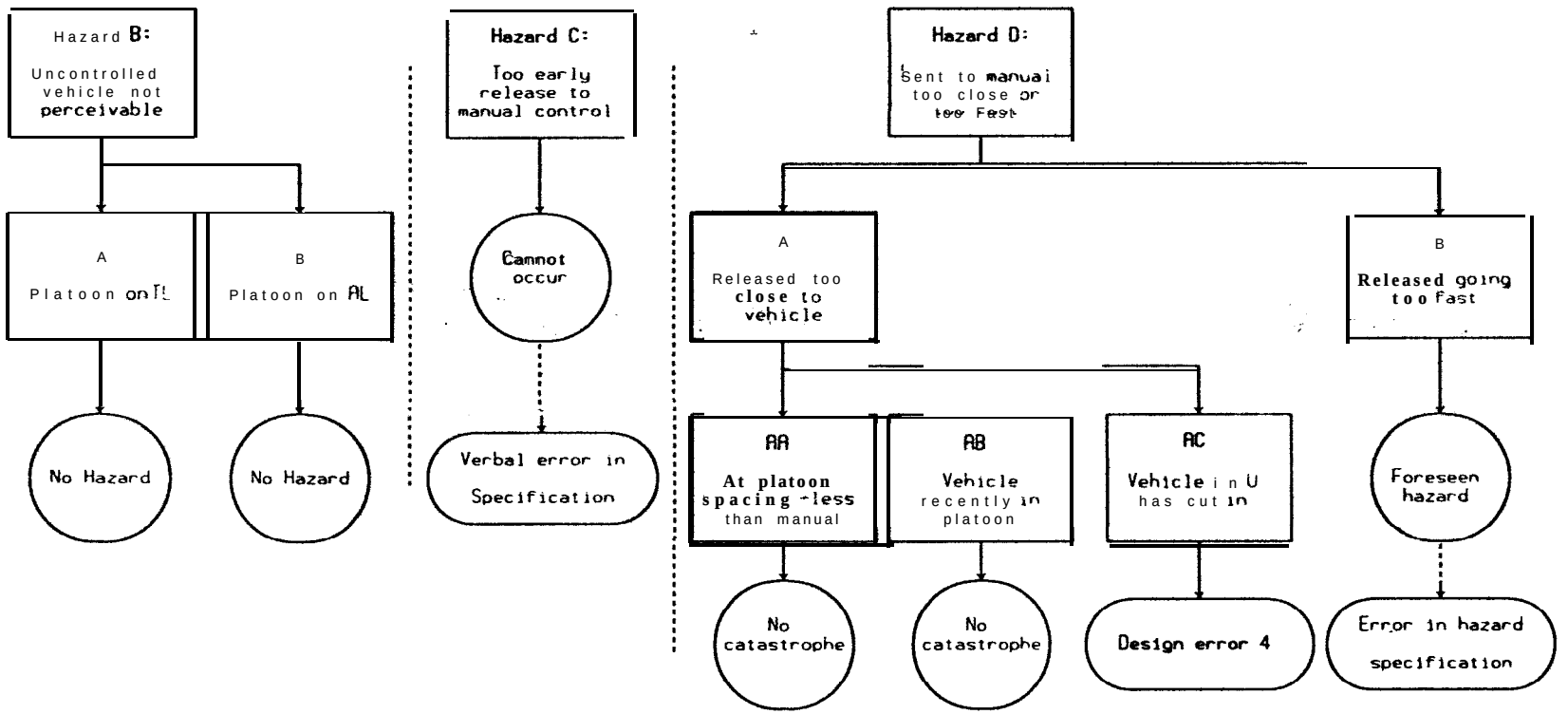
ECD is "Vehicle (platoon) receives speed message and does not reduce speed".

Vehicle controller failure exists at exit from AL. Therefore the fault has occurred after vehicle has entered system, and had not been detected while vehicle was on TL before entry to AL. If it has also not been detected on AL this a multifault case.

However, if the vehicle was in EX or PX, following detection of fault on AL, this is one fault only.

DESIGN ERROR - ONE FAULT.

Fig A.8. Hazards B, C, D
(for full descriptions see text)



Hazard B is shown in Fig A8

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

A is "Platoon is on TL".
B is "Platoon is on AL".

A is "Platoon is on TL".

In this case either presence detectors have failed systematically, or vehicle is off lower end of TL, beyond last gate. Former case is multiple VPD failure. Latter means that a platoon (or single controlled vehicle) is approaching end of TL.

At this point *Atenda* or *Atendp* should call *Stopita* or *Stopitxp,* and in either case the vehicles concerned get maxpeed = 0, and *so* come to rest. *Stoptl* is also to be called, which has same effect. Thus even if there is a vehicle in front of them it does not matter. Pedantically, it would be better to word this hazard in terms of a time spacing rather a distance one. If this were done there would be no semantic violation.

NO HAZARD.

B is "Platoon is on AL".

In this case the vehicle is an intruder. It should be detected by *Queryinton* or *Queryintoff*, both of which call SRC, thus eliminating the hazard. At exit from the presence detectors, which is the start of next block, the intruder vehicle will again be detected, by the counter. SRC will thus be called for each successive block.

NO HAZARD.

Hazard C is shown in Fig A8

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

The specification is deficient. There are no modules that disable and enable manual control. "Calls *Oniterlon*" and "calls *Offiterlof*" are not sufficient. One way out is to assume here that either the spec is remedied by addition of modules "*Manualoff*" called by *Okbut* and "*Manualon*" called by *Igotit* and *Ugotit*. Alternatively we must assume that these modules themselves restore or remove manual control. The first alternative is necessary if the design error detected in Hazard D is to be cured.

Igotit is sent by driver to indicate readiness - no problem. *Ugotit* is sent by Lonr in response to Itakeit. This response can be almost immediate. If a controlled vehicle has been some time in the system, it must be separated from vehicles ahead by platoon spacing. If the vehicle has only just joined, its separation from the vehicle ahead may be less than platoon spacing. However the separation will have increased since the vehicle joined. If a vehicle has cut in just ahead of it perhaps there will be a brief delay before the system appies brakes. If the driver has, under these awkward conditions, asked for control, he should be ready to receive it.

NO PROBLEM.

Hazard D is shown in Fig A8

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 two seconds".

There is a general design deficiency here. No account of speed or spacing is expressly taken in the checks made before release to manual control. The procedures *Brakehard* and *Dropoff* do in fact control speed to the right levels. The omission is therefore not catastrophic in every case.
A or B.

A is " Vehicle is released too close to vehicle ahead".
B is " Vehicle is released going too fast, relative to vehicle ahead".

A is " Vehicle is released too close to vehicle ahead".

A vehicle in a platoon cannot be released to manual.

A vehicle not in a platoon must be at least platoon spacing behind any vehicle ahead, in equilibrium, otherwise *Dropbackc* or *Dropbackx* will cause it to brake. If it has not been recently in a platoon, a vehicle must have "cut in" in front of it for the hazard to arise.

AA or AB or AC

AA is "Vehicle at platoon spacing, is less than manual spacing".

AB is "Vehicle has recently been in platoon".

AC is "Vehicle has cut in ahead of a controlled vehicle just before *Igotit* or *Ugotit*".

AA is "Vehicle at platoon spacing, is less than manual spacing".

This happens if speed is less than 8mph. At such a speed it is not a catastrophe if there is a collision.

POTENTIAL CRITICAL CONDITION.

AI3 is "Vehicle has recently been in platoon".

One possibility is that the vehicle has been in a postplatoon, which it has left via *Dropoff*. *Dropoff* leaves the vehicle at manual spacing behind its predecessor. There is no hazard. Alternatively the vehicle has been in a preplatoon and left it via ***Brakehard.*** ***Brakehard*** is specified to leave the vehicle a "safe" distance behind the one ahead. This is ambiguous: It should mean "platoon spacing, or manual spacing, whichever is the greater".

In this case there is no hazard. If the words are interpreted to mean "platoon spacing" AA applies. If the spacings are not what is specified we have:

COMPUTER ERROR or MULTIPLE VPD FAILURE.

AC is "Vehicle has cut in in front of vehicle just before *Igotit* or *Ugotit*"

It is in principle possible that this will happen so soon before ***Igotit*** or ***Ugotit,*** that brakes have no time to be applied. The interval is a fraction of a second. Had the cut in occurred just after release there would have been no violation of the criteria. In any case, the action of the vehicle ahead is aberrant driving - a foreseen hazard.

However, though it is not covered in the statement of hazard the vehicle may be in the act of braking at the moment of release, whether within or without manual spacing. This may be hazardous - one should not release to manual the vehicle is while braking.

FORESEEN HAZARD.
HAZARD SPECIFICATION ERROR.

B is " Vehicle is released going too fast, relative to vehicle ahead".

A vehicle in a platoon cannot be released to manual.

A controlled solo vehicle which is doing less than 35mph can be within 2 sec of manual spacing, even if it is initially at platoon spacing. (This will only happen if the vehicle ahead is for some reason moving slowly. There is no check to prevent such a vehicle from being released to manual.

DESIGN ERROR
