Precursor Systems Analyses of Automated Highway Systems

RESOURCE MATERIALS

Activity Area N: AHS Safety Issues

U.S. Department of Transportation
Federal Highway Administration
Publication No. FHWA-RD-96-044
January 1996

FOREWORD

This report was a product of the Federal Highway Administration's Automated Highway System (AHS) Precursor Systems Analyses (PSA) studies. The AHS Program is part of the larger Department of Transportation (DOT) Intelligent Transportation Systems (ITS) Program and is a multi-year, multi-phase effort to develop the next major upgrade of our nation's vehicle-highway system.

The PSA studies were part of an initial Analysis Phase of the AHS Program and were initiated to identify the high level issues and risks associated with automated highway systems. Fifteen interdisciplinary contractor teams were selected to conduct these studies. The studies were structured around the following 16 activity areas:

(A) Urban and Rural AHS Comparison, (B) Automated Check-In, (C) Automated Check-Out, (D) Lateral and Longitudinal Control Analysis, (E) Malfunction Management and Analysis, (F) Commercial and Transit AHS Analysis, (G) Comparable Systems Analysis, (H) AHS Roadway Deployment Analysis, (I) Impact of AHS on Surrounding Non-AHS Roadways, (J) AHS Entry/Exit Implementation, (K) AHS Roadway Operational Analysis, (L) Vehicle Operational Analysis, (M) Alternative Propulsion Systems Impact, (N) AHS Safety Issues, (O) Institutional and Societal Aspects, and (P) Preliminary Cost/Benefit Factors Analysis.

To provide diverse perspectives, each of these 16 activity areas was studied by at least three of the contractor teams. Also, two of the contractor teams studied all 16 activity areas to provide a synergistic approach to their analyses. The combination of the individual activity studies and additional study topics resulted in a total of 69 studies. Individual reports, such as this one, have been prepared for each of these studies. In addition, each of the eight contractor teams that studied more than one activity area produced a report that summarized all their findings.

Lyle Saxton
Director, Office of Safety and Traffic Operations Research
and Development

NOTICE

Technical Report Documentation Page

1. Report No.	2. Government Accession No.	3. Recipient's Catalog No.
FHWA-RD-96-044		

4. Title and Subtitle	5. Report Date
PRECURSOR SYSTEMS ANALYSES OF AUTOMATED HIGHWAY SYSTEMS Activity Area N: AHS Safety Issues	January 1996
	6. Performing Organization Code
7. Author(s) Richard Leis	8. Performing Organization Report No.
9. Performing Organization Name and Address Battelle Transportation Systems 505 King Avenue Columbus, Ohio 43201 614-424-4748	10. Work Unit No. (TRAIS)
	11. Contract or Grant No. DTFH61-93-C-00195
12. Sponsoring Agency Name and Address Federal Highway Administration Finance Division, Room 4314 400 Seventh Street, S.W. Washington, D.C. 20590	13. Type of Report and Period Covered Final Report September 1993-November 1994
	14. Sponsoring Agency Code

15. Supplementary Notes

Contracting Officer's Technical Representative (COTR) – Dick Bishop (HSR-12)

16. Abstract

The objective of this activity area is to “identify, consolidate, and discuss the major technical, design, and implementation issues and risks to be resolved for providing AHS users with a collision-free driving environment under normal operating conditions, including entry to and exit from the system.” Normal operating conditions are taken to be all conditions, (specifically including threat conditions) that may occur while the AHS is operating in the absence of system malfunction. In other words, if all possible conditions that have unsafe implications are considered, only a portion of them are allocated to AHS malfunctions. The remainder are allocated to “normal operating conditions.” To identify safety issues and asses their significance, formal system safety analysis procedures were used in conjunction with each system concept. Issues associated with critical safety performance assumptions were identified for the safety goals for which the concept has accepted control responsibility. These were expanded to include issues arising from threats not allocated to or accepted by system control. Formal evaluation and documentation procedures (parallel to those in MIL-STD 882B) were used not only to document the relative insignificance of an issue, but also to provide the beginnings of a tracking procedure to ensure satisfactory resolution of significant remaining issues in later work.

This document type is resource materials.

17. Key Words	18. Distribution Statement
Automated Highway Systems AHS	This document is available to the public through the National Technical Information Services (NTIS), Springfield, Virginia 22161—Telephone (703) 487-4650

19. Security Classif. (of this report)	20. Security Classif. (of this page)	21. No. of Pages	22. Price
Unclassified	Unclassified	170	

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF FIGURES
(Continued)

LIST OF FIGURES
(Continued)

LIST OF FIGURES
(Continued)

LIST OF FIGURES
(Continued)

ACRONYMS/ABBREVIATIONS

AARP	American Association of Retired Persons
AASHTO	American Association of State Highway and Transportation Officials
ABS	Antilock Braking System
ADT	Average Daily Traffic
AE	Architectural Engineer
AHMCT	Advanced Highway Maintenance and Construction Technology Program
AHS	National Automated Highway System
AICC	Autonomous Intelligent Cruise Control
ANSI	American National Standards Institute
APTS	Automated Public Transportation System
ARPA	Advanced Research Project Agency
ARTS	Automated Rural Transportation System
ASTM	American Society for Testing Materials
ATIS	Automated Traffic Information System
ATMS	Advanced Traffic Management System
AVCS	Automatic Vehicle Control System
AVI	Automatic Vehicle Identification
AVLS	Automatic Vehicle Location System
BBS	Bulletin Board System
CASA	Computer and Automated System Association
CE	Civil Engineering
CI	Configuration Items
CVO	Commercial Vehicle Operation
DC	Direct Current
DCAA	Defense Contract Audit Agency
DOT	Department of Transportation
DVI	Driver Vehicle Interface
EPS	Electric Power Steering
FAA	Federal Aviation Administration
FCC	Federal Communications Commission
FHWA	Federal Highway Administration
FMEA	Failure Modes Effects Analyses

FMVSS	Federal Motor Vehicle Safety Standard
FOT	Field Operational Test
FREE-SIM	Freeway Simulation
FTA	Federal Transit Authority
FY	Fiscal Year
GIS	Geographic Information System
GPS	Global Positioning System
HOV	High Occupancy Vehicle
HW	Hardware
IAVD	International Association of Vehicle Dynamics
IEEE	Institute of Electrical and Electronic Engineers
IR	Infrared
IR&D	Independent Research and Development
ISO	International Standards Organization
ISTEA	Intermodal Surface Transportation Efficiency Act
IVHS	Intelligent Vehicle Highway Systems
MOE	Measure of Effectiveness
MOP	Measure of Performance
MPR	Mean Personal Rating
MTBCF	Mean-Time Between Critical Failure
MTBF	Mean-Time Between Failures
MVMT	Million Vehicle Miles Traveled
NADS	National Advanced Driving Simulator
NAHTSA	National Automotive Highway Transportation Society of America
NDS	National Driving Simulator
NES	National Energy Strategy
NHTSA	National Highway Traffic Safety Administration
NSC	National Safety Council
OEM	Original Equipment Manufacturer
PC	Personal Computer
PBMS	Performance Based Measurement System
PSA	Precursor Systems Analysis
QFD	Quality Function Deployment
R&D	Research and Development

SAE	Society of Automotive Engineers
TMC	Traffic Management Center
TRB	Transportation Research Board
TRAF-NET	Traffic Network Simulation
UL	Underwriters Laboratories
USG	United States Government
V&V	Validation and Verification
VMT	Vehicle Miles Traveled

EXECUTIVE SUMMARY

Objective and Scope

The objective of the area N activities was to identify, consolidate, and discuss the major technical, design, and implementation issues and risks to be resolved for providing AHS users with a collision-free driving environment under normal operating conditions. Normal operating conditions in this context means in the *absence of malfunctions*. Providing safe operation despite the *occurrence of potential malfunctions* was the domain of activity area E (malfunction management and analysis). Area E and area N activities were coordinated to assure comprehensive safety coverage while preventing appreciable duplication.

The scope of the area N analysis covered the entire automated highway system (AHS) operating spectrum beginning with entry onto the system to safe exit from the system. With regard to the range of AHS configurations considered, area N's scope was largely non-RSC specific, but did cover (at a relatively high conceptual level) 1) all of the generic AHS elements (e.g., the vehicle, the roadway, and the driver) and 2) generic AHS functions (e.g., lane tracking, braking, merging with a stream of AHS vehicles, maintenance of vehicle-to-vehicle gap requirements, execution of collision avoidance actions) featured by this program team's selected set of representative system configurations (RSCs).

Methodology

Early area N activities included 1) participating in the entire team activity of defining and selecting a set of RSCs and 2) beginning the process of identifying what constitutes normal operation for these types of RSCs. Construction of a high level fault tree led to an understanding of the general fault paths that could lead to the undesired outcome of a collision in the absence of a malfunction.

Normal operating conditions were defined as all conditions (specifically including threat conditions) that might occur while the AHS is operating in the absence of system malfunctions. It was decided that the threats to be considered for an AHS include all threats currently faced on a highway system (e.g., threats posed by inclement weather), plus special AHS related threats such as those associated with operating under AHS control in strings of vehicles at close headways and automated exiting of vehicles into potentially unsafe situations.

As each of these threat types was further reviewed, it became necessary to do various ad hoc analyses to develop a better understanding of the nature and magnitude of some of the potential threats.

Results

The key activity area N findings are summarized below. Additional findings and supporting material are presented in the area N topical report.

Safety Goals

The stringent safety goals anticipated for an AHS should be achievable through carefully executing a comprehensive system safety plan that encompasses not only normal operation (i.e., operation in the absence of malfunctions), but operation in the presence of malfunctions.

Operating Threats

A thorough analysis of the operating conditions that can or should be expected in the course of normal operation reveals that a significant number of threats to safe operation exist even in the absence of vehicle or infrastructure malfunction/loss of function. AHS designers should not fail to address threats because of oversights or arbitrary decisions. Our posture at the outset is that all threats currently faced on a highway system will be faced on an AHS and must be handled. This does not mean that some threats may not be controlled. Some may simply be impractical to control, e.g., the bullet, the bowling ball, and a crash landing 747. (Even these, however, might be controlled if money is not an issue.) In broad categories, the range of primary threats include:

- Primary in-line collision threat agents:
  - Moving manually controlled vehicles operating in the AHS lane.
  - Moving AHS controlled vehicles.
  - Fixed objects (dropped load, stopped vehicle, etc.).
  - Any non-vehicle—assumed fixed object (e.g., lane-fouling from adjacent lanes, animals).
- Primary in-line threat situations
  - Forward.
  - Behind.
  - Merging.
- Intrinsic threats, e.g., factors that degrade the ability of a vehicle to control its trajectory (snow, ice, wind, sand, road surface changes, and vehicle factors such as heavy loading and poor load distribution).

In addition to these primary threats, two other threat types were identified specific to AHS, partly because some AHS concepts enhance exposure to these threats and partly because an AHS offers the opportunity to control this exposure.

- Malfunction-related threats involving control-coupled vehicles, especially those malfunctions that can potentially lead to a worst-case incident.

- Transferred threats—a special case in which the threat control responsibilities of the lead vehicle in an AHS string of vehicles is suddenly transferred to the following vehicle.

Transient Situations

There is a tendency to focus on the steady-state situation in which a string of AHS controlled vehicles is proceeding at a given speed and under relatively short headways. However, as is the case with commercial aircraft, the safety critical periods of operation tend to focus on the transient situations (e.g., landings and takeoffs). In the AHS environment, these key transients include entry and exit; changes in leading and following vehicle relationships; and (at some relatively small frequency) overall startup, shutdown, and restart of the AHS facility.

Safety Control Systems

Unlike the commercial aircraft situation, the AHS on-board and off-board control systems must essentially constitute the expert system of a typical driver. For example, the AHS control system(s) must be able to detect and identify threats, assess road and environmental conditions, decide how much it can trust the leadership capabilities/behavior of the vehicle preceding it, etc.

The variations in safety control demands and threats suggest that a portfolio of safety control options will be required for an AHS. This leads to the recognition of the need for a safety management function that directs the selection and application of a specific option, as well as the other responsibilities listed below. This function may be vehicle-based or central controller-based. In either event, however, it must be tasked with guarding the interest of individual vehicles. This function requires diverse capabilities and responsibilities in the following areas:

- Situation awareness—awareness of the current situation to be controlled.

- Restrictive state management, including transitions—i.e., dropping back to less stringent operating conditions/engagement strategies (e.g., longer headways) in response to current conditions.

- Transferred threat management—responding to unusual behavior of the preceding/lead vehicle.

- Normal malfunction management.

- Transition into and out of the AHS.

- Human participation management—authorizing and/or allowing selected driver inputs.

- "True" exit management—extending the safety boundary of the AHS to prevent "outmerging" of an AHS vehicle into a situation that exceeds the ability of the vehicle and its driver to maintain proper control.

The basic concept for collision avoidance used in this report is the management of separation between independently controlled, paired vehicles. The normal control actions of a subject vehicle are determined on the basis of its dynamic relationship with adjacent vehicles (leading and trailing) as developed by inference from sensors on the subject vehicle and/or direct communication between paired vehicles. The response of a string of vehicles to a forward threat reflects, therefore, the effects of daisy chain communications between vehicle pairs in the string.

Additionally, separation requirements do not recognize a "steer around" potential as a viable normal collision avoidance maneuver. The analyses included in this report are all based on in-line maneuvers for collision avoidance.

Operator Input

While normal operation of an AHS will be "hands off, feet off, brain on," from a safety perspective, the system must function safely with the operator brain *off*. This means that, from a safety control situation, the safety manager cannot *require* operator input to resolve an unsafe situation. Furthermore, while operator inputs may be solicited and accommodated, they should be processed by the safety manager, with the results translated into vehicle motion alteration only after it is determined that this alteration will not result in an uncontrollable threat to the subject vehicle or to other vehicles in proximity. This does not preclude the possible need for an AHS initiated "panic" stop.

Pallet-Based AHS

The use of an AHS featuring pallets would cause a shift of safety management from individual vehicles to the infrastructure. Several benefits could accrue:

- Improved control over system design would increase similarity/consistency of the vehicles (i.e., traveling units) and their operating characteristics.

- Improved control over vehicle/traveling unit maintenance would reduce the likelihood of degraded performance.

- Reduced interruption due to ACI/ACO (i.e., ACI and ACO could be handled off-line).

- Virtual elimination of the problem of transferring control to the human operator. (Transfer would be under stopped conditions. The concern for “true exit” safety problems would also be reduced.)

- Opportunities for incorporating reusable energy absorption techniques may lessen the demand for no collisions and allow minor collisions not perceived as is allowed with other RSCs.

- Controlled use of alternative propulsion systems and/or fuels.

Because of improved control over the designed-in capabilities, maintenance, and check-out of the critical on-board AHS systems—the use of pallets should result in a net increase in safety over the other candidate RSCs. These gains would, however, need to be weighed against possible losses in throughput and changes in the liability situation, financing requirements, land use requirements, etc.

INTRODUCTION

This report contains the results of investigations of the AHS issues and risks associated with providing a collision-free environment in the absence of system malfunctions.

The following issue areas were investigated:

- The implications of minimum safe separations for all AHS separation concepts, with all expected threat agents.
- The problems of separation management; that is establishing the correct engagement strategy and calibrating it for existing conditions.
- The problems of navigating between engagement states in a deliberate and fail-safe manner.
- The problems of transition maneuvers between steady state engagements.
- Possible fault intervention to minimize the extent and severity of collisions.

The representative system configuration assumptions on which these investigations were guided are contained in appendix D.

RESEARCH APPROACH

This section presents the scope established to focus the analysis of AHS safety issues, describes the investigative approach to conduct this analysis, and describes the organization of the remainder of this report.

Threats

The emphasis of the analysis was toward a subset of AHS safety threats that concern avoidance of in-line collisions; i.e., collisions between an AHS vehicle on an AHS-controlled facility and all threat agents that may exist on that facility. (For vehicle-to-vehicle collisions, this is the classic rear-end collision.) This definition is expanded below.

Threat Situations

Figure 1 is a very high-level fault diagram that displays the general range of unsafe occurrences that will be faced by an AHS. The shaded nodes represent the activity area N focus. (Issues identified that are related to the unshaded nodes are included in appendix C.) As shown in figure 1, area N activities concentrated on in-line collisions between an AHS vehicle and threat agents that may exist in the AHS lane—from all possible sources.

Figure 1 also illustrates the inferred safety goal. The demand for AHS safety has been "to provide a collision-free environment under normal operations." "Normal operations" exist "in the absence of system malfunctions." This definition has been extended to a "collision-free

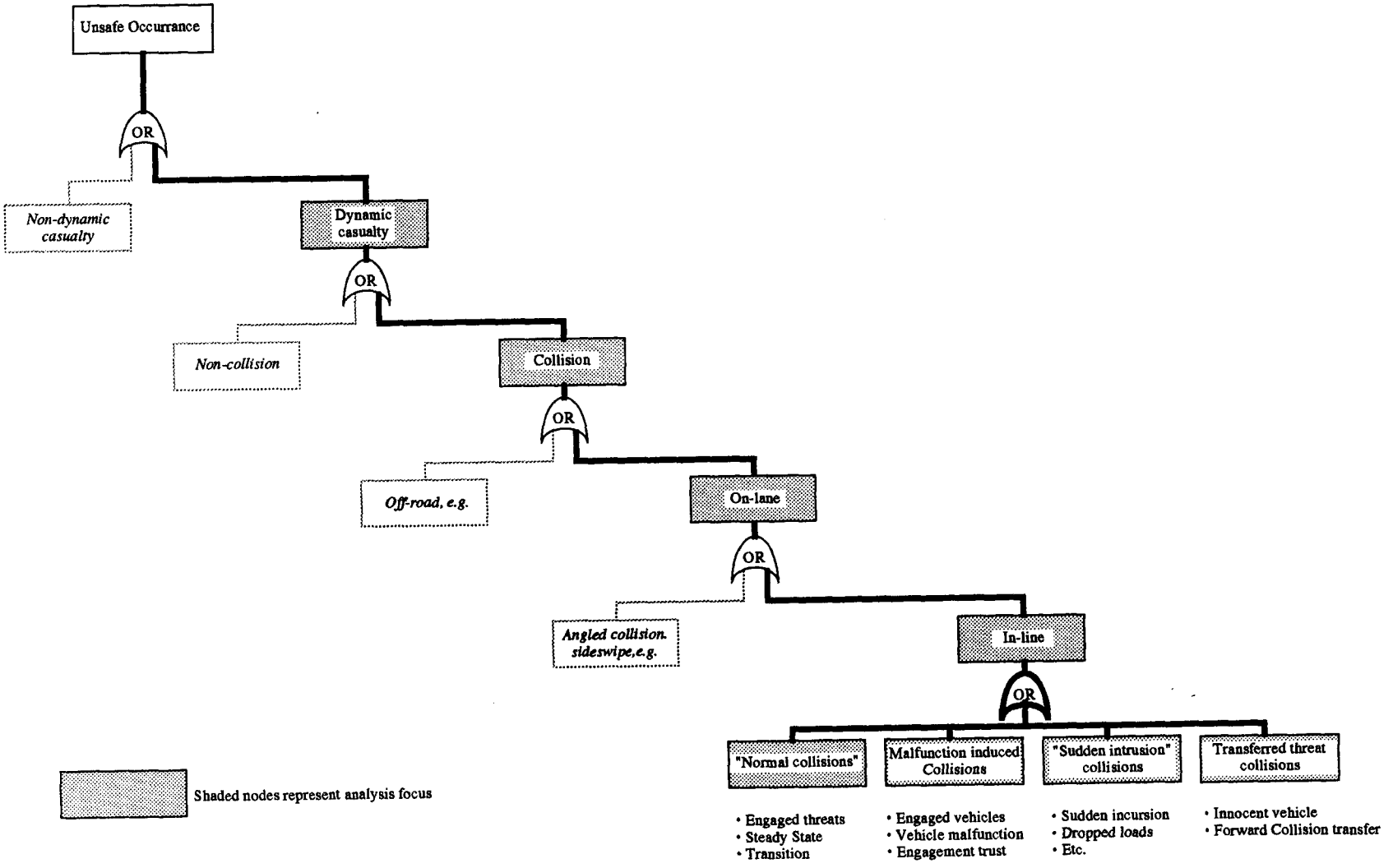


Figure 1. General fault path identifying threat situation emphasis.

environment for an innocent vehicle"—even if there are collisions elsewhere in the system. Therefore, as shown in figure 1, the in-line collisions within our focus area are divided into four categories, based on the major initiator of the collision.

- The first of these is "*normal collisions*." These are collisions that occur under conditions that appear to be within the design envelope of the AHS. There is no malfunction that alters a vehicle's performance such that it induces a collision. This class of collisions is directly related to established safety requirement of an AHS: the elimination of collisions under "normal" operations.

- The next two collision categories are based on expanded view of AHS safety requirements, as well as a recognition that the sophisticated separation management capabilities of an AHS to handle normal collisions can be effectively utilized to provide some intervention control over these collisions:

  — Collisions that are induced by *malfunctions* that alter the safe separation requirements between vehicles such that an existing separation relationship becomes invalid. The malfunction may be real, as in brake failure, or perceived, as in a loss of knowledge that the brakes are functional.

  — Collisions that are induced by a *sudden intrusion* of a threat agent onto the AHS lane at a position such that the distance ahead of the following vehicle, already on the lane, is less than the minimum safe separation required under the normal engagement capabilities of the following vehicle. Collision avoidance cannot be accommodated by the stopping capabilities of the threatened vehicle.

While it may be argued that these latter threat situations are not a part of normal operations, normal separation management should accommodate these as possible. The requirement for a high capacity AHS will involve small separations that can be safely maintained under a no-failure assumption. In general, as we decrease separation to achieve this goal, we increase exposure to collisions if a failure should occur. Therefore, the AHS is establishing exposure for an innocent vehicle. We believe that normal separation management should be charged with the responsibility, to the degree possible and practical, for managing this exposure.

- The last category is "*transferred threats*." These are threats to a vehicle that result from forward collision threats faced by the adjacent leading vehicle. Again, these threats may be real or imagined. The obvious concern here is the actual *collision* transfer. However, control options should not wait until a forward collision occurs to begin taking an avoidance action. These actions should be taken while the threat of a forward collision is still a threat. Controlling these threats should be a high priority in AHS design. Such collisions involve an innocent vehicle because of its proximity to another failure or collision—a proximity established by the AHS separation strategy. While we recognize the best strategy for eliminating transferred threats is to eliminate collisions; we also recognize that collisions will

occur, and the AHS should be charged, within the normal control system, with the responsibility to alleviate the resulting domino effect.

Figure 2 is a graphical representation of the relationships between these various threat situations.

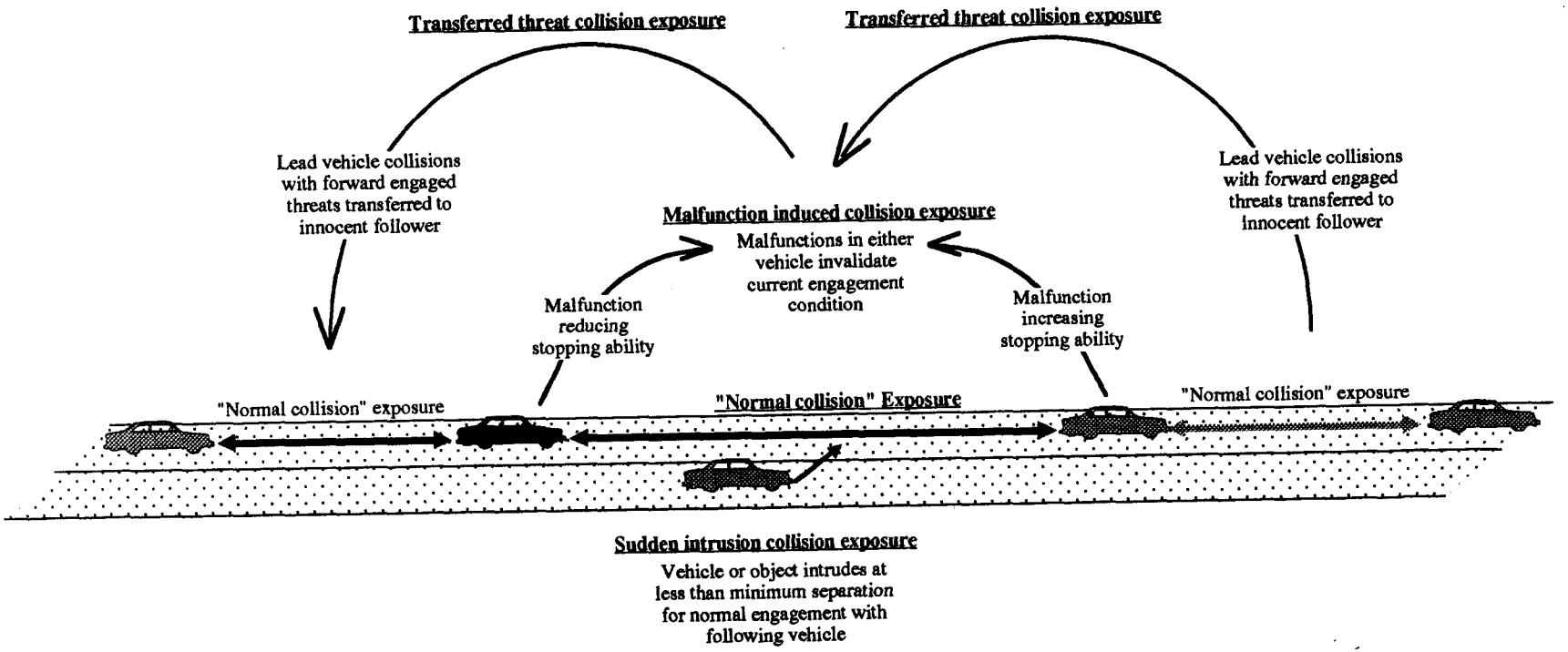


Figure 2. Relationship of normal collisions, malfunction induced collisions, sudden intrusion collisions, and transferred threat collisions.

Threat Agents

The collision situations considered all involve an AHS vehicle and a threat agent. The following threat agents were considered:

- *Fixed objects*. Fixed objects are those threat agents that have no ability to move out of the way. All collision avoidance capability must be provided by the subject vehicle. Included in this category are lane fouling objects from adjacent lanes, dropped loads, intentional placement, etc. No distinction was made on the basis of object size. Obviously, a small object may not represent a real "collision" threat. However, it does represent a threat to control capability—throwing a vehicle off course (bump steer) or inducing wheel-hop at a critical point where lateral and longitudinal control requirements are critical. Transient agents are also included in this category (people and animals). However, because of the unpredictability of their motions, their mobility was not considered in a collision avoidance strategy. Fixed objects also include stopped vehicles—without consideration of why they are stopped. It may be the result of a backup from AHS lane exits or AHS vehicle malfunctions. A more general view of a fixed object includes any impediment to travel that must be managed solely by the stopping characteristic of a vehicle. Therefore, any natural calamity, fire, or hazardous material spill in the lane or adjacent lane is included.

- *Rogue vehicles*. A rogue vehicle is a vehicle that, for whatever reason, is not under some level of AHS control. More than likely, this will be a non-AHS vehicle, on the AHS lane either by design or inappropriate intent.

- *Other AHS vehicles*. An AHS vehicle in this report is always meant to be an AHS-controlled vehicle—controlled, in full, as intended by the particular control protocol in force at the time.

The capability of AHS vehicles to safely coexist with the first two threat agents are considered obligatory engagements. While a number of AHS concepts use various techniques to exclude these agents, it is unwise to assume the absolute effectiveness of these exclusion approaches. An AHS vehicle, for whatever the reason, may revert to manual control or may suffer a malfunction rendering its control reliability suspect. Such vehicles would have to be engaged as a rogue vehicle. Furthermore, AHS operations in rural areas will probably require mixed traffic engagement capability. Therefore, in terms of AHS engagement strategies, we must include *fixed object engagement* and *rogue vehicle engagement* must be included.

Engagements of other AHS vehicles are also obligatory; but a number of engagement options are available. Depending on the demand for system capacity, AHS vehicles may be engaged with different strategies:

1. *AHS compliant engagement*, where separation is based on the "as is" braking capability of the coupled vehicles. This is the minimum capability for an AHS. It is most nearly represented in the spectrum of concepts by terms such as "autonomous control" and

"independent control." Basically, AHS vehicles coupled by this engagement strategy adjust separation on the basis of "as-is, unmodified" worst case assumptions.

2. *Loose platoon engagement*, where brake suppression is employed to reduce braking rates to the value of the minimum capable vehicle. Because the vehicles are similar in braking performance capability, the average separation between vehicles can be less than that required under an AHS compliant engagement.

3. *Tight platoon engagement*, where separation is established at some small, fixed separation. The usual values for this engagement are three to five feet.

Investigative Approach

As indicated previously and illustrated in figure 1, the major focus of the area N investigation was to address the elimination of in-line collisions. Within this focus area, primary emphasis was placed on the elimination of normal collisions. Figure 3 expands this collision type to provide further definition and a further narrowing of emphasis. In this figure, two nodes are crossed out:

1. The node that recognizes the potential of a capability to "steer around" a forward threat agent. Some options using this capability probably exist. However, they are sufficiently problematical that they cannot be expected as a routine option for collision avoidance. If full automatic control is not available for off-line maneuvers, a transition to manual control is required. However, such a transition would come at a very difficult time, under the threat of an imminent collision (an "extremis" condition). Operator performance in this situation cannot be expected to have sufficient consistency to utilize it as an integral part of extremis management. Furthermore, to do so would require the operator to be in a "hands off, feet off, *brain on*" operating mode. While the system should seek to utilize his/her involvement under these conditions, it must be designed to accommodate the safety of the operator in a "hands off, feet off, *brain off*" mode. Therefore, collision avoidance capability is structured to function in-line; that is based on stopping capabilities.

2. The second node eliminated considers "separation controller" faults as enabling an inadequate separation. Separation controllers can be developed to maintain separation relative to some established reference value. Although this is not a trivial assumption, the much larger problem is in establishing the desired reference values such that they reflect real minimum safe requirements. This is the responsibility of the separation manager.

Therefore, area N activities were focused on the separation management fault path: the faults associated with inadequate separation algorithms and inadequate separation management capability. Figure 4 illustrates the general context of these fault nodes as well as the nature of the contributing faults. This figure also illustrates the effects of removing the two nodes discussed above. As indicated in this figure, each of these nodes was developed in detail and are reported in appendices A and B. In these details, the connector between levels is an "OR" gate. Furthermore, faults are

generally stated as “inadequacies” of functionality. As a result, they can be readily converted to functional requirements by replacing all “OR” gates with “AND” gates and replacing the “inadequate” descriptor with “provide adequate.”

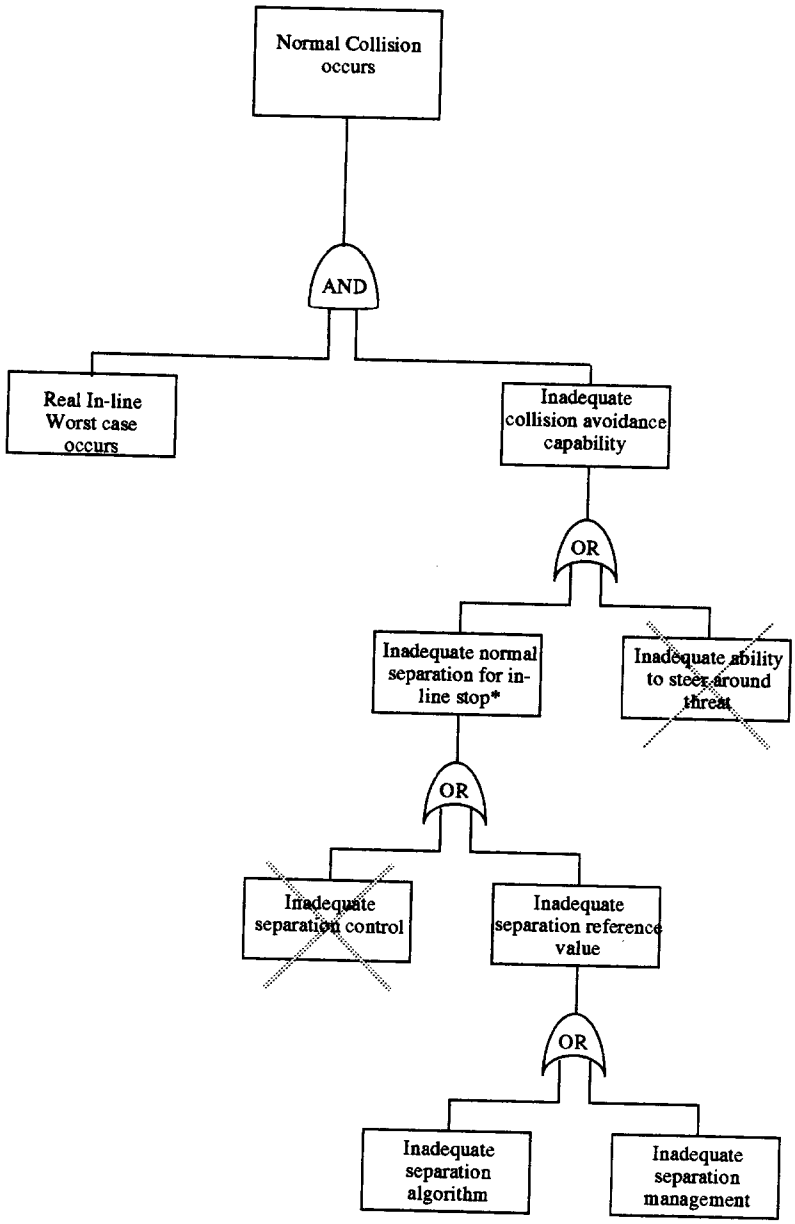


Figure 3. General in-line collision fault path identifying rejected control options.

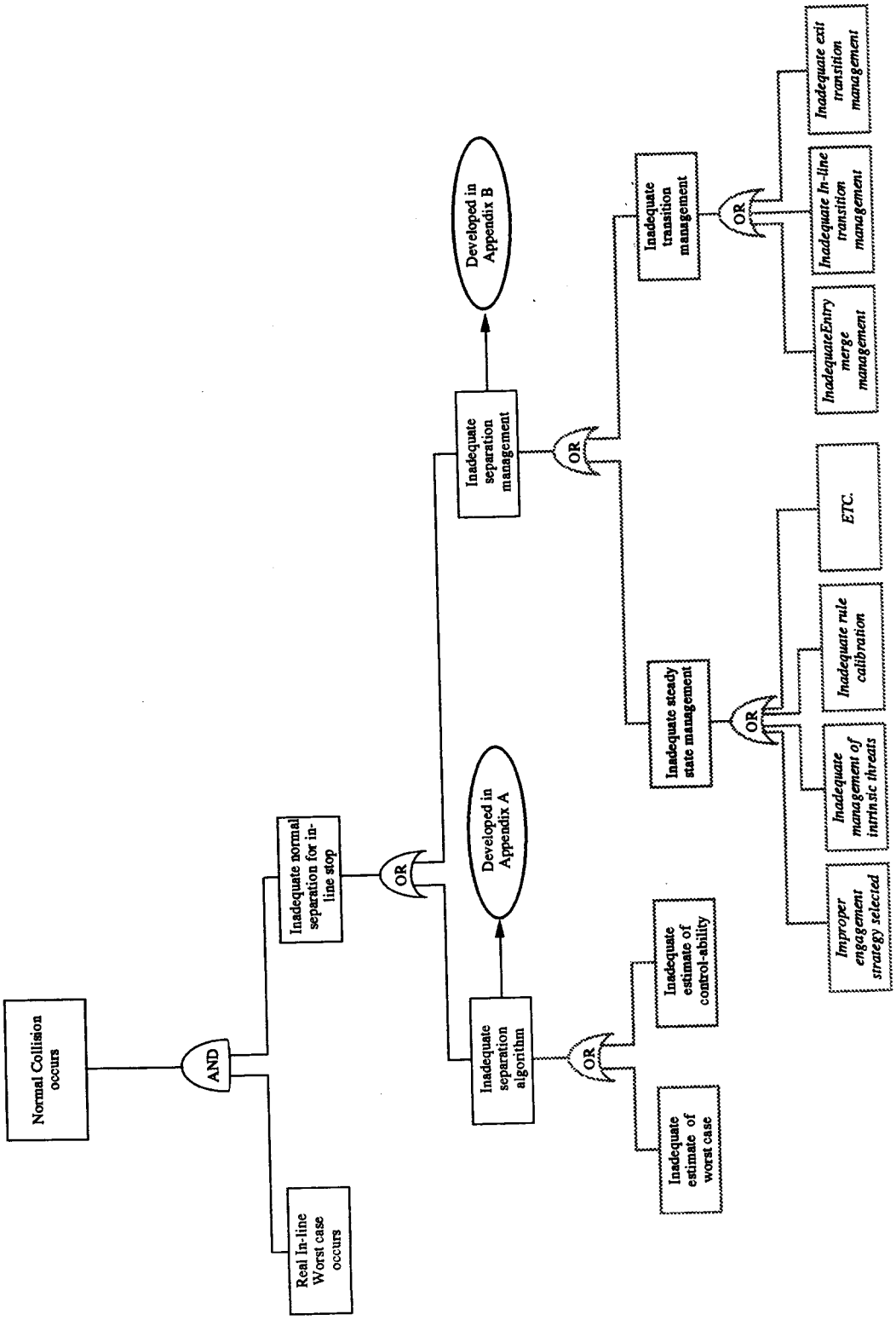


Figure 4. General normal collision fault path expansion.

In addition to the detailed fault development of these nodes, two other concurrent activities were conducted:

1. Detailed analyses were conducted to investigate the separation implications of various engagement strategies and engaged threat agents. These analyses served not only to characterize these separation requirements, but also to identify issues and concerns associated with the requirements for the algorithms and management capabilities.

2. An effort was initiated to develop the functional requirements for the separation management function—a high level capability structure to respond to concerns developed during the analyses addressed in (1) above and from the capability requirements inferred from the detailed analyses in appendices A and B. In addition, the development of a basic concept of operation for the separation manager was initiated. These were embellished as other parts of the investigation progressed.

Previous activities addressed normal collisions. The fundamental skepticism of safety analysis requires the expectation that these collision prevention measures will not be adequate. Furthermore, the collision potential of malfunctions and sudden intrusion threats, as well as the domino effect of transferred threats, result in fault paths that are not controlled to the satisfaction of a safety engineer. While a crucial part of safety management is to divert the fault paths that enable a collision, this is only the first line of defense. We must also include capabilities to accommodate breaches in this line.

The key to accommodating these breaches is conceptual. “Never consider that failures in these preventive measures must inevitably result in a collision. Until the collision actually occurs, purposefully introduced intervention strategies can be effective, if not to eliminate the collision, at least to reduce its severity.” This concept is illustrated in figure 5, which also includes the four collision threats investigated. As illustrated in fault tree representations, intervention actions are introduced as strategically placed “AND” gates. The intent is to create a tortuous path for any fault to reach a collision level. As illustrated in this figure, intervention options are placed at two levels in the fault stream:

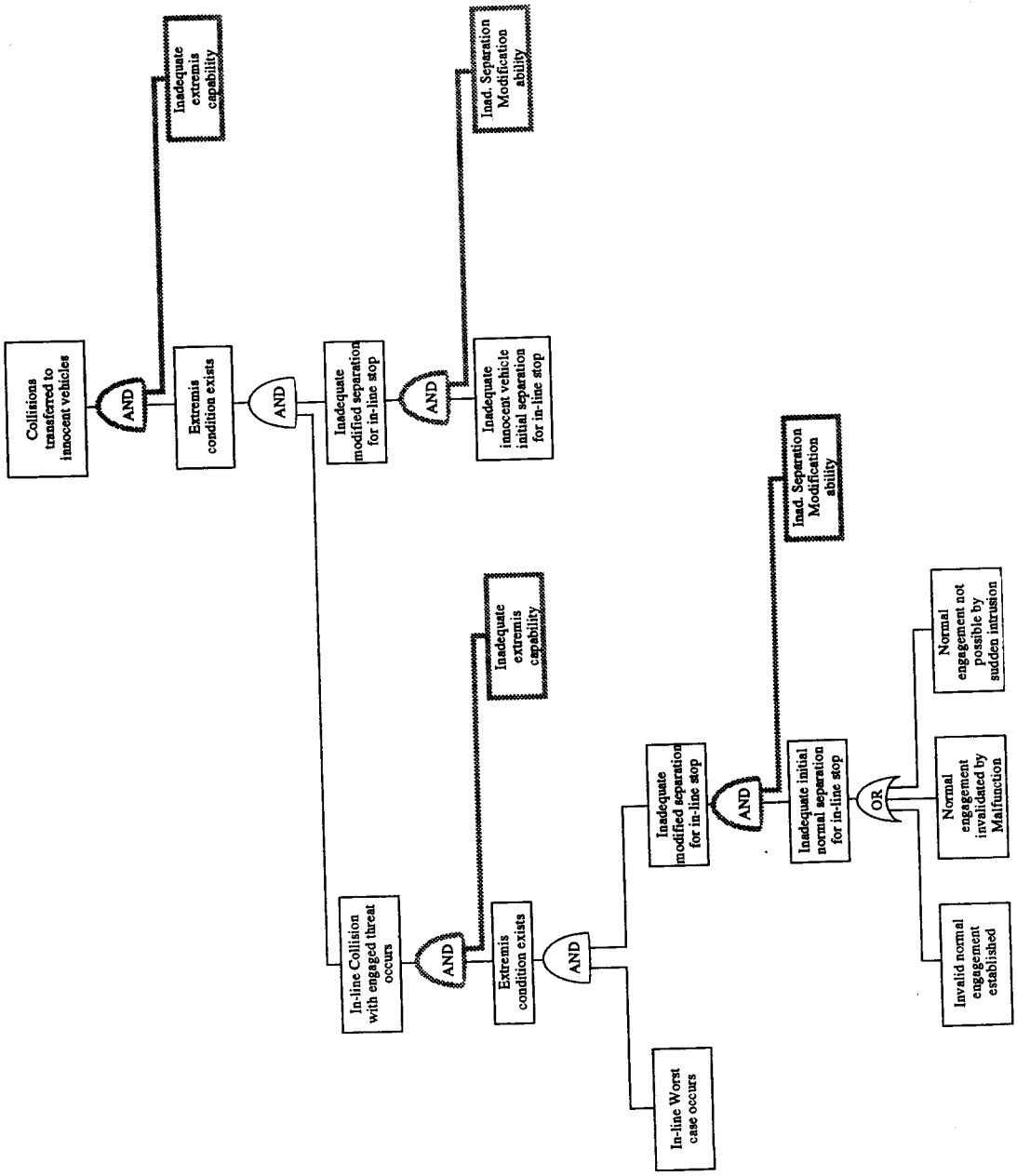


Figure 5. General fault paths identifying fault intervention strategy.

1. One is positioned such that it can intervene before a worst case encounter for the purposes of correcting the separation inadequacy. In all of the situations investigated, the proper corrective action was always to increase separation to a value that could tolerate the worst case. No scenarios were found where this was not a desired intervention action.

2. The second intervention option involves the imposition of emergency maneuvers in extremis conditions (conditions that result from the ability to be successful with the first intervention option). These actions can still be effective in eliminating the apparently imminent collision.

A number of analyses were conducted to characterize the collision situations from the four sources considered and to explore the effectiveness of various strategies. The results of these analyses were folded into the separation manager fault tree, as well as the functional requirements and concept of operation for the separation manager.

In all analyses that examined chain collisions, a basic centerline, front-to-rear collision model was used. This model assumed no centerline offset between vehicles prior to the collision and no offset or vehicle rotation was induced by the collision.

Report Organization

The remaining sections of this report are organized as follows:

·*Collision Avoidance Considerations.* This section contains background information on the nature of the in-line collision causes from the viewpoint of the human operator in current driving situations and from the viewpoint of implied requirements for AHS separation management.

·*Normal Collision Avoidance Separation Implications.* This section contains the results of the analysis of normal collisions. Charts are included to characterize the separation requirements and the implications of selected influencing variables.

·*Collision Threat Intervention Strategies.* This section contains the results of the intervention analysis. Charts are included to characterize the collision events and the influence of intervention strategies. From these, the required capabilities of intervention actions were developed.

·*Separation Manager Implications.* This section contains the required capabilities for the safety manager to effectively control separation.

·*Findings and Conclusions.* This section contains selected issues and concerns that emerged during these investigations. These are highly aggregated and by no means constitute an exhaustive list.

·*Appendix A* contains the detailed fault representation of the fault node identified as “inadequate separation algorithm” in figure 4.

·*Appendix B* contains the detailed fault representation of the fault node identified as “inadequate separation management” in figure 4.

·*Appendix C* contains selected issues and concerns relative to threat situations outside of our focus area. These are largely unsupported and, in a sense, this appendix contains issues and risks “not elsewhere classified.”

· *Appendix D* contains a detailed description of the Representative System Configurations for the AHS considered in this research.

COLLISION AVOIDANCE CONSIDERATIONS

Eliminating in-line collisions is often assumed to be a significant benefit of an AHS. At the same time, it is assumed that this benefit will accrue as a natural by-product of automation—based on data that suggest that most of these collisions are caused by "human error." Because automation will replace the human on the control loop, it is assumed that this accident cause will naturally disappear. This may be a false hypothesis. There is a growing perception that human error in this context is not nearly as related to error as might be implied. Analysis of these types of accidents supports a thesis that these human errors are rather a reasonably expected response under the conditions of information and control capability that exist at that time. In other words, the standard of performance used as a reference for determining error is itself being questioned. Without a doubt, when we automate the human driving functions, we will demand greatly enhanced capabilities in situation awareness, decision prowess, and control options than we currently have available in our manual system. It is important to understand these distinctions to ensure that the AHS does not simply automate the same frailties that currently exist in the manual systems. To force this result, it is necessary to understand the factors underlying human error that enable in-line collisions to occur.

Separation Management From the Human Perspective

It is rather easy to identify the cause of in-line collisions as human error because it is so bottom-line oriented. The bottom line cause of in-line collisions is inadequate separation—for whatever reason. Because safe separation management and control is delegated to the driver, it is clearly his/her fault, generally expressed as "failure to maintain assured clear distance." Another cause less frequently mentioned is "driving too fast for existing conditions." Even this cause, however, is related to insufficient separation under the conditions that exist. If a collision occurs, it is clear that the separation prior to the collision was insufficient to enable the trailing vehicle to respond to the demands imposed by the motions of the leading vehicle.

To develop an appreciation for this problem, the components of safe separation management must be identified. Was the separation inadequate because the driver could not or did not *maintain* a desired separation (functional error)? Or, was the cause a failure to *establish* the correct desired separation (judgment error)? Figure 6 illustrates these differences in the form of a control schematic diagram. The emphasis on the "functional" side—separation control—is not intentional; it is the result of the fact that we know a lot about automation of *function*; we know less about automation of *judgment*. (This figure also defines roles for a "separation manager" and a "separation controller." Throughout the remainder of this report, required capabilities will be added to these functions).

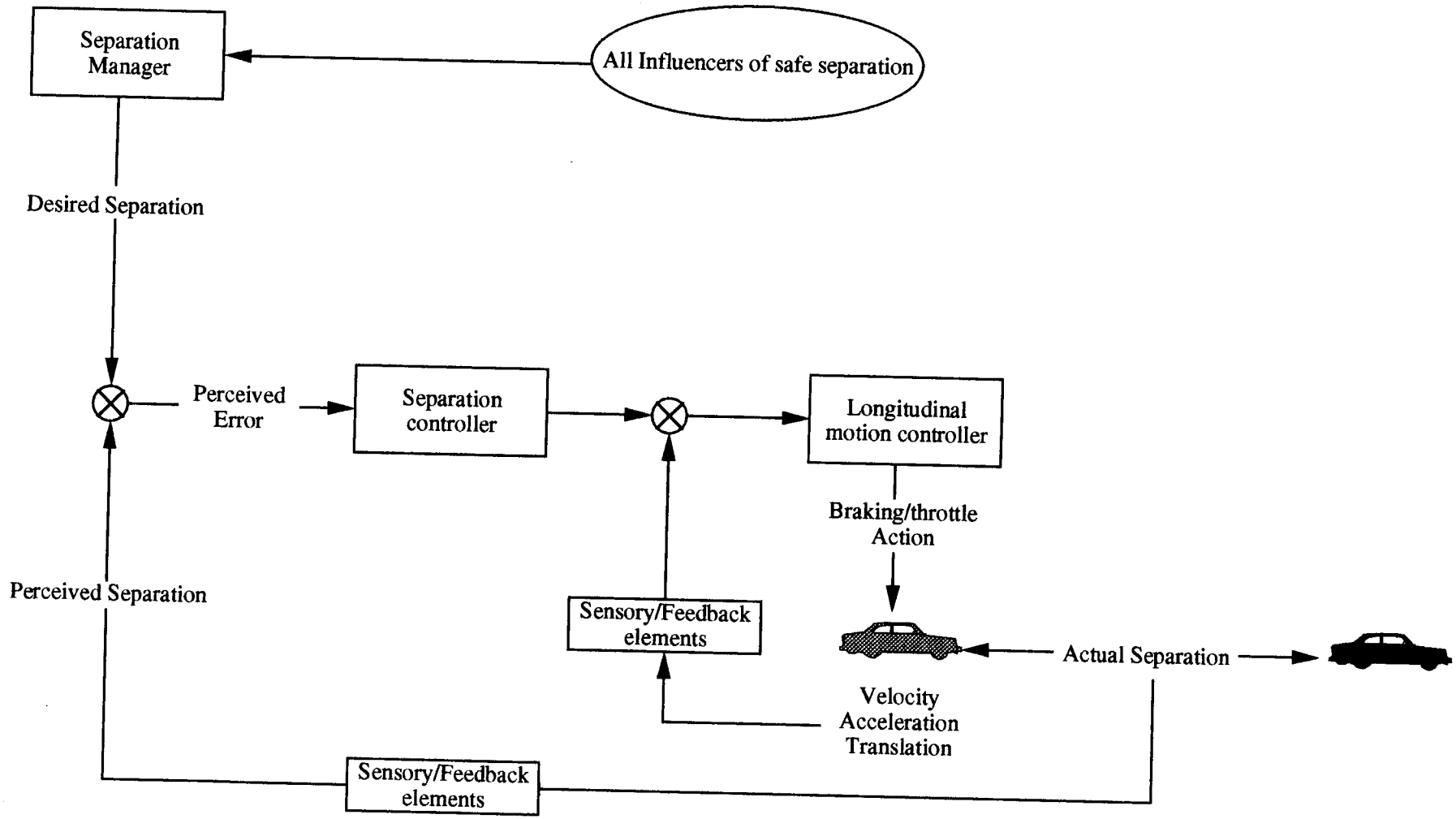


Figure 6. Relationship of function and judgement in maintaining safe separation.

Over the last 25 years we have had occasion to analyze hundreds of accidents, from all transportation modes, have been analyzed to gain an understanding of the role of the human operator. These analyses have led to the following observations:

- The human operator is quite adept at following a defined course of action—executing an hypothesis. A small portion of human error may involve actual mechanical errors of function (steering the wrong way, accelerating rather than braking, etc.). However, humans, as a group, are quite competent and consistent in this role. The greatest failings in this regard are associated with failure to maintain diligence: complacency, fatigue, boredom, expectancy, habit interference, drug/alcohol influences, and the like.

- The majority of human frailties are associated with forming a hypothesis—the judgments and decisions that establish the reference values that drive the mechanical control actions. This type of error has led to a concept of guided collisions, where a vehicle is driven, under full and purposeful control, into an uncontrollable situation.

Clearly, functional errors are leading candidates for elimination as a natural by-product of automation. In its minimal form, any separation controller must be capable of maintaining some desired separation value or set point. The separation controller is the tool used by a separation manager function (or an overall safety manager function) to execute the separation requirements it establishes. In any AHS proposal, the characteristics of the separation controller form a portion of the givens that must be accommodated in establishing the safe separation set point. (This implies that separate black boxes must exist for each function. This is not intended, nor is it a requirement. However, experience has proven the wisdom of separating safety systems from operating systems. Also, in our generic approach, there is no assumption that the separation manager is vehicle-based—as opposed to infrastructure-based. The separation controller will probably be vehicle-based to execute separation commands, regardless of their source, but even this is not a pre-determined requirement).

However, addressing functional errors (i.e., automating “function”) will not achieve the safety goal. This goal can only be reached by successfully automating the judgments involved; that is the decisions that establish the correct desired separation. Based on our accident analyses, two recurring themes emerge for almost any human control inadequacy:

1. We tend to underestimate the worst case interaction that may exist between our vehicle and a threat agent; including:

   - underestimation of the magnitude of the threat, and
   - overestimation of our ability to control it.

2. We tend to assume the worst case will *not* occur.

The implication is that people drive at a separation that is technically less than safe. By almost any yardstick for measuring minimum safe separation, observed separation is inadequate. It is almost

axiomatic that if a worst case situation arises, collisions will result. Examples of purposeful entry into unsafe situations are that:

1. We readily close on a lead vehicle in a passing maneuver. We approach to small separations and a significant speed differential. If the lead vehicle were to suddenly stop, at even a modest rate, we would most likely collide.

2. We readily close on a vehicle slowing for a turn or lane change under the assumption that it will vacate the lane space before we need it. If that vehicle were to suddenly stop, we would most likely collide.

3. We readily close on a merging and accelerating vehicle under the assumption that it will get out of our way. If it were to suddenly stop, we would most likely collide.

4. We readily merge into gaps that, sometimes, are barely longer than the vehicle. There is a lot of trust involved in this maneuver. Any number of conditions could occur that would result in a collision, but we trust they will not occur.

Other examples would only reinforce the point that there is a tendency to ignore the potential for a worst case demand occurring at a very vulnerable time. However, this is a *calculated* risk. We use confidence and trust in the lead vehicle to not behave in an unexpected manner. If it begins operating in an erratic behavior, that is, invalidate the trust, we increase our cushion. We use "threat transfer" management techniques to isolate us from conditions that may force a sudden and drastic maneuver on the part of the lead vehicle by looking ahead and identifying situations that may cause this and taking action before the lead vehicle forces us to respond in an emergency manner. In these cases we actually use a "negative delay"—an approach very similar to "braking from the rear" approaches in AHS concepts. Further, in very close quarters, our threat concern may cause us to be ready to apply brakes in fractions of a second, compared to the one to two seconds exhibited in a more leisurely environment.

Separation Management From the AHS Perspective

The significance of these observations for AHS is that:

1. They outline the safety task of an AHS for safe separation management, i.e.,:

   - Do *not* underestimate the worst case interaction, and
   - Assume that the worst case *will* occur.

2. They provide background to explain why, depending on the particular operational conditions, the separation requirements for an AHS are greater than we currently observe—perhaps significantly so.

3. The driving public is accustomed to the risks involved and have accepted them. However, the public may not have any logical stance on risk. De facto risk acceptance by the public has been used for decades as a decision rationale and a marketing approach. The prediction and demonstration of very low risk to the public of nuclear power plants illustrates the problem of assuming de facto risk acceptance. In spite of risks that are orders of magnitude lower than risks associated with childhood diseases, we have not made significant strides in consumer acceptance of power plants.

4. The techniques we use to limit our risk to a comfortable level have direct functional counterparts in AHS control strategies, i.e.,:

   · The use of confidence and trust in establishing and maintaining an engagement.

   · Forward threat awareness to reduce transferred threat exposure.

   · Incredible (and, at that, still limited) situation awareness and powers of observation that allow a panorama of signals to be assessed to isolate the signal that is relevant to a particular action.

The bottom line is that there is no quantitative information regarding what constitutes “adequate” (except for some rules of thumb). We have ample evidence of what is *not* adequate—whatever the separation was before a rear-end collision occurred. The AHS will not be allowed to operate in this intelligence vacuum. Establishing and maintaining separations based on a sound perception of safe separation requirements is the fundamental requirement if a no-collision environment is to be achieved.

General Principles of Minimum Safe Separation

Figure 7 shows the relationship between three separations and the variables influencing them (steady state conditions):

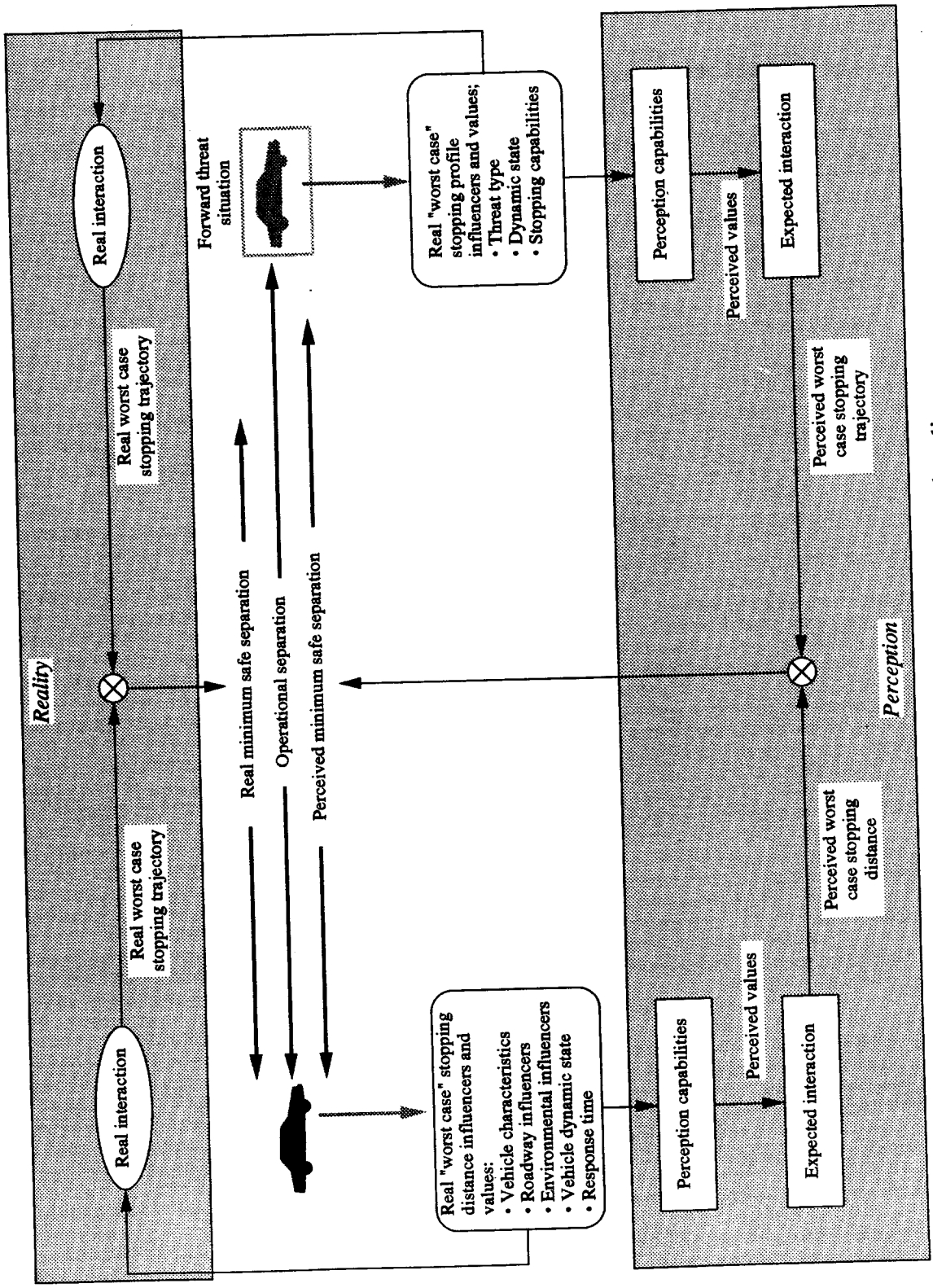


Figure 7. Safe separation perception and reality.

1. **Operating minimum separation (operating min Δ)**. The separation established as a desired value by a operational decision; the separation "set point" used as the reference value for the separation controller. This may be set as a constant or a variable dependent on some dynamic parameter such as separation time or vehicle velocity. Operating separation is an operational decision. Any algorithm is acceptable, as long as it results in separations greater than the real minimum safe separation—as conditioned by perception.

2. **Perceived minimum required separation (perceived min req Δ)**. The minimum separation for a no-collision situation based on assumed interactions between the perceived values of influencing variables. This is our best estimate of the real minimum required separation. The calculation is based on the expected worst case stopping trajectory of the forward threat object and the expected worst case stopping capability of the following vehicle—the minimum stopping capability under maximum vehicle performance. Conditions influencing this minimum stopping capability are the minimum value of the maximum braking rate (min-max BR) over the stopping profile and the maximum value of the minimum response time to initiate this maximum braking capability (max-min Td).

3. **Real minimum required separation (real min req Δ).** This is the result of the *real* interaction of the *real* influencing variables at their *real* values as they influence the *real* worst case threat agent stopping profile and the *real* maximum stopping trajectory of the following vehicle.

For a no-collision situation, under the worst case conditions, these separations must be related as follows:

Operating min Δ ≥ perceived min req Δ ≥ real min req Δ

In the absence of any demand for capacity, the separation manager (performing the perception function) has a very easy task: estimate reality using a very unsophisticated approach and very conservative estimates for the influencing variables. The separation manager will then add an additional cushion to account for unknowns, and multiply it by a factor that accounts for additional unknowns and lack of precision. The manager may also seek to avoid the responsibility for even a modest amount of real-time monitoring of conditions and base the separation on assumptions that the road will always be icy or snow covered. This value is then passed to the separation controller, to be used as the desired separation. Before passing on this value, the separation manager may also add a further cushion to account for functionally deficient controllers (e.g., inadequate sensing capability, large transient characteristics, significant steady state error, etc.).

This scenario probably represents the situation most safety engineers would like to engage. The problem is that it would completely destroy the capacity of the highway. At 60 mph, the resulting separations would be several hundred feet, resulting in capacities well below 1,000 vehicles per hour.

The separation manager, therefore, cannot operate in such an unconstrained environment. The demand for capacity that significantly surpasses current freeway values creates pressure on the separation manager to allow decreased separation without sacrificing collision avoidance goals.

The first opportunity to reduce separation is to increase the separation controller's functional competence to increase the precision with which it can control actual separation about a set point. This allows the set point to become very close to the perceived minimum separation requirement. However, in this scenario, this may be of little value.

To further reduce separation and still ensure safety requires sharpening the perception of the real separation requirements. This requires enhanced knowledge of influencing variables and their qualitative and quantitative role in determining minimum safe separation. It also requires operating in real time (as-is conditions) to permit adjustments to requirements as conditions change (weather, etc.) An implicit corollary is the need for enhanced situation awareness capabilities to provide the precision necessary to support this as-is decision capability. Incorporating this capability into the separation management function can significantly reduce operating separations while maintaining confidence in collision avoidance capability. However, separations may still be unacceptable (from a capacity view).

It is important to note that, throughout this process, the real required minimum separation has not changed. What has changed is the precision with which its value can be estimated.

The above approaches to separation reduction share a common characteristic: they are all responsive to uncontrolled real-world situations. Separation is the dependent variable—adjusted as necessary to respond to a perception of reality that is basically uncontrolled. The following logic is employed:

IF<threat situation>; **THEN**<separation>; **ELSE**<.....>

This logic structure is the basis for AHS engagements with fixed objects, rogue vehicles, and AHS compliant engagement with other AHS vehicles.

Following this logic, even with the best of intelligence, we are limited in how far we can go in reducing separations. Very small separations may be allowed between certain vehicle pairs because of their performance capabilities. However, very large separations will be required for other vehicle pairs. To reduce the average separation, we must increase the population of the vehicles capable of safely operating at small separations. This can be accomplished by reducing the variations in performance. This process changes the above logic statement so that it appears to be as follows:

IF<separation>; **THEN**<threat situation>; **ELSE**<.....>

In other words, if we want very small separations, we must first create the population that can function safely at these separations. Next, we must limit the opportunity to engage at small separations to vehicles in that population.

A primary technique for promoting consistent vehicle performance is to suppress the performance of the most capable vehicle to that of the worst performer. We have chosen to identify engagements that require or take advantage of capability suppression procedures as platoons. Two types of platoons represent different approaches that span the range of options:

1. A loose platoon is composed of vehicles where the stopping capabilities of the most capable vehicles have been suppressed to the levels of the least capable vehicle. A suppression action would make all vehicles equal. Separations between these vehicles can approach a fixed time criterion, approximately equal to the response time of a vehicle.

2. A tight platoon is a platoon in which the lead vehicle performance is suppressed to a value significantly below that of the least capable vehicle to enable following vehicles to consistently possess a capability superior to that of the leader. In this arrangement, minimum safe separations can approach a small fixed distance.

Managing safe separations for these engagements requires emphasis on establishing the credentials of a vehicle to ensure that it is capable of following the rules in cooperation with other vehicles in the platoon.

NORMAL COLLISION AVOIDANCE SEPARATION IMPLICATIONS

This section explores some of the variables to be considered in establishing a minimum safe separation between an AHS vehicle and the forward threats faced in a normal collision environment. The results of these analyses are not intended to be definitive—as would be necessary for design decisions. They are rather intended to be illustrative—to illustrate the minimum separation effects of selected influencing variables.

Normal Collision Definition

A collision is defined as straight line trajectory interference: the worst case maneuver of the threat agent creates a boundary that cannot be crossed by the braking trajectory of the threatened vehicle. A "normal collision" is a collision that could occur under the conditions expected in a normal engagement of an AHS vehicle with a threat agent. A "normal engagement" exists when the AHS vehicle and the threat agent are operating within the limits of normal capabilities; i.e., when performance of neither entity is influenced by malfunctions or conditions that are considered to be within the design range.

In most cases, where the worst case trajectories can be approximated as constant accelerations, trajectory interference will occur at the end of the maneuver and the separation requirement resolves itself into the difference in stopping distances. This type of control is termed "endpoint" control conditions. For engagements where the braking capability of the threatened vehicle is greater than that of the threat agent, endpoint control is not a valid indicator of trajectory interference. Even if end conditions are satisfied, trajectory interference will occur during the maneuver. A similar situation exists for very small separations where the distance traveled during the response time of the threatened vehicle is greater than twice the desired separation. We may refer to these situations as "midpoint" control conditions.

In these analyses, minimum safe separation is defined as the perceived minimum separation that will allow an AHS vehicle to avoid a normal collision with a threat agent. The avoidance capability is constrained to straight line braking. We did not include lane changing or other evasive maneuvers as a viable collision avoidance strategy for these normal collisions. This does not discount the value of evasive maneuvers in extremis situations (situations where a collision is imminent).

Separation Analysis Assumptions

The models used for the analysis of separation requirements were not sophisticated. They were the basic equations of motion evaluated at 0.05 second time intervals. Where possible, all analyses used a common set of assumptions. In general, unless otherwise indicated, the following assumptions apply:

- All accelerations for both worst case and response trajectory definition were assumed to be constant.

- Acceleration changes were assumed to occur instantaneously (infinite jerk).

- All reaction or response times were assumed to be 0.3 seconds. This represents the time delay between the time a worst case demand is initiated and full application of braking rate by the threatened vehicle. While this value may include signal delays, once the signal is received, it becomes perfect with no delay. This means that the virtual reality developed by the signals is a perfect representation of reality.

- Trajectory interference assumed zero separation as acceptable (tangent paths). No allowance was established for a minimum separation at the end of the encounter.

- All braking rate estimates were based on conditions that represent test conditions used by popular automotive magazines for production automobile brake tests (clean, smooth and dry road conditions). The minimum and maximum vehicle braking capabilities were based on the results of these tests for recent production vehicles, most equipped with ABS.

Figure 8 shows the results of a number of these braking tests, as well as the constant braking rates selected to represent the range. By using these values, the separation estimates are probably biased toward minimum values. Additionally, the minimum separations derived are based *solely* on trajectory interference. The implications of this assumption is that no other influences are operating; such as a separation controller that imposes operational limits or sensor capabilities that may restrict separations.

Steady State Separation Implications

This section discusses the separation requirements under steady conditions, such as those a line of vehicles traveling at the same velocity would present. The question asked in this section is: What is the required separation to avoid a collision under a worst case maneuver of a leading vehicle?

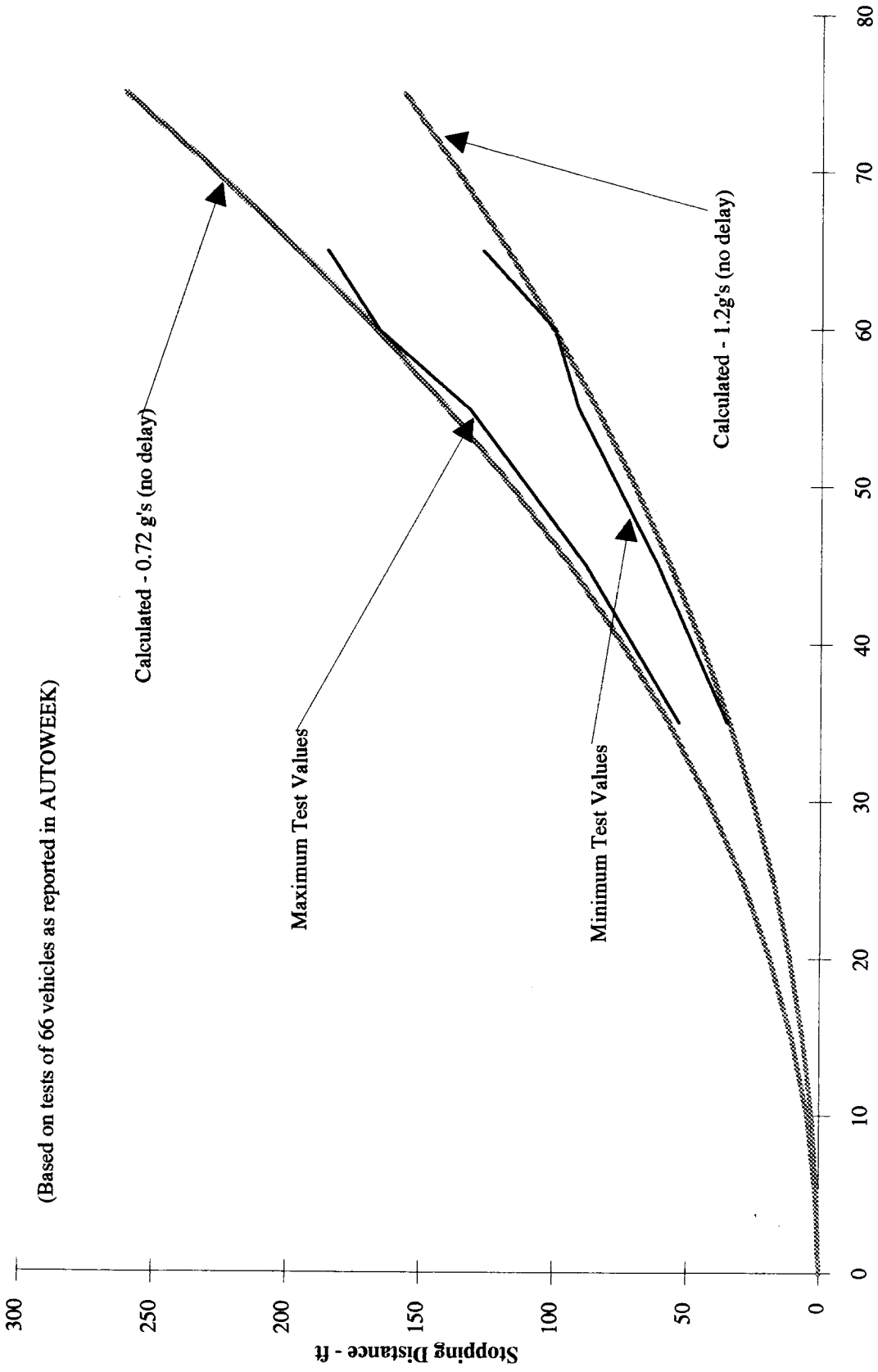


Figure 8. Production vehicle brake test results.

Five steady state engagement strategies are examined—generally classified on the basis of the expected worst case maneuver. The first three examine the separation implications to safely engage the various threat agents identified previously:

1. Fixed objects.

2. Rogue vehicles.

3. Other AHS vehicles.

Three different concepts of engagement between AHS vehicles were assumed, reflecting the range of options reflected in most AHS concepts:

1. AHS compliant.

2. Loose platoon.

3. Tight platoon.

The following sections illustrate the implications on separation requirements to provide adequate avoidance capability for these collisions under the engagement strategies listed above. Many charts are presented to illustrate the influence of selected variables within the context of the strategies outlined above. It is emphasized that these are for *illustrative* purposes only. They are *not intended to be definitive,* in the sense that they could be translated into real operational strategies. Their purpose is to indicate relationships that may not otherwise be considered and to foster some appreciation for the level of intelligence and control rigor that accompanies these strategies.

Fixed Object Engagements

Figure 9 shows the stopping distances of vehicles with selected braking rates. Included are the results of professional braking tests reference in figure 8, as well as curves to represent various AASHTO guidelines under various conditions. All curves reflect a response delay (Td) of 0.3 secs. The AASHTO wet curve is overlaid with a constant braking rate of 0.3 Gs, to illustrate the influence of our assumptions of fixed braking rates in these analyses. Also, 0.3 Gs is a common value referenced as the suppressed braking rate of the leader. The relationship of a loose platoon leader to a fixed object is illustrated by the curve labeled 0.72 Gs. Separation from a fixed object for AHS vehicles that are allowed to use their full braking capability are illustrated by the area bounded on the top by the 0.72 G curve and on the bottom by the 1.2 G curve (representing the range of capabilities present in production vehicles).

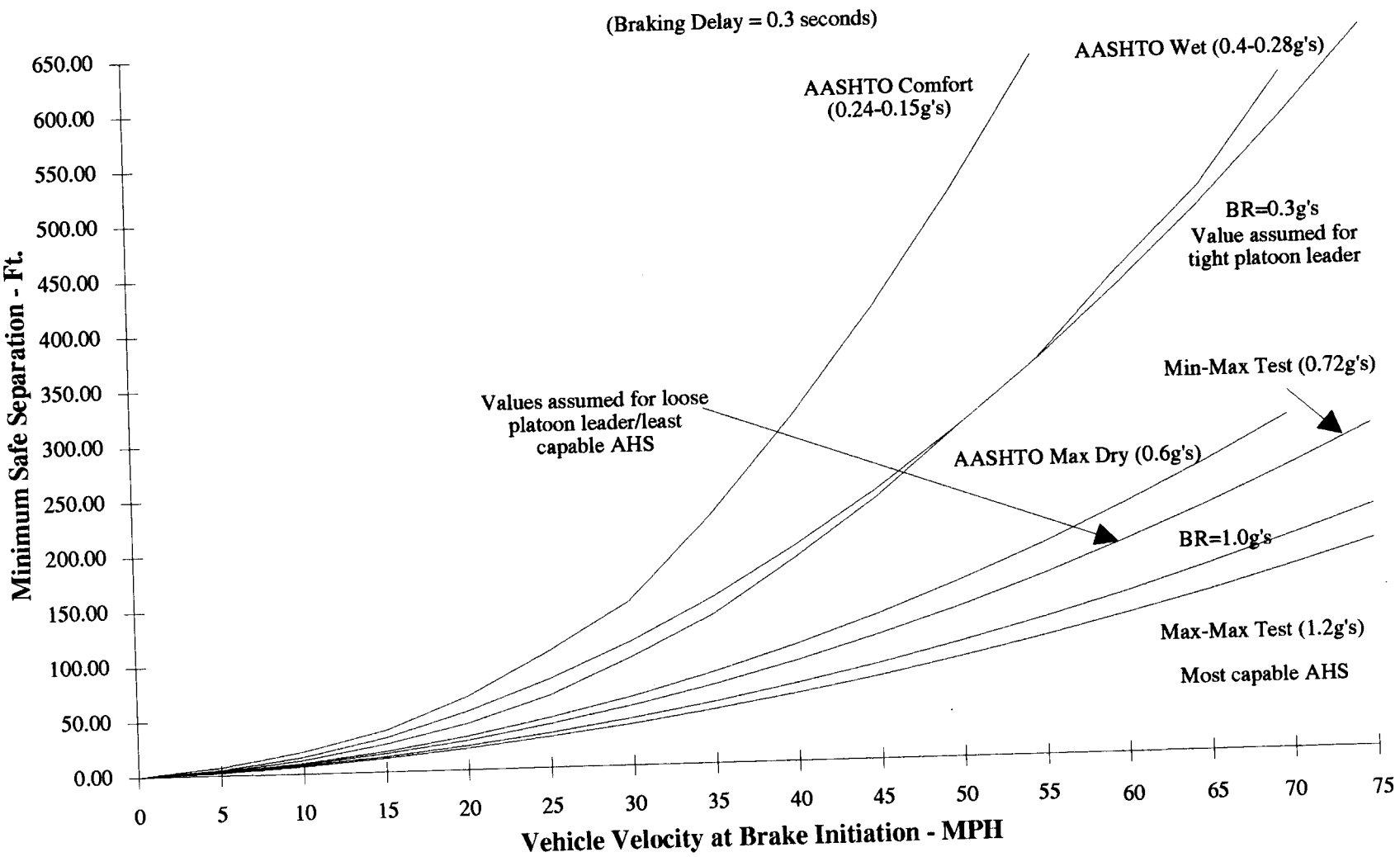


Figure 9. Minimum safe distance to fixed object for selecting braking rates.

It is difficult to grasp the concept of a steady state engagement with a fixed object. It becomes easier if we consider a fixed object to be a leading "phantom" vehicle with an infinite braking rate traveling at the same velocity as the following vehicle. The stopping distances shown are the minimum separation distances required to engage a fixed object. With no intervening vehicles. we assume this phantom vehicle is just outside the stopping distance of the following vehicle. The following vehicle must adjust it sensor range to this value.

While this engagement strategy is nominally related to a fixed object, it is also the appropriate strategy for a "least knowledge" engagement. If we know nothing about a detected leading object, a fixed object must be assumed. Also, if we know nothing about our as-is braking capability, we would calibrate our separation equation to represent a low braking rate. This situation is identical to the least knowledge scenario discussed in the general principles of safe operation section.

Rogue Vehicle Engagements

Figure 10 shows a number of curves of separation requirements for vehicle pairs with 10 selected braking rate ratios. The values selected for display correspond to those relevant to the range of vehicle-to-vehicle engagement strategies considered as candidates for AHS. This master chart will be used for all the vehicle-to-vehicle engagement strategies to follow. It will be tailored as appropriate, but will maintain the overall content to enable a relational perspective as each strategy is discussed.

Figure 11 shows the tailored version for engagement of an AHS vehicle and a rogue vehicle (a moving vehicle not known to be under AHS control). The darkened curves represent the separation required by an AHS vehicle assumed to be operating in an unrestricted node (defined in the next section as an AHS compliant operation). This is the operating strategy that results in the smallest separation requirements from a rogue. The two accented curves show the range of separation requirements under the assumption the rogue vehicle can stop at 1.2 Gs.

As will be shown in the following section, engagement of a rogue by an AHS compliant vehicle lies within the spectrum of engagement between two AHS compliant vehicles. It is treated here separately because it represents another level of assumption that must be made to substitute for knowledge. Rogue engagement must be assumed whenever our knowledge is limited to the fact that a threat agent is a moving vehicle and its motion parameters are known, with no knowledge of how it is being controlled. The rogue vehicle also represents the worst situation for rear engagement.

As shown in figure 11, at 60 to 70 mph, the minimum separation between an AHS vehicle ranges from approximately 40 feet for the maximum capable AHS vehicle to approximately 125 feet for the least capable AHS vehicle.

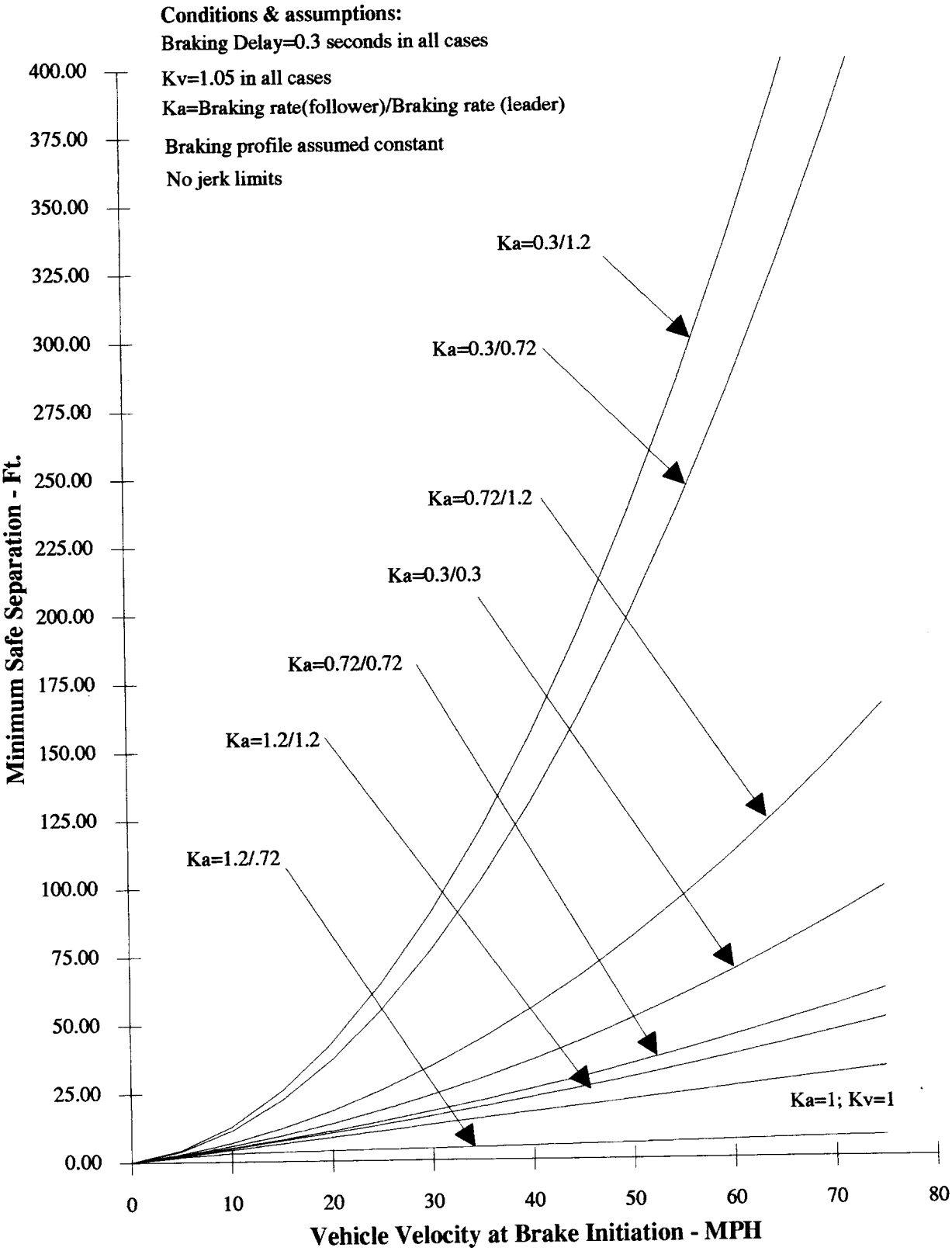


Figure 10. Curves illustrating minimum separation requirements between vehicles with different stopping capabilities.

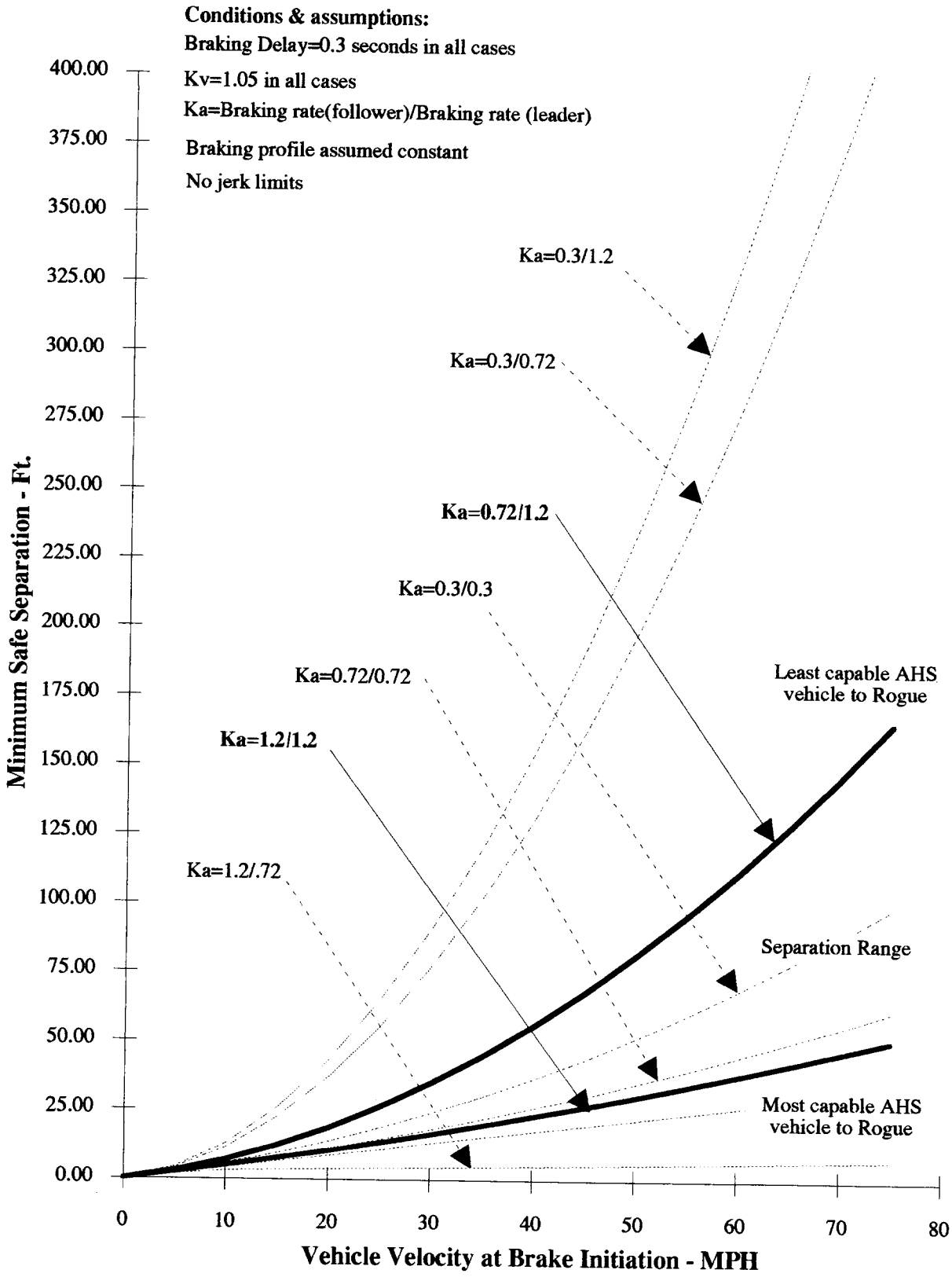


Figure 11. Curves illustrating minimum separation requirements between vehicles with different stopping capabilities tailored for rogues.

AHS Compliant Engagements

This engagement strategy is an extension of a rogue vehicle engagement; but, in this engagement, the leader is an AHS vehicle capable of communicating its "worst case" threat potential as a leading vehicle—the maximum value of its maximum braking capability. This permits the minimum separations achievable between two AHS vehicles for as-is conditions. It also represents the minimum engagement for AHS vehicles—autonomous vehicle controls with separations between vehicles based on a known and trustworthy worst case potential.

The range of separation values attainable for this engagement is shown in figure 12. The upper bound is the same as for engagement with a rogue. The lower bound is considerably less than attainable with a rogue. Depending on the characteristic of the population of vehicles, an average separation will evolve that is lower than that attainable for rogue engagements. The lower bound illustrates the need for an overbearing follower to achieve very small separations (Ka > 1.0).

The nominal threat information requirement for this engagement is knowledge and communication from the leading vehicle that it is an AHS vehicle. We do not need to know whether that worst case is being suppressed; we simply need to know what it is and have a high degree of confidence that the lead vehicle is capable of compliance.

As shown in figure 12, at 60 to 70 mph, the separation between AHS vehicles under this rule can range from a few feet for the most capable vehicle following a least capable vehicle to approximately 125 feet for the reverse situation. The required separation to a rogue vehicle is not changed from that addressed in the previous engagement strategy—approximately 40 feet for a maximum capable AHS vehicle to approximately 125 feet for the least capable AHS vehicle.

Loose Platoon Engagements

The loose platoon uses suppression of vehicle braking capabilities to reduce worst case situations as a tool for reducing minimum separation requirements between AHS vehicles. Figure 13 shows the separation implications of this form of engagement. The lower curve represents the minimum separation between vehicles if both were constrained to a value that represented the minimum capable vehicle (0.72 Gs in our examples). As illustrated, this separation is still slightly velocity sensitive, but is approaching a fixed time separation. If all AHS vehicles are similarly constrained, intra-platoon vehicle spacing could be equal. Under this engagement strategy, impact of the inverse relationship between capacity and velocity would be reduced.

The upper curve illustrates the separation of an AHS loose platoon leader with a rogue vehicle or a leading maximum capability AHS vehicle operating in AHS compliant mode. The minimum separations between AHS vehicles under a loose platoon strategy are considerably higher than the

minimums achievable under AHS compliant rules. The reason is, of course, because AHS compliant rules could respond to braking rate ratios (Ka) greater than 1, while a loose platoon uses Ka values that approach 1.0.

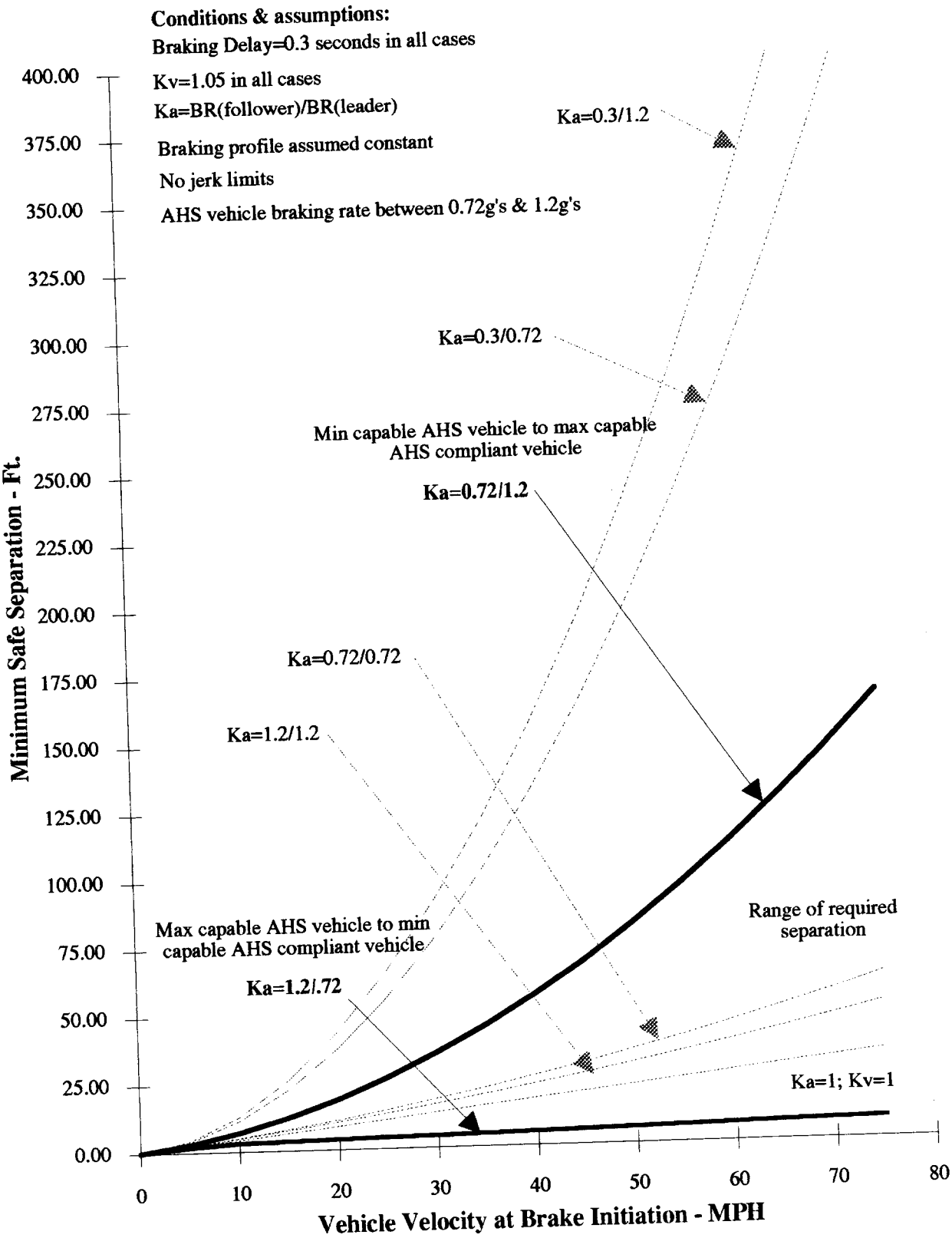


Figure 12. Curves illustrating minimum separation range requirements between AHS compliant vehicle and forward threat agents.

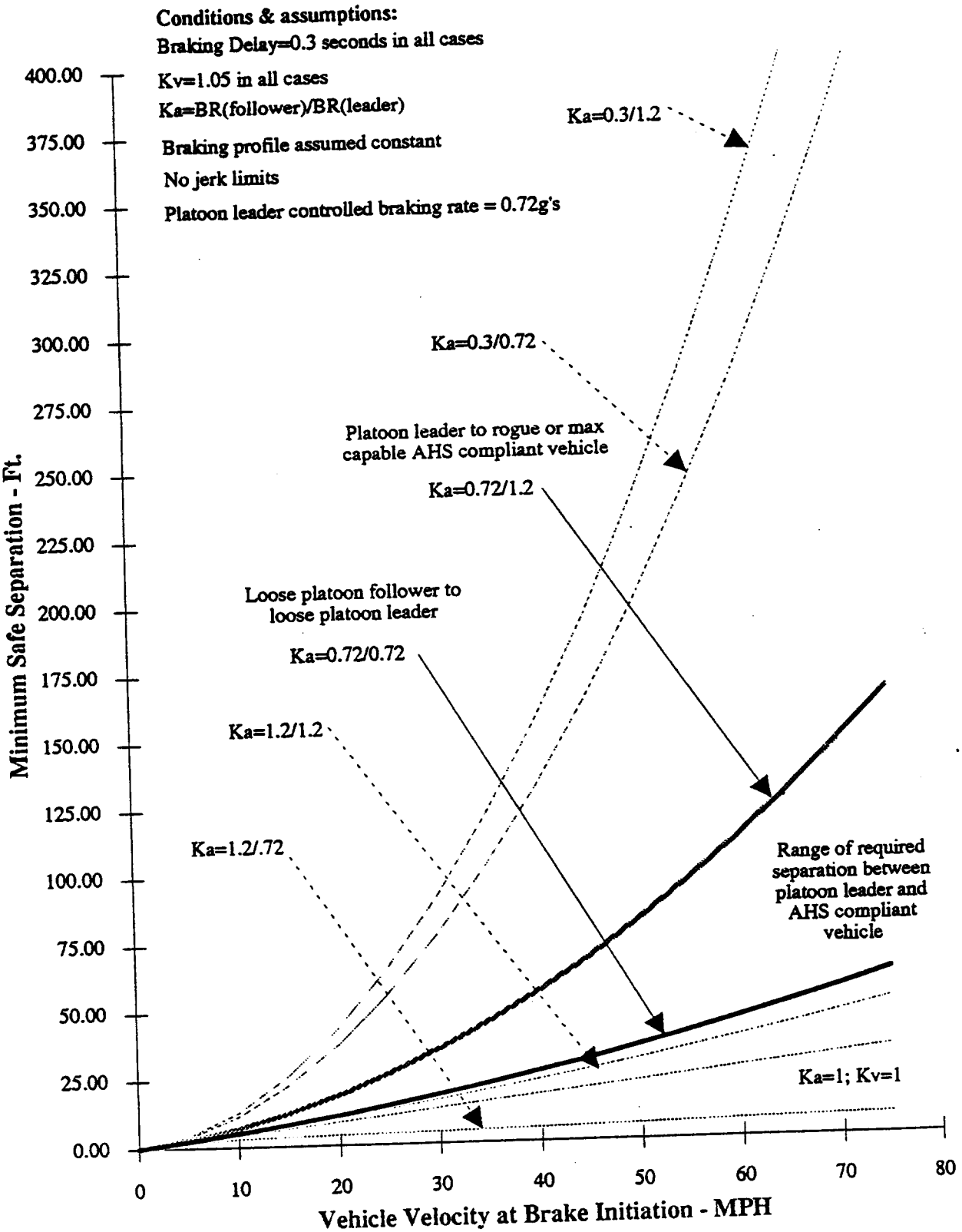


Figure 13. Curves illustrating minimum separation range requirements between loose platoon leader and forward threat agents.

As shown in figure 13, a loose platoon can operate at minimum inter-vehicle spacing of 30 to 50 feet at 60 to 70 mph. The minimum separation to a rogue vehicle is approximately 125 feet for all AHS vehicles because they are all minimum capable vehicles in the context of rouge vehicle engagement. Engagement of a platoon leader to a leading vehicle under AHS compliant rules requires separations between 50 feet and 125 feet, depending on the capability of the lead vehicle.

Tight Platoon Engagements

The tight platoon represents the limit of situation control as a separation management tool. In this engagement strategy, operating separation is established at a value in the three to five ft range. As indicated earlier, such separations can only be safe if the following vehicle is more capable than the leader. To create this opportunity, the leading vehicle braking capability must be severely suppressed. A value of 0.3 Gs is generally used for this concept of operation.

Figure 14 shows the separation implications for this engagement strategy using the same display as used in the previous sections. The bottom curve represents the minimum attainable under the assumed conditions when the leader is suppressed to 0.3 Gs and the following vehicle has a maximum capability (1.2 Gs in these analyses). To examine the requirements with other than these limit conditions, figure 15 was prepared to expand the small separation area and illustrate the influence of Ka. As this figure shows, maintaining a separation of less than five feet at 60 to 70 mph requires this maximum capable vehicle. This implies that, under the conditions of this analysis, we can only sustain a two-vehicle platoon. This minimal capability results from two of the conditions assumed:

1. A slight variation in velocity between vehicles was assumed by using Kv = 1.05. This is certainly not unlikely. Furthermore it is a fact that small velocity variation can have a significant influence on safe separation. Therefore, it will be critical to have a separation controller that allows minimal variations around the set point—velocity and separation.

2. Also, delay has a large effect on the safety of small separations. In these calculations, delay was assumed to be 0.3 seconds for each vehicle in the platoon (each vehicle receives its cue to stop from the adjacent leading vehicle).

If we can assume Kv=1.0, we allow some length to a platoon, but very quickly become restricted by the way delay is handled. This is illustrated in figure 16, which illustrates the braking requirements of vehicles at different positions in the platoon as influenced by delay and platoon leader suppressed braking rate. For all cases, Kv = 1.0. For the case where delay equals 0.3 seconds, a platoon length of seven vehicles reaches the maximum capability we may assume to exist (the minimum capable AHS vehicle). What is not explicit in this figure is the concept of vehicle slots in a tight platoon. The upper curve in this figure suggests that a platoon length of seven vehicles can be supported before we reach a maximum braking capability. In this configuration, for example, the first vehicle behind the leader will require approximately 3.3 Gs braking rate. If it happens to use a higher value,

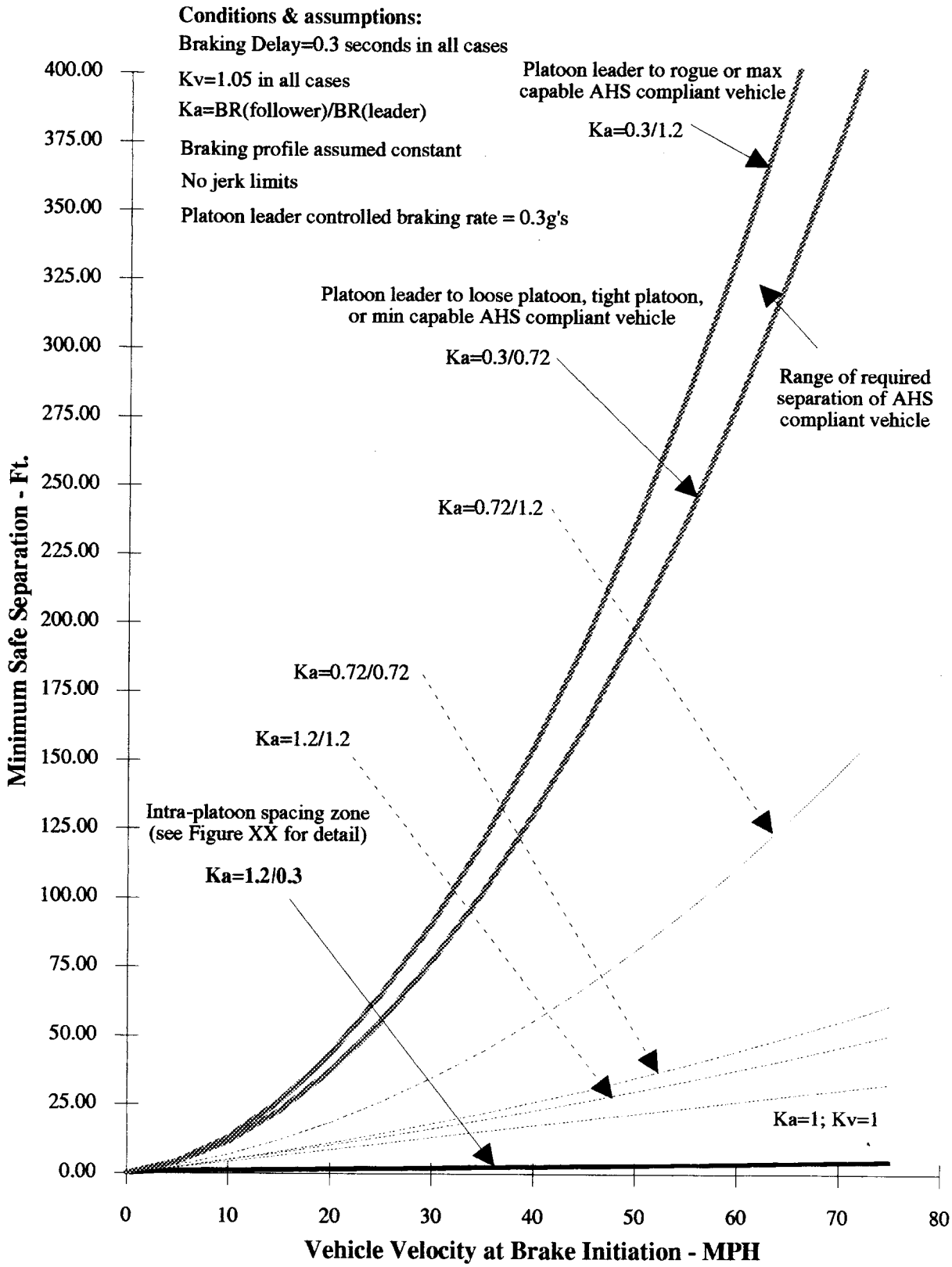


Figure 14. Curves illustrating minimum separation range requirements between tight platoon leader and forward threat agents.

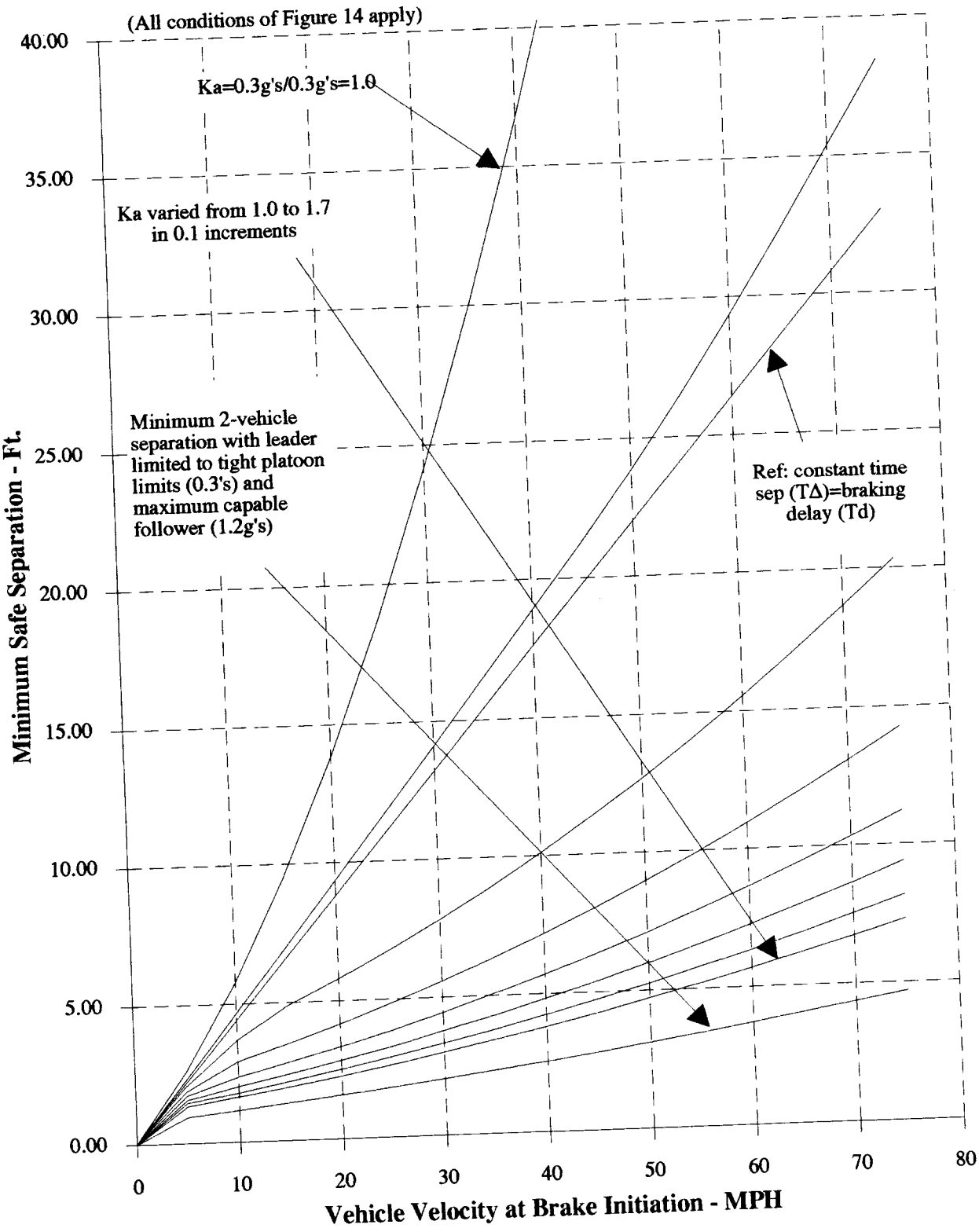


Figure 15. Small separation detail of figure 14.

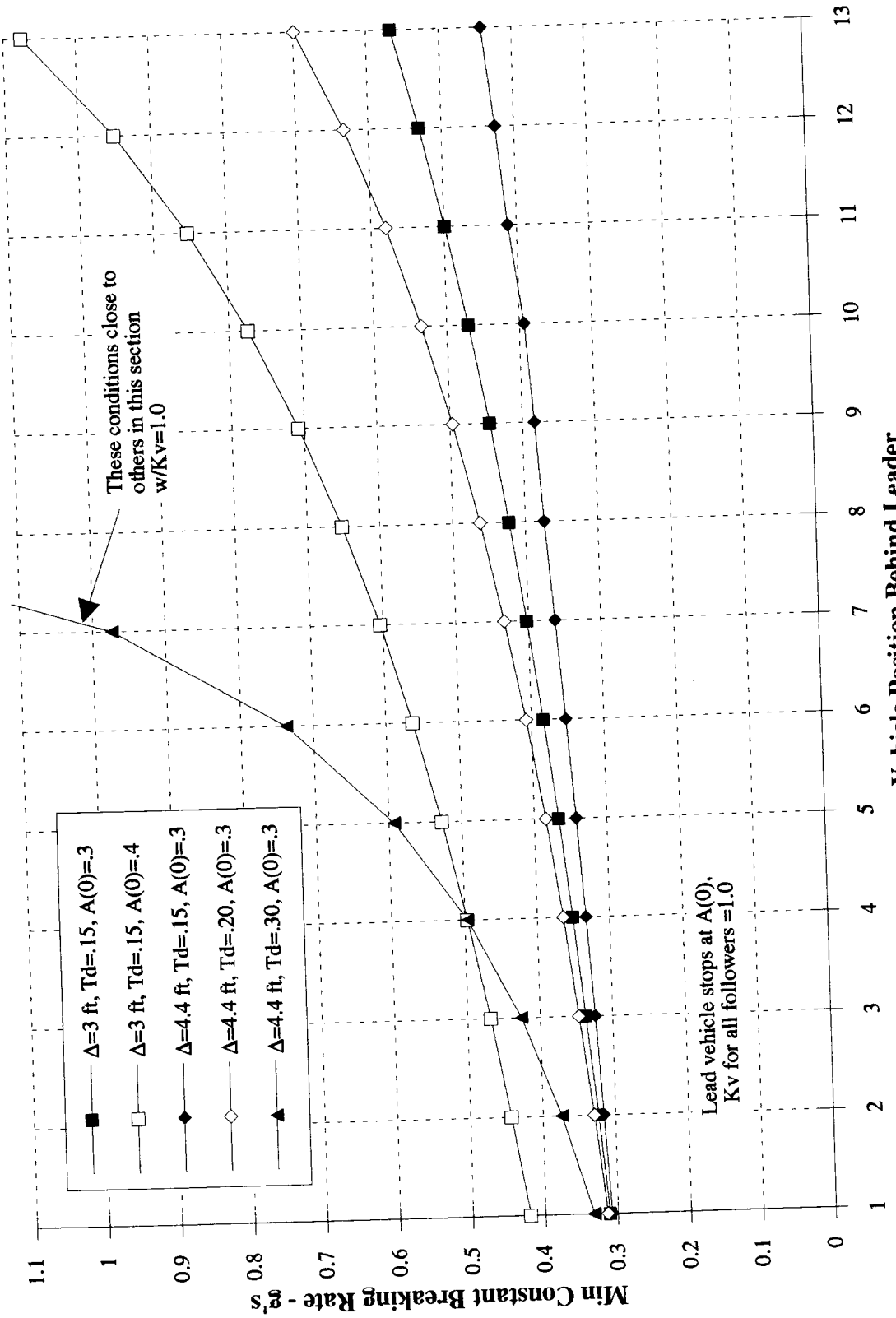


Figure 16. Braking rate requirements for following vehicles in tight platoon under various conditions.

To eliminate these deficiencies, a tight platoon must reduce the delay effects:

- Develop capabilities to greatly reduce delay.

- Develop capabilities to greatly reduce the influence of successive delays through coordinated braking (where all vehicles in the platoon take their cue from the leader) or braking from the rear of platoon in worst case situations.

Examining the potential effectiveness of options such as these is beyond the simplified models used in this analysis. Such effects can only be determined by complex and realistic simulation models. We have little doubt that tight platoons can be safely accommodated under carefully controlled conditions. The concern here lies with knowing what these conditions are, and having the ability to measure the real world with sufficient precision to determine that these conditions are present.

The above discussion has been directed to the intra-platoon separations. As with loose platoons, when a subject vehicle's performance is limited as a leader (to accommodate the capabilities of a following vehicle), the ability of that subject vehicle to act in its own right as a follower is influenced. Tight platoons are most influenced in this regard. As shown in figure 14, while intra-platoon spacing may be on the order of a few feet, the spacing requirement of the platoon (that is the platoon leader) to other forward threats is greatly increased. At velocities in the 60 to 70 mph range, separations to forward vehicles of all types are in the range of 300 to 400 feet.

Dual Control Implications

All of the preceding analyses have taken the view of forward threat engagement. The implications of these engagement scenarios is that engagement strategies are one-directional. However, every vehicle functions in a dual role as leader as well as follower. Therefore, at any given time, a specific vehicle is suspended between two engagement rules: one that controls its relationship to a leading vehicle and one that controls its relationship to a following vehicle. In some cases these rules may be the same; but they need not be and, in some cases, cannot be the same. (For example, an AHS vehicle must engage a forward rogue vehicle under rogue vehicle rules, regardless of how that AHS vehicle is engaged with following vehicles).
What may be obvious, but should be stated, is that while a single vehicle may be involved in two different relationships at the same time, it does not have the freedom to independently establish its role in these relationships. For example, if a vehicle promises to limit its braking capability to satisfy a platooning relationship with following vehicles, it cannot use a higher braking rate to establish separation requirements in a forward engagement. These capabilities must be equal. The implication is that a vehicle's separation manager must always be aware of this connection when changing or calibrating one of the engagement strategies associated with that vehicle.

Figures 17 through 19 illustrate these implications as they influence steady state separation requirements. These figures illustrate required steady state separations in before and after situations.

Figure 17 illustrates the effects of changing from an AHS compliant engagement strategy to a loose platoon. Figure 18 illustrates the effects of changing from a loose platoon to a tight platoon. Because of the severe suppression of lead vehicle capabilities required for this engagement, dramatic increases in separation requirements for forward engagements are required. Figure 19 illustrates the effects of a blanket decrease in braking capabilities, as, for example, might be experienced if it begins raining. The assumption in this figure is that all braking capabilities are reduced by 50 percent.

These figures also illustrate the implication on forward range requirements to engage a forward phantom vehicle (any object not known to be a moving vehicle). They introduce the concept of a rear phantom vehicle that serves the same purpose as the forward phantom. The phantom serves as threat condition to establish a minimum rear range requirement in the absence of any other rear threat. In these figures, we assumed the characteristic of this phantom vehicle as a rogue, traveling at a speed in excess of the legal limit (e.g., 70 mph), and possessing a braking capability less than the least capable production vehicle (e.g., 0.7 Gs).

Rear Separation Management

As illustrated in the previous section, a single vehicle is always suspended between two engagement rules; one coupling it to a leading vehicle and the other coupling it to a following vehicle (using the concept of phantom vehicles as required). In a similar fashion, a specific engagement rule is suspended between two vehicles; with each vehicle playing a separate and distinct role relative to that engagement. One vehicle is considered to be burdened and the other is considered to be privileged. These terms, borrowed from marine navigation rules-of-the-road imply certain responsibilities and rights with respect to each other:

- A privileged vehicle has the right-of-way; but in exercising this right has the responsibility to provide a consistent and predictable worst case profile against which the burdened vehicle can manage its avoidance strategy. In return, the privileged vehicle has the right to expect the burdened vehicle to keep clear.

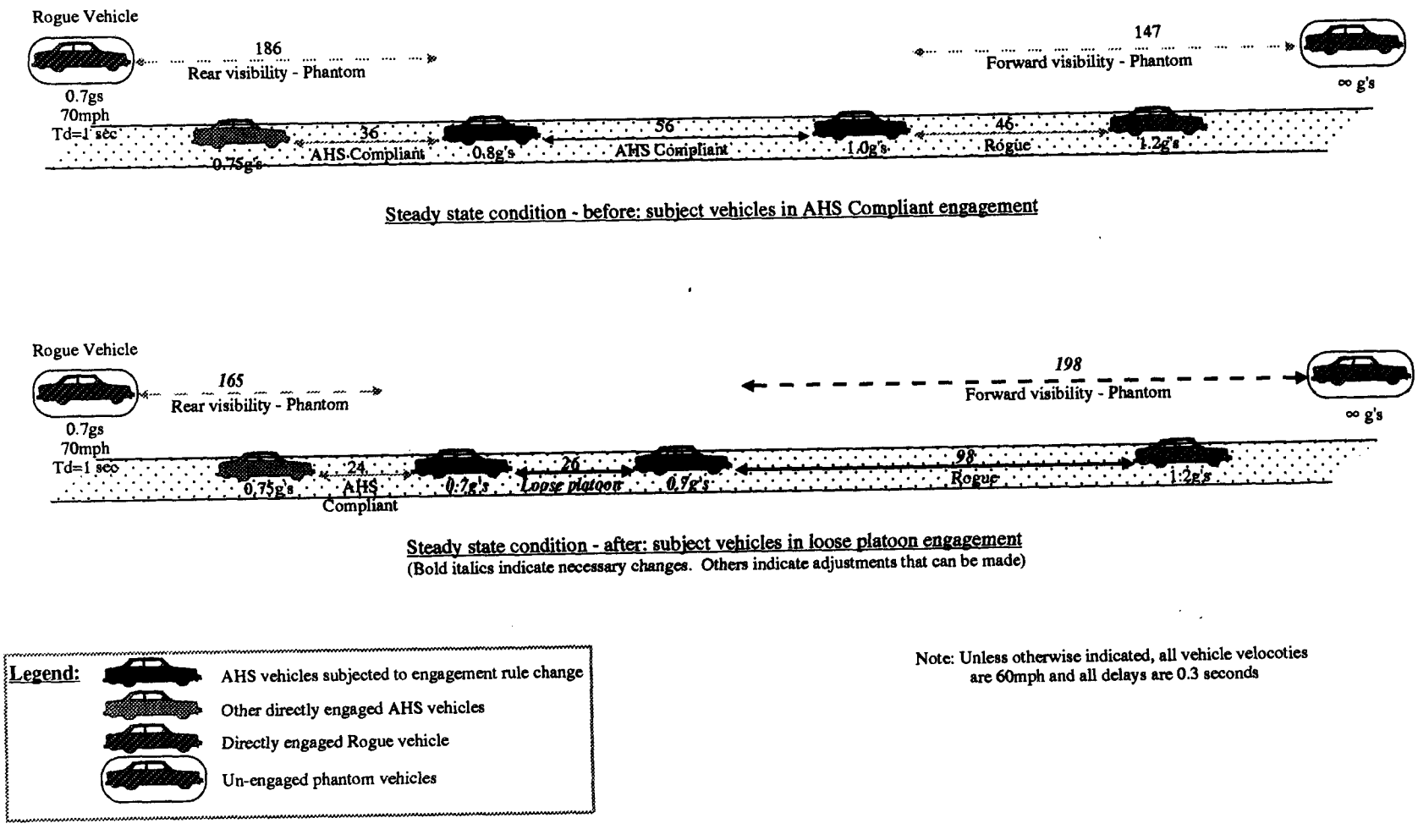


Figure 17. Example effects of changing engagement rule from AHS compliant to loose platoon.

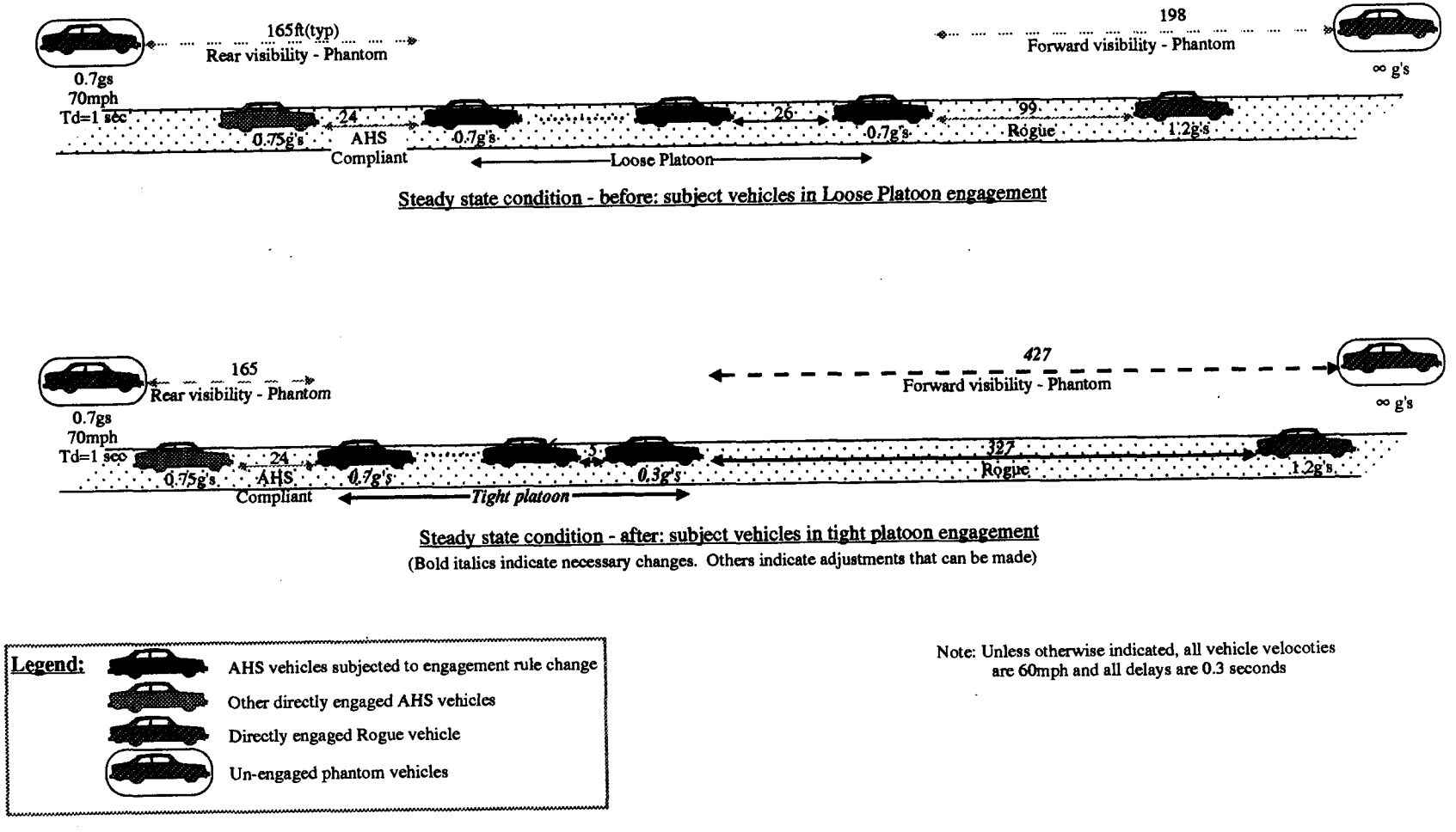


Figure 18. Example effects of changing engagement rule from loose platoon to tight platoon.

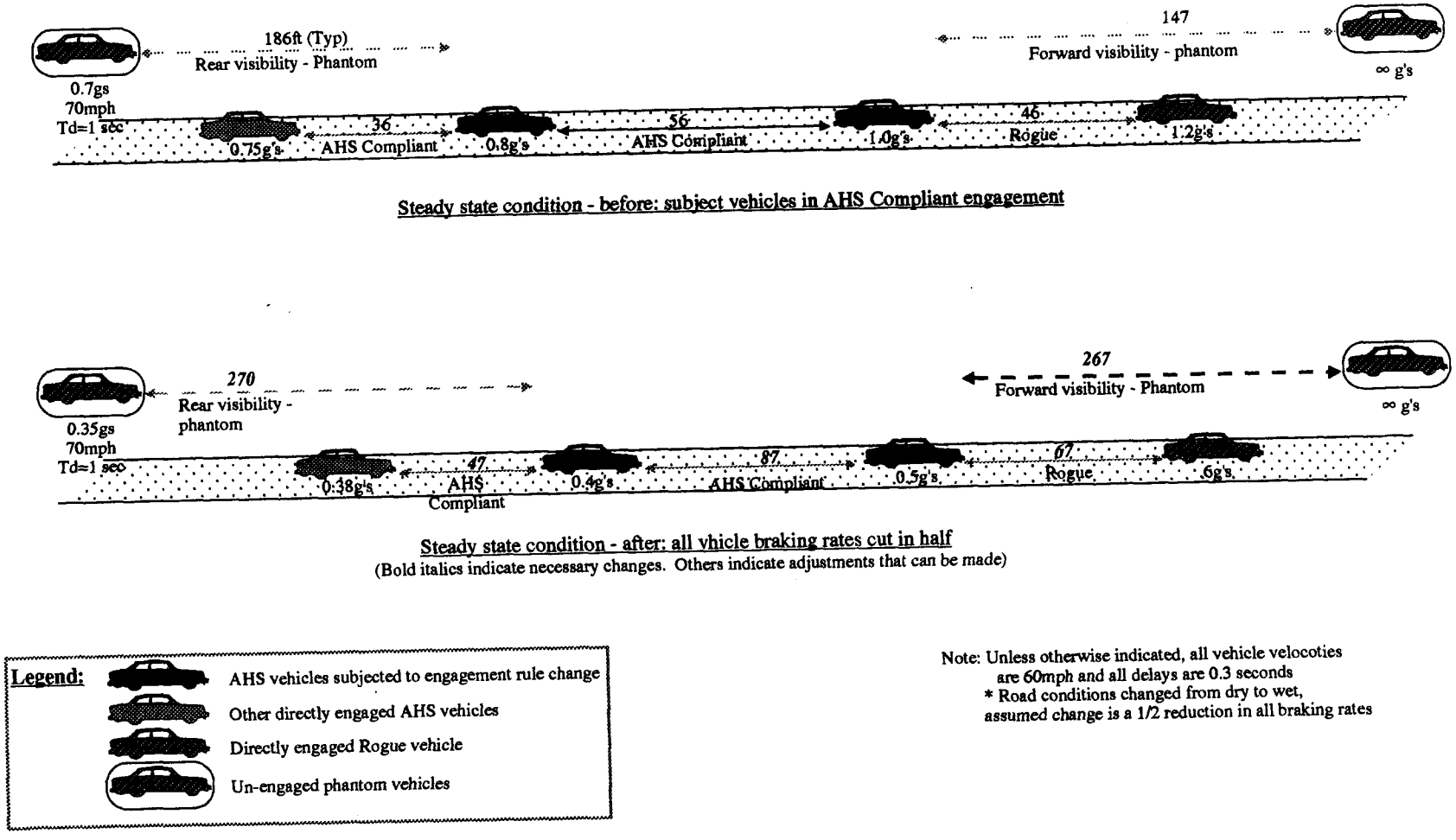


Figure 19. Example effects of changing road conditions* while under AHS compliant rule.

- A burdened vehicle has the responsibility to keep clear of the privileged vehicle. In return, it has the right to expect consistent and predictable maneuvers from the privileged vehicle.

The burden is assigned to the vehicle most capable of avoiding the collision; that is, possesses the most control-ability and has the least constraints on maneuvering options. The control-ability issue establishes the role an AHS vehicle must assume with respect to a rogue vehicle or any vehicle not known to be under AHS control: the AHS vehicle must assume the burden of collision avoidance, regardless of its location relative to the rogue vehicle.

If both vehicles are AHS vehicles, the maneuverability issue determines the roles. In general, the burden is placed on the trailing vehicle, while privilege is assigned to the leading vehicle. Note that this is not some physical law. It is rather a result of maneuvering limitations faced by the leading vehicle because of its responsibility as a burdened vehicle to its forward engagement.

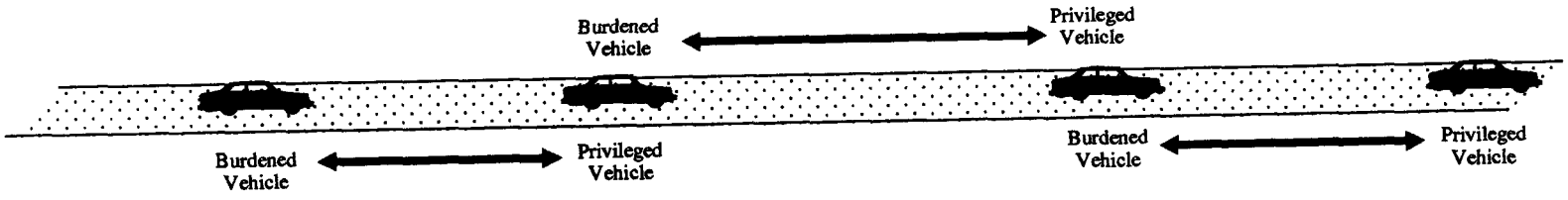
Figure 20 shows these privileged/burdened relationships. The upper display is the normal relationship between AHS controlled vehicles. As shown, each vehicle functions as a burdened vehicle to the vehicle ahead, and as a privileged vehicle to the vehicle behind. This arrangement is the best for collision avoidance and is the one assumed as normal for all AHS to AHS engagements in this report.

The lower display illustrates the AHS vehicle roles when engaged with a rogue vehicle. The vehicle leading the rogue is burdened in both the forward and rear engagement rules. This is a very difficult position. This vehicle is charged with the responsibility for collision avoidance from a rear threat, but has no direct means to control separation. Two options may be effective, but neither is totally adequate:

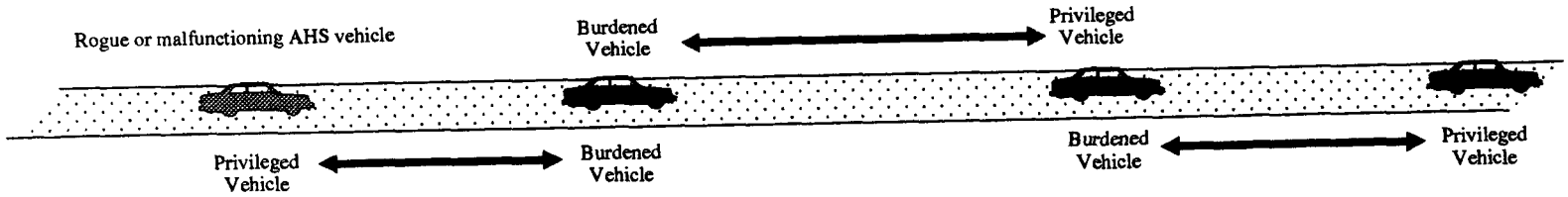
1. Communication options to influence the driver of following vehicle to adequately control separation (useful only if this vehicle is under manual control). Flashing lights, lights that vary in intensity as separation is reduced, and signs that advise of required and actual separation are representative of techniques that may be quite effective.

2. Adjustments to the AHS vehicle situation to permit it to keep ahead of the rogue in a severe maneuver. For example, the AHS vehicle could increase its separation from its leading vehicle to allow it to stop with reduced braking rates. This could be used in combination with (1) for manual vehicles, but it may be the only option for accommodating a malfunction.

Figure 21 illustrates the effects of situation alteration as a rear separation management tool. The upper display represents the steady state situation before a rogue approaches an AHS vehicle from the rear. The lower display illustrates the steady state condition after engagement. Of particular interest is the recalibration of separation required by this rear AHS vehicle to continue to successfully perform its role as a burdened vehicle to its leader.



Normal Burdened Vehicle/Privileged Vehicle relationships - all vehicles controlled by AHS



Changes in Burdened Vehicle/Privileged Vehicle relationships - one vehicle not under AHS control

Figure 20. Relationship of privileged and burdened vehicles—steady state.

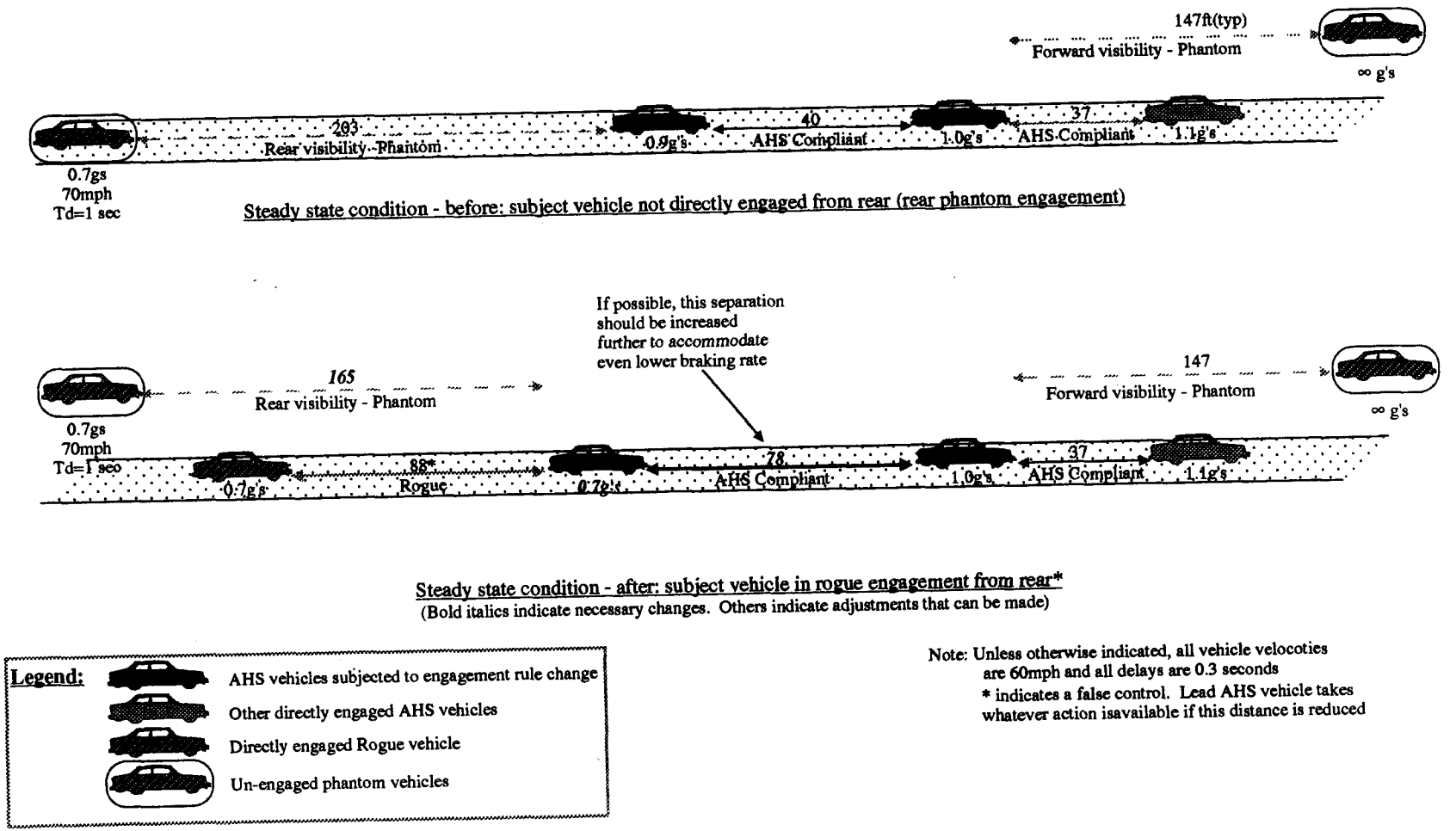


Figure 21. Example effects of engaging rogue vehicle from rear.

Steady State Separation Concerns

Trends are implied in each of the previous engagement strategies—implications on precision, level of knowledge, etc. and how these are influenced by different separation strategies. Figure 22 illustrates, in qualitative terms, how these implications relate to the various engagement strategies analyzed. In general, almost every implied requirement for safe separation increases as separation decreases: knowledge, situation awareness, and quality and precision of calibration. It is obvious that the complexity of safe separation management increases as separation decreases. Attaining these performance levels is a definite concern. However, we believe that their attainment is possible.

In addition to this general concern, five other, more specific concerns exist:

1. The adequacy of a specific rule to truly provide the necessary tolerance to a worst case maneuver (i.e., Is the perceived and predicted collision bubble outside the real collision bubble?): This concern is associated with the validity of the worst case assumptions and the validity of the control-ability assumptions. Appendix A contains a fault tree that dissects inadequate separation into detailed sub-level inadequacies. Most sources are derived from a concern that all the factors that influence real minimum separation requirements are considered. Simply stated, the concern here involves the credibility of the perceived separation requirement as a safe representation of reality.

2. The adequacy of the separation management function to know which rule to apply and to keep it properly calibrated to account for changing as-is conditions: The former requires exceptional capabilities of situation awareness in terms of the threat environment. The latter requires equally exceptional capabilities with regard to the effects of changing values for the influences of safe separation; e.g., rain, snow, or sand. These variables are identified in the fault tree referenced above. As we move toward small separations, it will be necessary to close the gap between perception and reality—including specific treatment of influencing variables as well as specific scalar relationships to enable us to improve the precision of our estimates. Without such capability, we would be forced to establish our minimum separations with such a large ignorance factor that capacity would be severely limited.

3. Uncontrolled variables: Whenever decisions are based on uncontrolled variables, such as weather, we expose ourselves to a class of threats termed “intrinsic threats.” These result from the sometimes subtle shifts in values for the influencing variables that can result in a degradation in controllability (changes in road surface, amount of rain, and temperature). Therefore, to counter these intrinsic threats, the corollary requirement of precision is the obligation to establish metrics for these variables and to monitor these metrics to permit continual recalibration of the separation so that the minimum separation remains safe under all operating conditions. This process is complicated by the fact that we must know the conditions and effects of these conditions on controllability *before we encounter them*. If a wet or snow-covered road ahead will affect braking capability, we need to adjust our separations before we get there. (Figure 19 illustrates the adjustment needed when pavement

becomes wet.) If we can't adjust an engagement prior to its need, we are at risk of collision under normal worst case maneuvers. To minimize this poten

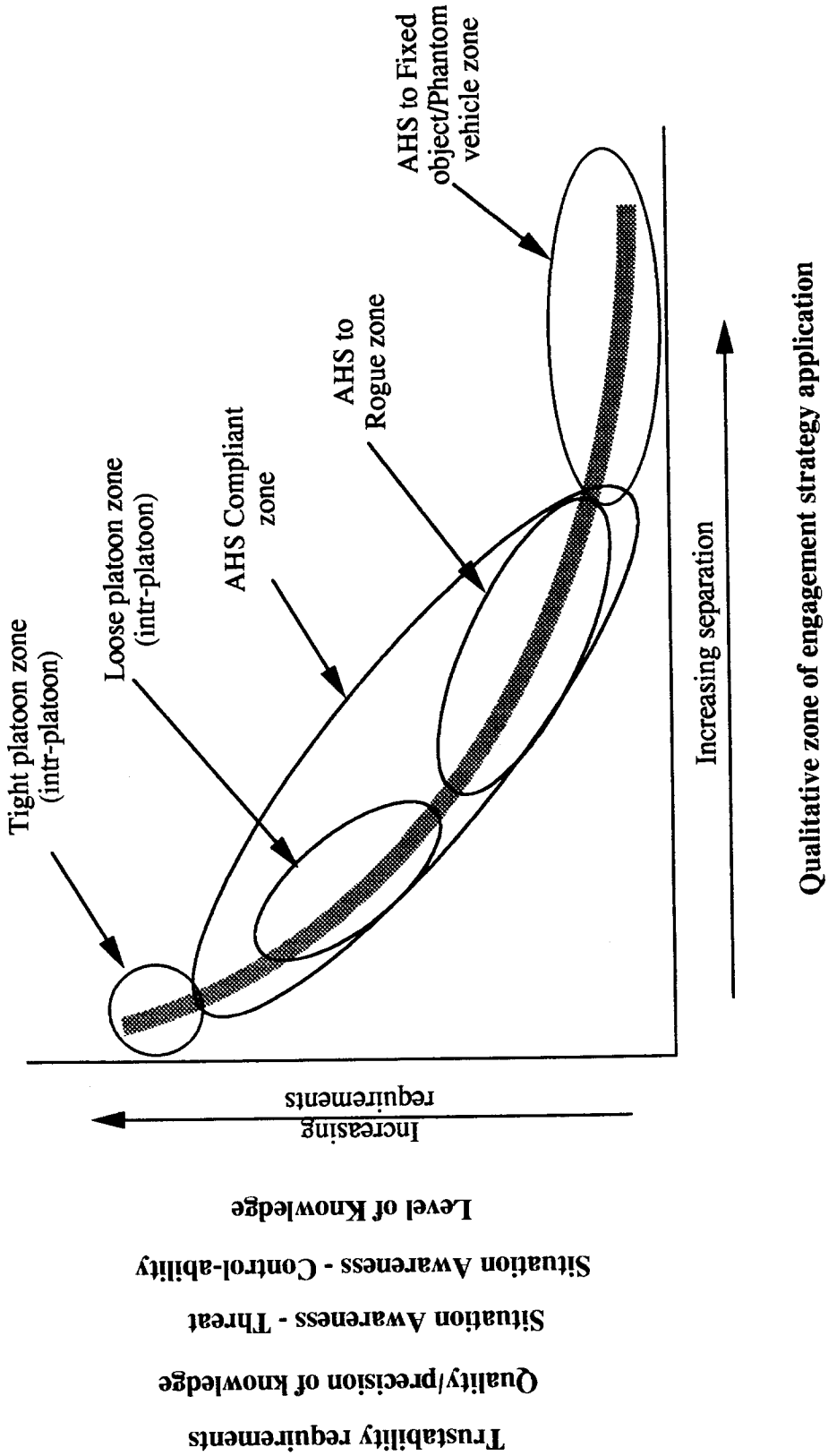


Figure 22. Qualitative relationship between selected engagement strategies and separation control complicating factors.

tial, we must seek a safer condition with urgency, perhaps employing extremis capabilities along the way, as described later under malfunction accommodation approaches.

4. Braking capability suppression: Platoon operating strategies require braking capability suppression tactics to force a population of vehicles with appropriate capabilities to support small separations. Accomplishment of this function is not trivial.

5. The capability of an AHS to operate under a variety of engagement strategies: A portfolio of rules must be available to the separation manager to safely accommodate all the situations that may exist. A general theme of many concepts is the exclusive AHS lane. While exclusive facilities are desirable, they may not be absolutely achievable. Furthermore, a number of options need to be available for engagements between AHS vehicles to accommodate transitions and relaxed engagements if the pressure for capacity is not present.

Also, it is important that situation awareness requirements not be trivialized. To achieve desired capacity improvements, vehicles must be operated in a manner that pushes the limits of their capability. To do this safely and by design, we must improve not only our qualitative and quantitative understanding of the variables that influence these limits, but also our ability to adequately measure these variables, in real time, to determine these limits. Situation awareness, in all its facets, will present a very significant challenge to an AHS.

Normal Transition Implications

All engagement strategies discussed previously were based on steady state conditions. While not intending to diminish the difficulties associated with establishing and maintaining these steady state aspects of separation management, transition situations are more difficult. Steady state considerations assumed a reasonably faithful controller to ensure that relative vehicle motion remains reasonably close to a prescribed value established by the separation manager. The influence of slight deviations was estimated through the use of a small velocity differential (Kv) assumed to exist at exactly the desired separation (characteristic of sine wave representation of the separation value around the desired value). During transition maneuvers, however, large variations in relative vehicle motions cannot be denied. As was illustrated in figures 17 through 19, significantly different separation requirements exist between different steady state engagement strategies. At a minimum, these must be accommodated. Additionally, the transition maneuvers involved in a merging situation can result in large variations in relative vehicle trajectories. This section examines some of these transition maneuvers to identify the implications of the relationship between the relative motions of the involved vehicles and the minimum safe separations that are required to accompany these motions.

Three transition situations are discussed:

1. A merging situation as it may occur at a point of entry to an AHS lane. The issue examined is the gap requirement to permit a safe maneuver. The relationships established are also

applicable to merging situations from parallel AHS lanes on a multiple lane system. Many curves are presented to illustrate the influence of selected variables on gap requirements.

2. In-line transitions, that is transitions between engagement states, without the complicating factor of another vehicle disturbing the process. Two conditions are discussed. The first addresses the situation where a high velocity vehicle approaches a slower vehicle and the issue is where to begin the slowdown maneuver to achieve a desired end position. The second, not totally different, looks at the safe separation implications of changing from a loose platoon engagement to a tight platoon engagement.

3. Exit transitions, where the concern relates primarily to the transition from operations on the automated lane to the manual world that must be accommodated in this transition. This transition was analyzed in qualitative terms only.

In all quantitative analyses, values for the common variables are the same used in previous analyses; e.g., 0.3 second delay, constant braking rates, and dry road. The separation criterion in all analyses is that no collision will occur if the leading vehicle executes its worst case maneuver at any point during the transition.

Merge Transitions

The primary variable to be controlled in a merge situation is the creation of a gap sufficiently large to accommodate the incursion of a merging vehicle while maintaining adequate separation, both forward and behind, according to the rules engaging the merging vehicle with its newly acquired partners. Figure 23 illustrates this merge situation in terms of the privileged and burdened vehicle roles used previously. If there happened to be a large gap available, such that the merging vehicle did not interfere with line vehicles, the problem disappears. However, this would be a very unusual and fortuitous circumstance. More likely, as reflected in figure 23, is that a merging vehicle will disturb an existing steady state engagement already running at minimum separation. This figure illustrates the roles each vehicle must play and the changes in role that occur during the transition.

In the analyses that follow, a very small portion of the merging situations is examined—specifically the considerations that influence the determination of the separation requirements between the merging vehicle and the designated follower in an entry/merge situation. The complications illustrated in these limited analyses lead to the conclusion that the most problematic aspect of automation for an AHS may well be entry/merge management. While lane change merges (between two AHS lanes) exhibit the same characteristics, they are much more likely to be done under matched conditions, resulting in minimal complications compared to entry transitions.

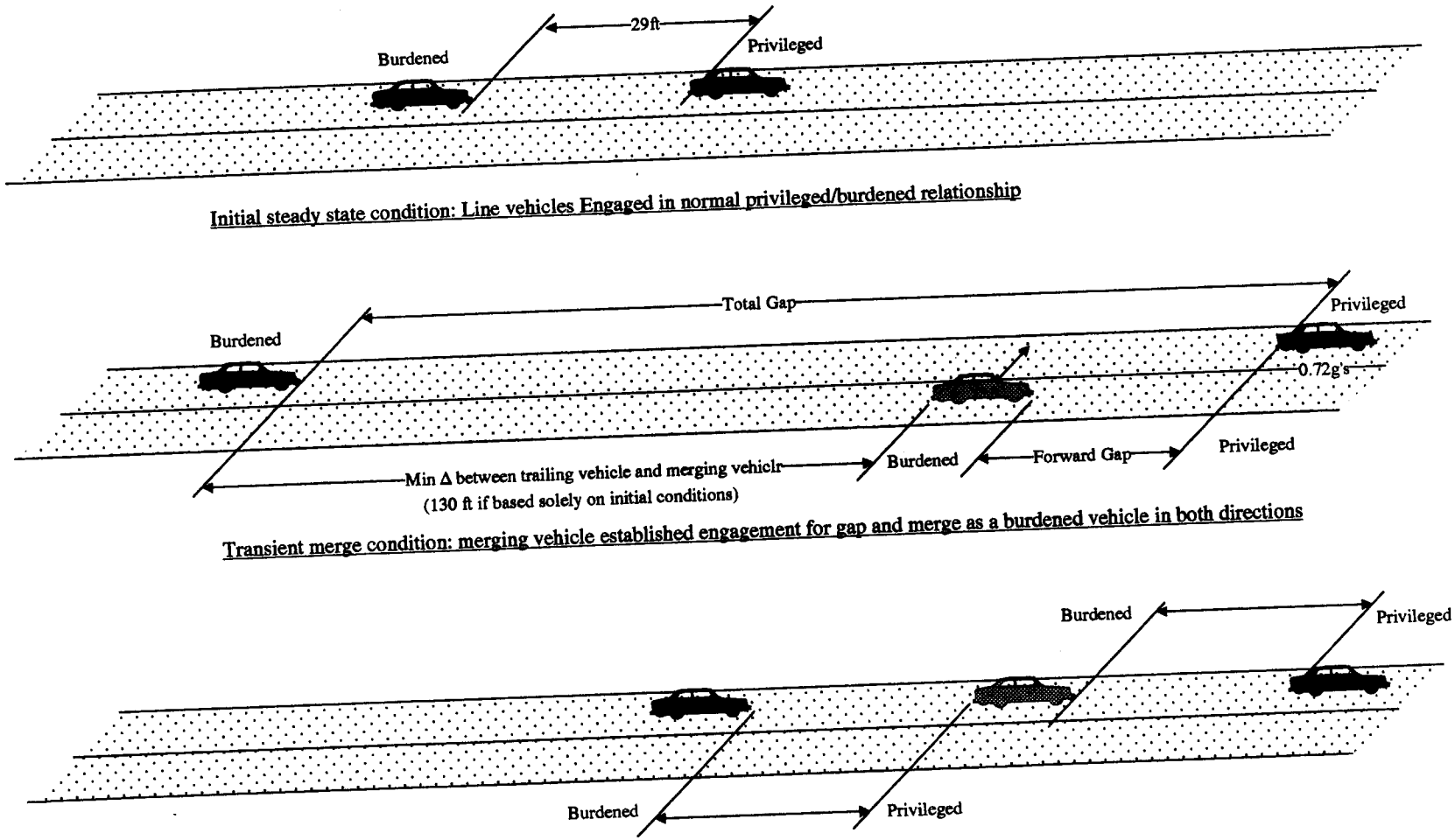


Figure 23. Changes in vehicle roles during merge.

General analysis procedure: The technique used to analyze separation requirements during merge transitions (and all transitions discussed later) involved the following steps:

1. The determination of the closure between the vehicles under some desired closing algorithm. The algorithm chosen for merge situations assumed a desired condition that the designated following vehicle would not be disturbed—that is enter the engagement at full line speed and maintain it during the maneuver. The motion algorithm for the merging vehicle was that it would enter at a specified velocity and accelerate to line speed at 0.15 Gs (typical of production vehicles in the 45 to 60 mph range)

2. At each point along the closing path (at 0.05-second intervals), the stopping distance of each vehicle was determined.

3. By combining the differences in stopping distance with the closure trajectory, a stopping point trajectory was determined for each vehicle (actually the locus of stopping positions from each point along the maneuver).

4. Minimum separation was based on non-interference between the stopping point trajectories.

In simpler terms, we attached a variable-length probe to the front of the following vehicle and another leading forward from the rear of the merging vehicle. The lengths of these probes represent the stopping distance of each vehicle as determined at each point along the way. A no-collision criterion required that there be no conflict between the trajectories defined by the forward ends of these probes.

Figure 24 illustrates the results of this process and is used here to define terms and explain all further charts for transition analyses. The curves depicted in this figure represent one of the merge analyses conducted—specifically a base case around which the effects of changes in selected variables could be examined.

In this figure, the dark curve labeled (1) illustrates the closure trajectory between the vehicles under the above closure rule with a merge velocity of 45 mph, accelerating to 65 mph at 0.15 Gs. The end point of this curve (89.07 feet) is the minimum separation required at the beginning of the maneuver if no other factors were involved. The line vehicle would just touch the merging vehicle at the instant it reached line speed. The dark curve labeled (2) is the difference between stopping distances of each vehicle at all points along the way. The initial value (130.66 feet) is the separation required to withstand the situation where the merging vehicle executes its worst case maneuver immediately upon entry to the AHS lane. The end value (28.6 feet) is the separation required for final steady state conditions using AHS compliant rules.

The upper shaded curve is simply the sum of these dark curves and represents the difference in stopping point trajectories as it varies during the maneuver. As shown, this curve has a maximum value of 151.47 feet at approximately three seconds into the maneuver. If we want to be safe against

a worst case exposure during the maneuver, the separation at the start of the maneuver must be this maximum value—151.47 feet. Therefore, the minimum gap between the designated follower and the merging vehicle before the merge is authorized must be 151.47 feet.

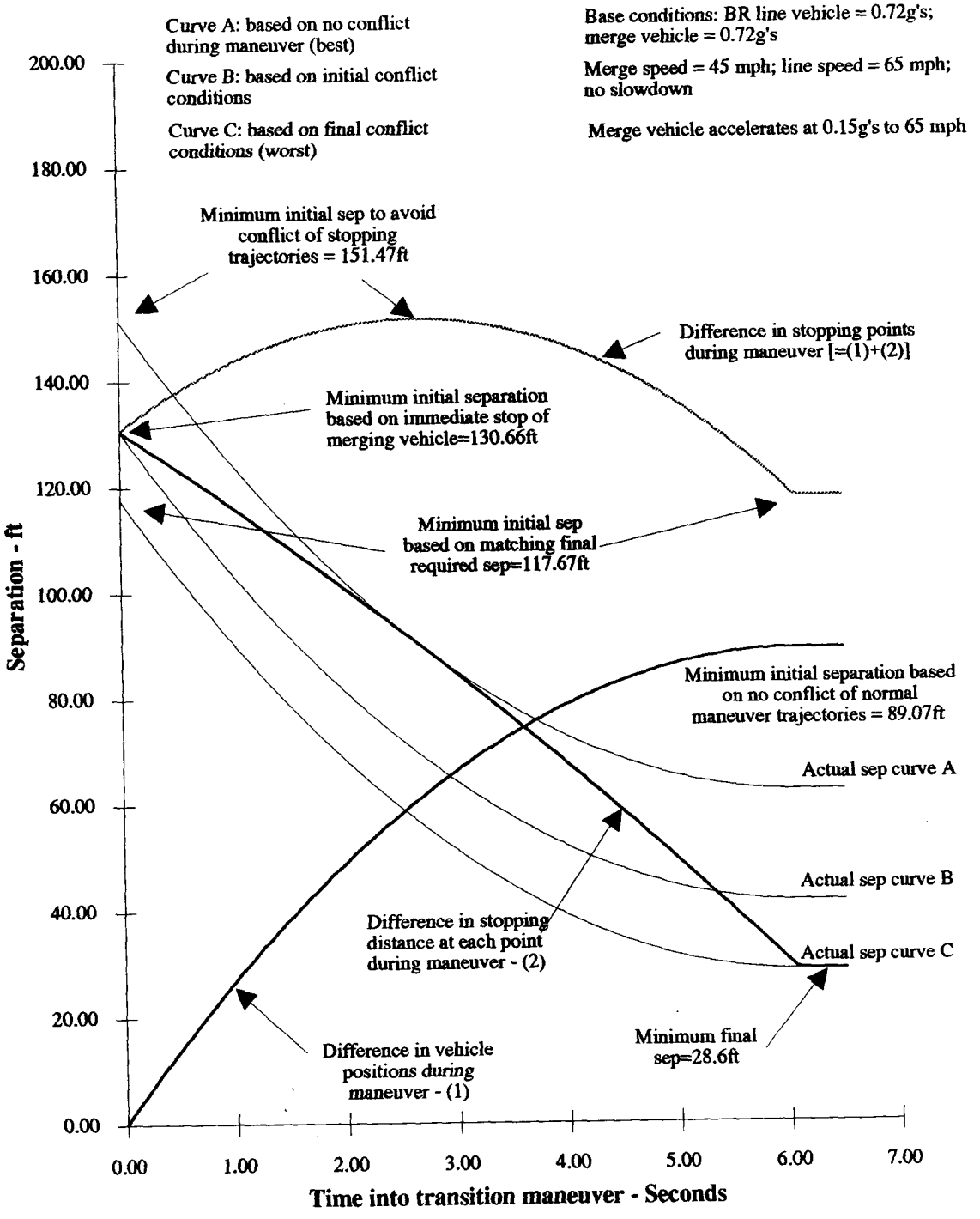


Figure 24. Curves illustrating initial merge separation dependence stopping trajectory interference during merging maneuver.

This safe case is illustrated in the curve labeled “actual sep curve A.” This curve is the negative of the closure curve (curve 1) translated by the initial value. The other separation curves illustrate the effects of different criteria for establishing the initial separation. Curve B results from establishing the initial gap on the basis of an immediate stop when the merging vehicle enters the line. Curve C results from establishing the initial gap on the basis of reaching a desired ending condition under the closure algorithm. As can be seen, both approaches are everywhere below curve (2) and, therefore, would not be adequate to avoid a collision at any time during the maneuver, should a worst case develop.

Dealing with initial separations that are based on situations yet to be established is problematical. This is reflected in these analyses—we basically used the dynamics of the maneuver to determine what the initial separation *should have been*. Obviously, this is unacceptable, but to circumvent this problem we must seek closing algorithms that shape the stopping point difference curve (the upper shaded curve in figure 24) such that its maximum value occurs at T=0. Therefore, the initial gap requirement can be based on the worst case occurring at T=0—using values that exist at that time. The initial urge is to simply establish a closing algorithm that more closely follows curve (2) in figure 24. However, this curve is itself a function of the closing algorithm. Therefore, choosing an appropriate closing algorithm is neither arbitrary nor trivial.

Influence of relative braking capability on merge gap requirements: Figure 25 shows a number of curves for various ratios of Ka. Each of these curves represents the minimum required separation between a line vehicle (represented by the numerator of the Ka ratio) and a merging vehicle (represented by the denominator of the Ka ratio) as determined for the same merge algorithm used in figure 24: the merging vehicle enters the automated lane at 45 mph and accelerates to line speed of 65 mph at 0.15 G's. The designated following vehicle maintains a constant line speed. These curves relate to the dark curve labeled (2) in figure 24. The legend for converting the Ka ratios to vehicle counterparts is shown in the upper left of figure 25. For example, the top curve, labeled “Ka= 0.3 Gs/1.2 Gs” translates to a leader of a tight platoon as the designated follower of a merging maximum capable AHS vehicle or a rogue.

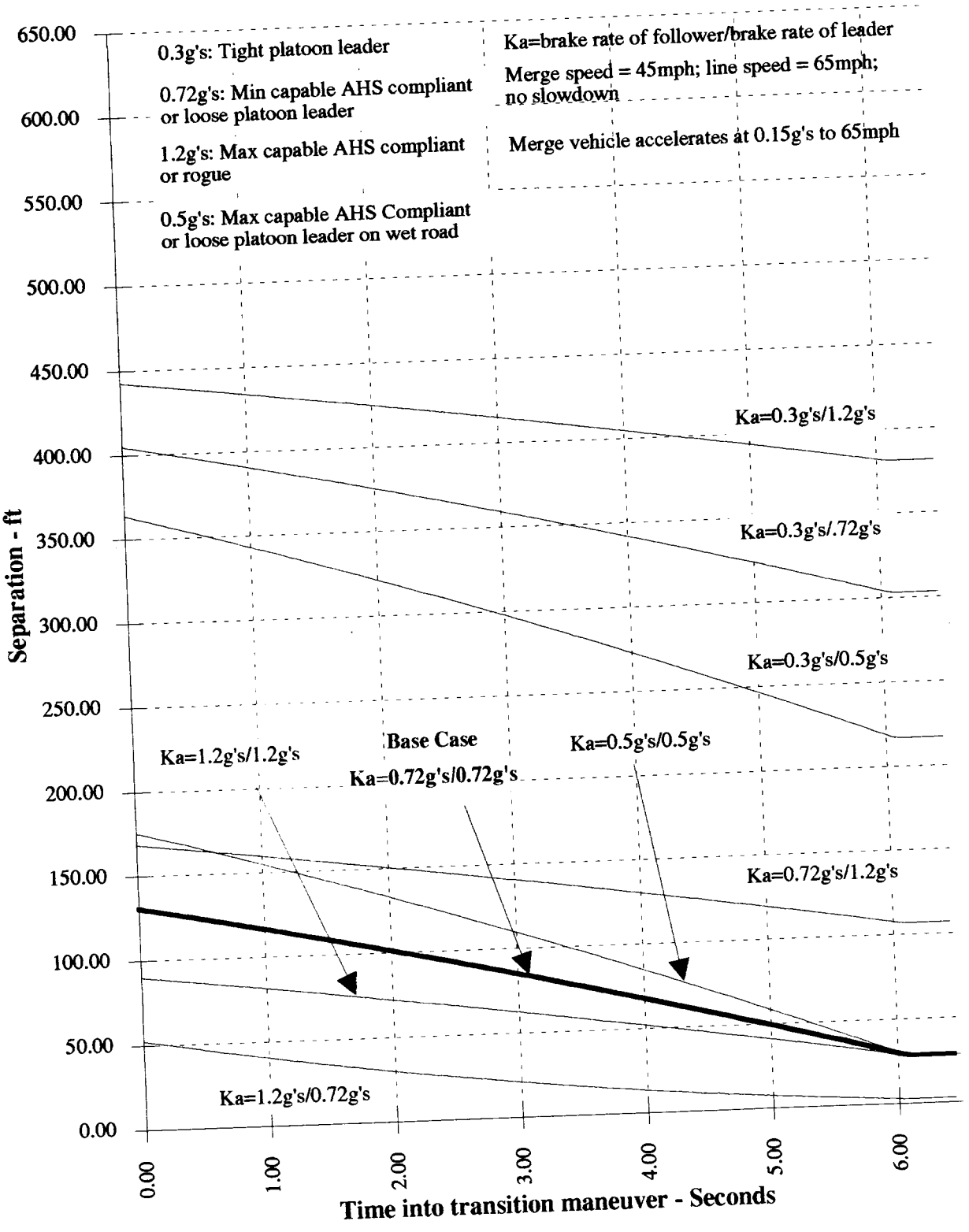


Figure 25. Stopping distance differences during merge maneuver for various values of Ka.

Figure 26 shows the difference in stopping points during the merge as determined by adding the curves from figure 25 to the overtaking differential displayed on figure 26. (These curves correspond to the upper shaded curve in figure 24.) The maximum values of these curves indicate the minimum initial gap required between the line vehicle and the merging vehicle if they are to have the capability of tolerating a worst case condition at any and all points during the specified desired maneuver. Two observations are made regarding these curves:

Figure 26. Stopping point differences during merge maneuver for various values of Ka.

1. The minimum gap increases as the stopping distance of the line vehicle increases and as Ka increases. This is not enlightening; the same conclusion would be drawn by simply analyzing steady state separation requirements.

2. Of more significance is the observation that, in all cases, the minimum gap requirements are greater than estimated solely on the basis of an initial worst case exposure. In some cases these differences are significant. So many variables are depicted in this figure that we hesitate to draw any significant conclusion except to reinforce the conviction that establishing the initial gap for merging is a very complex task, if we are to guarantee tolerance to a worst case situation that may develop at any point during the maneuver.

In the next section, we will illustrate the influence of merge velocity, braking delay, and merging vehicle acceleration rate on the magnitude of the differential stopping point trajectories and, therefore, on the minimum initial gap requirements. Before these analyses, however, two additional displays are presented. Figures 27 and 28 illustrate the required gaps that must be created under two conditions: figure 27 addresses the situation where the designated following vehicle is the leader of a loose platoon or is a minimum capable AHS vehicle. In either case, its maximum braking rate is 0.72 Gs and remains constant throughout the maneuver. Figure 28 addresses the situation where the designated following vehicle is the leader if a tight platoon, with a suppressed maximum braking rate of 0.3 Gs. In both situations, the merging vehicle has the same braking rate: 0.72 Gs. In addition to the rear gap formation requirements, these figures illustrate the total gap required, including the required forward separation and the length of the merging vehicle.

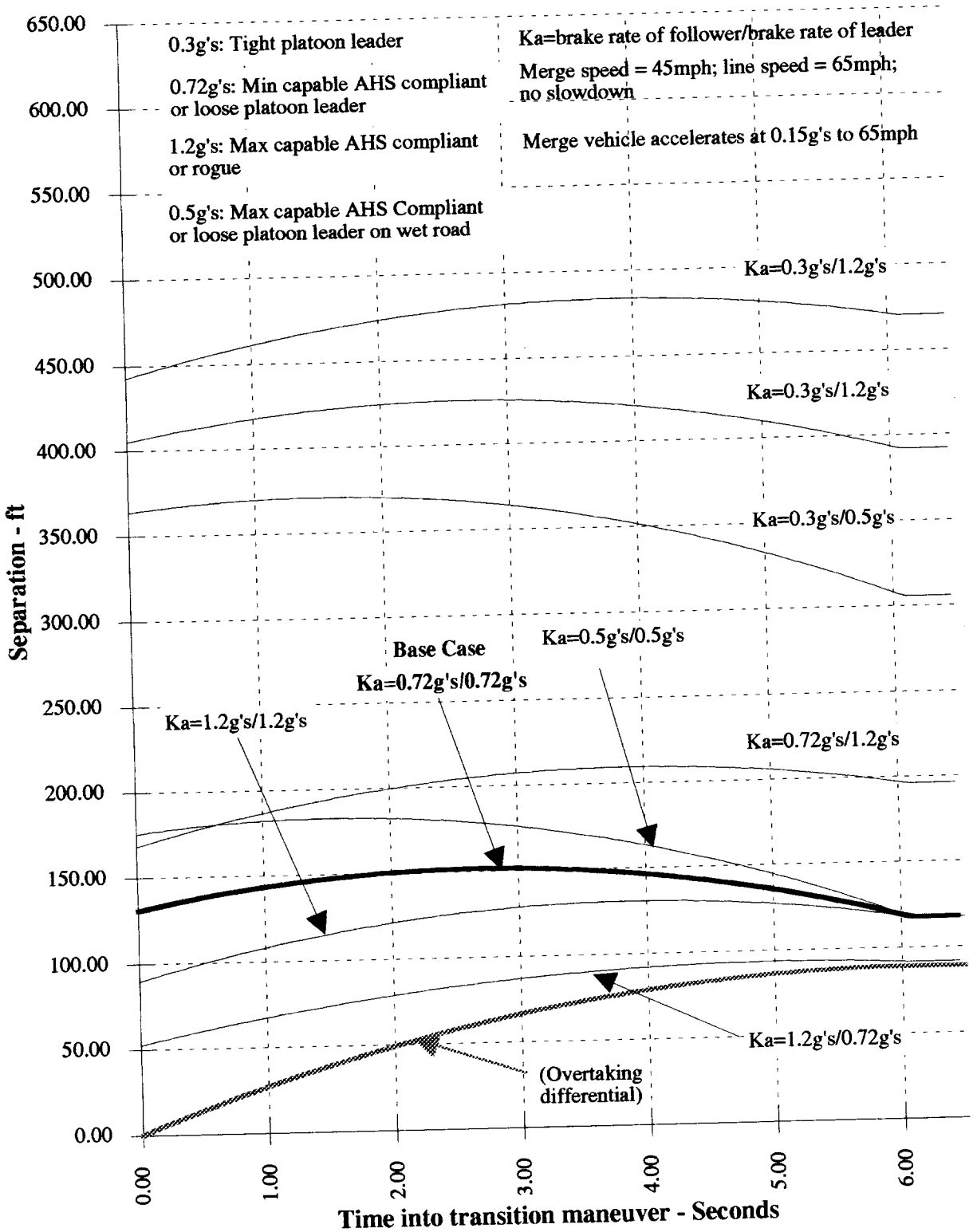


Figure 26. Stopping point differences during merge maneuver for various values of Ka.

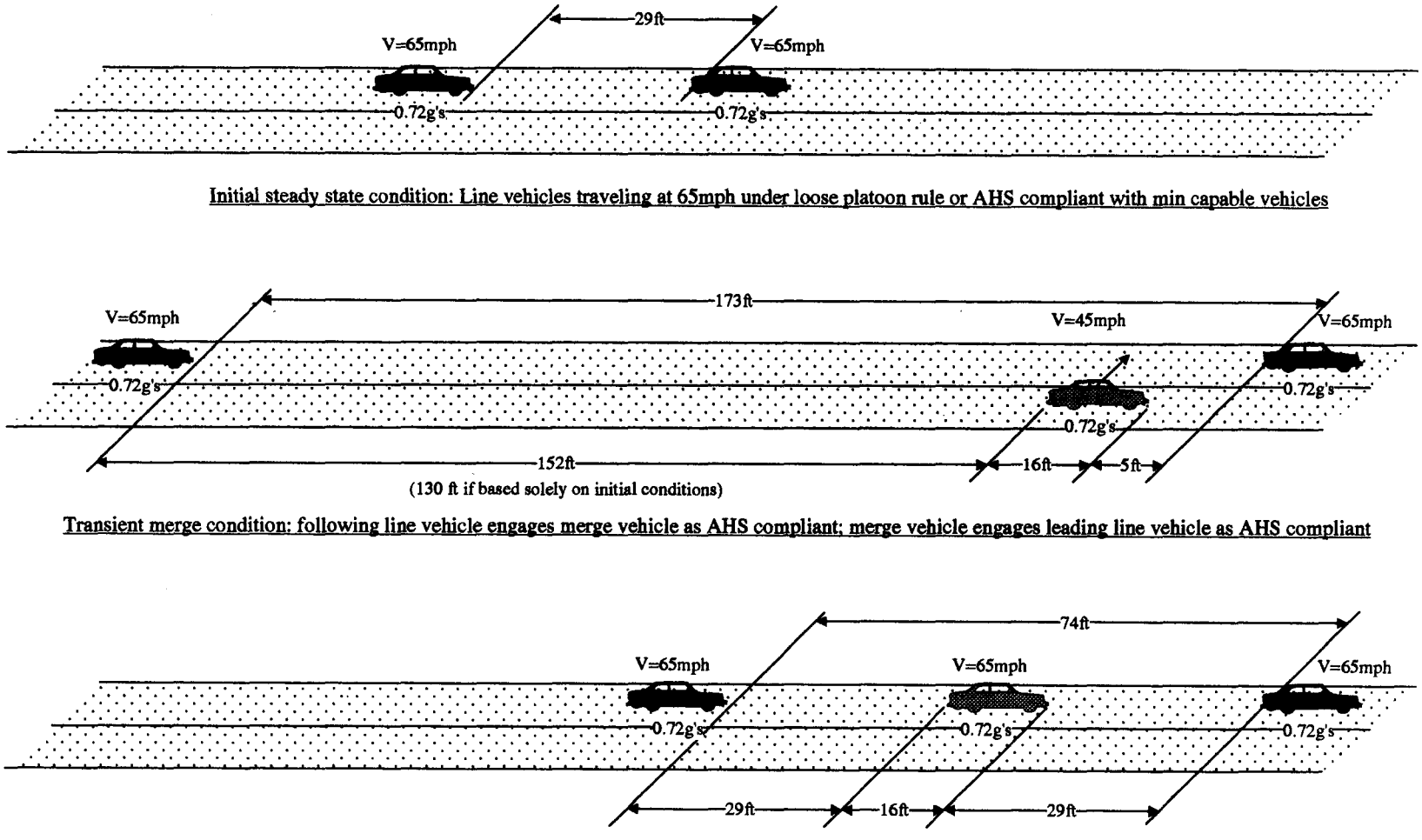
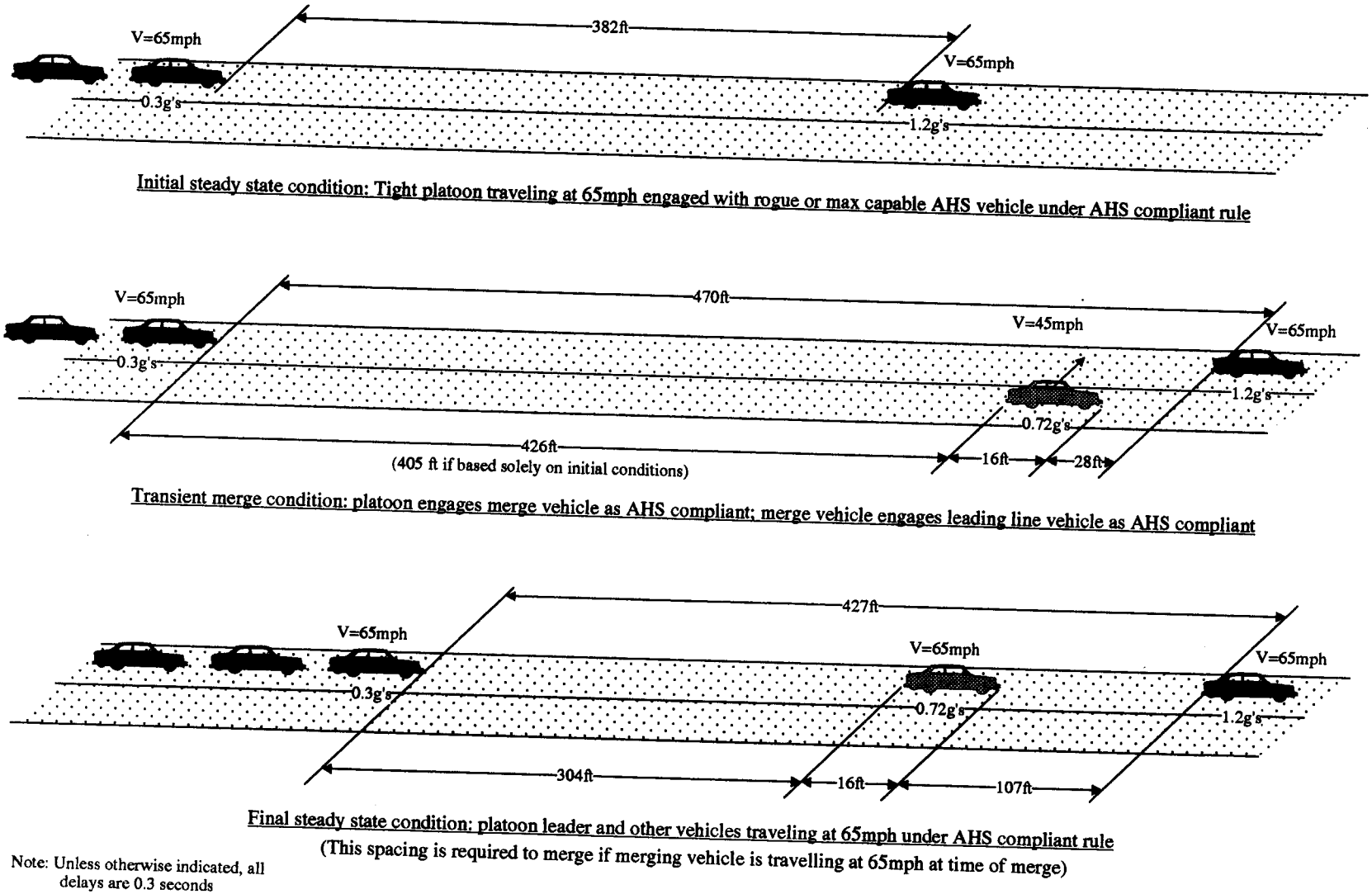


Figure 27. Example merge situation with loose platoon or maximum capable AHS vehicle.



Note: Unless otherwise indicated, all delays are 0.3 seconds

Figure 28. Example merge situation with tight platoon and rogue or maximum capable AHS vehicle.

As shown, the required initial forward separation is a small part of the gap formation problem. While only a few cases from this total gap perspective were analyzed, two observations emerged:

1. With a slow speed merge, initial required forward gap is very small, even for large braking rate differentials.

2. In no case that we analyzed was a forward gap greater than that required under the initial merge conditions.

Therefore, it would seem that the forward separation portion of the gap is at least relatively predictable on the basis of conditions that exist at the time of the merge.

Of interest in these figures is the relatively large gap to accommodate the transient merge conditions as compared to the final steady state separation conditions. This is primarily the result of the speed differential between the merging vehicle and the line vehicles. If the merge could be coordinated such that it could occur at line speed, the gap requirements would be identical to the final steady state separations. This strongly suggests an emphasis in facility design to facilitate the ability to reach the pseudo steady-state conditions while the merging vehicle is traveling a parallel entry lane. When these conditions are reached, the vehicle could slip into the line stream with no interruption.

Gap sensitivity to selected variables: In this section, the influence of three variables are illustrated:

1. Merge speed.

2. Braking response delay.

3. Merge vehicle acceleration to line speed.

The base case depicted in figure 24 is used as the reference value. Two figures are presented for each analysis:

1. A display of the influence of the variable on the relative stopping distances of the vehicles (corresponding to the dark curve labeled [2] in figure 24).

2. A display of the difference in stopping point trajectories of the two vehicles (corresponding to the upper shaded curve in figure 24).

Figures 29 and 30 show the influence of merge velocity on the gap requirements between the designated follower vehicle and the merging vehicle. For the cases shown, it is evident from figure 29 that, as the merge velocity approaches the line speed, the more accurate the estimate of gap requirements on the basis of initial conditions. (This was also indicated previously in figures 27

and 28.) It can also be observed that the merge velocity need not necessarily equal the line speed to reach this situation. For the merge algorithm selected, a merge velocity of 55 mph, compared to a line speed of 65 mph, achieves the same results.

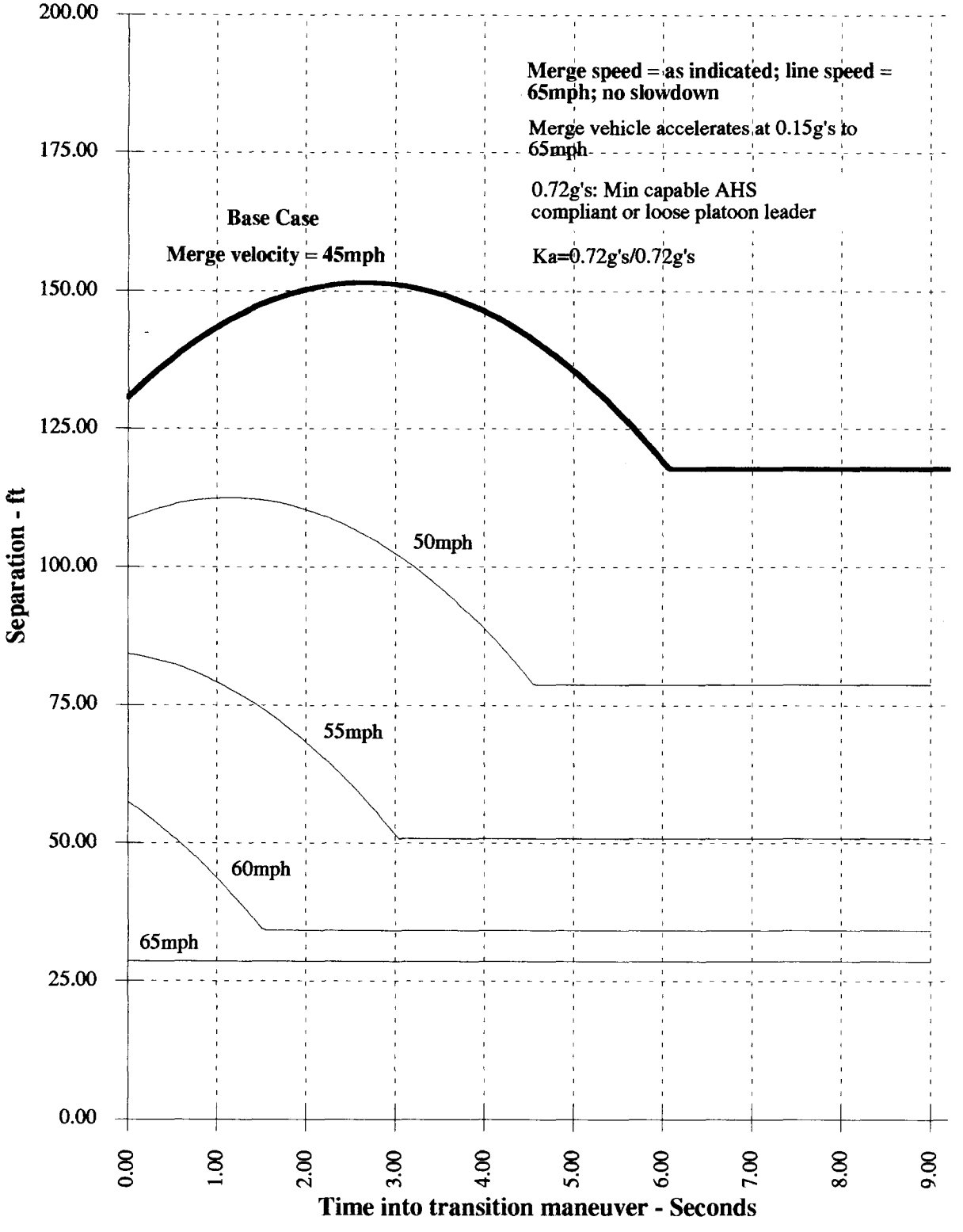


Figure 29. Stopping point differences during merge maneuver for various values of merge vehicle velocity.

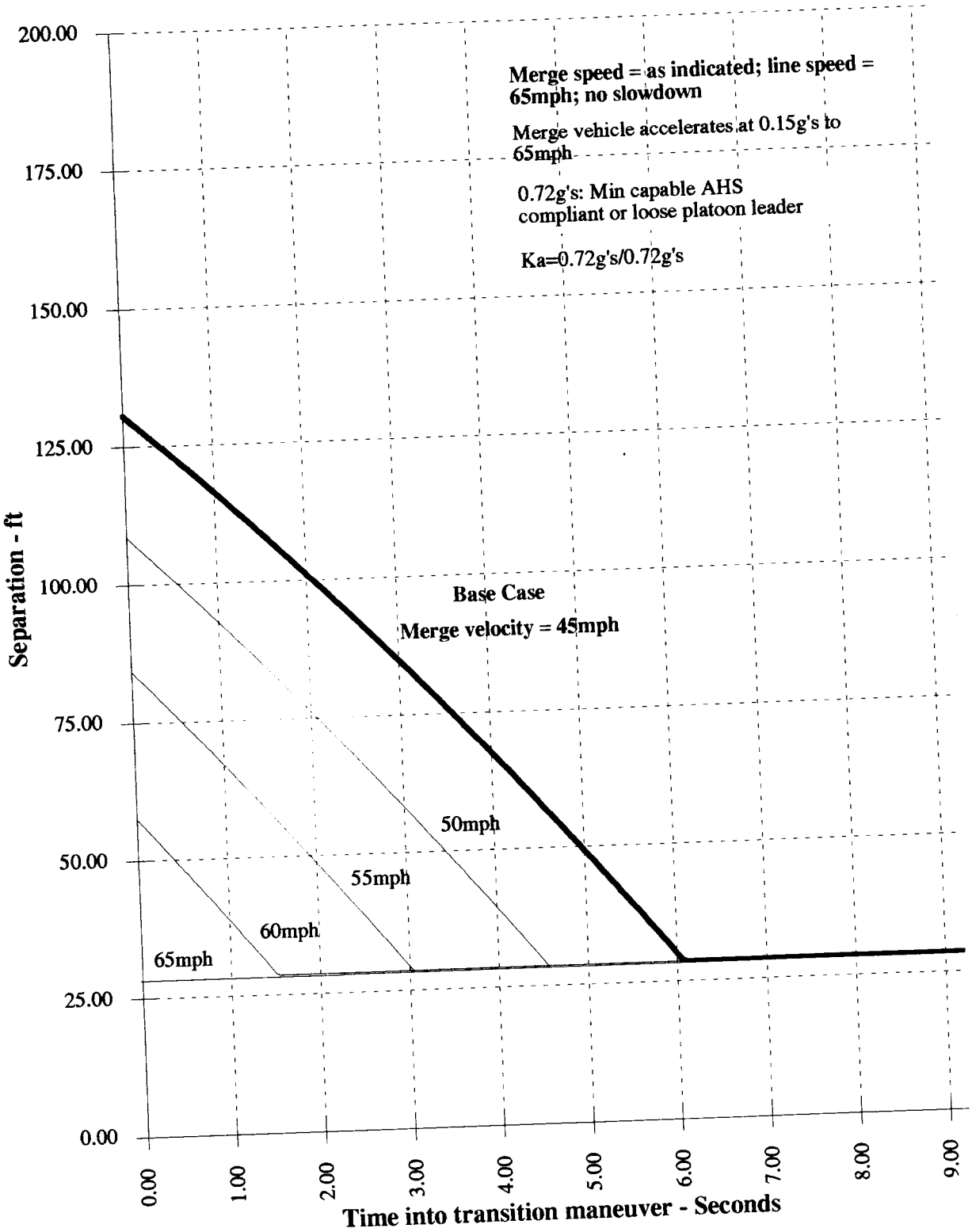


Figure 30. Stopping distance differences during merge maneuver for various values of merge vehicle velocity.

Figures 31 and 32 show the influence of the acceleration of the merging vehicle to achieve line speed. As shown in figure 31, increases in merge vehicle acceleration influence minimum gap in a manner very similar to reductions in the velocity differential between the merging vehicle and the line vehicles.

The influence of the last variable analyzed is shown in figures 33 and 34. As can be seen from figure 33, changes in delay affects only the stopping distance differential and is not effective in altering the shape of differential stopping point curve. The reason is that delay alters neither the overtaking trajectory not the shape of the stopping distance differential curve. It does, however, have a direct effect on the magnitude of the stopping distance differential and, therefore, directly affects the magnitude of the required gap. It is not a tool, however, for promoting the ability to estimate gap requirements on the basis of initial merge conditions.

Therefore, as was indicated on several previous occasions, the most effective gap minimizing approaches involve establishing a near steady state engagement on parallel lanes prior to the execution of the merge. This option may be more possible if the line vehicle slows to meet the engagement. A limited analysis showed that even a modest slowdown rate by the line vehicle was very effective in moving the gap requirement closer to that required on the basis of initial conditions.

Summary merging transition concerns: The previous examples illustrated the problems of gap formation, length, and relationship to a fully controlled vehicle during a fully controlled merge situation. Additionally, the entry facility was assumed to be finite and dedicated to entry only. Even though the analyses were very simple and the conditions optimum, a number of questions arise:

1. An existing vehicle pair must be identified between which an appropriate gap is created to accept the merging vehicle. Since an appropriate gap must be created in time to physically match the merging vehicle's position, how are these vehicles selected from a string of vehicles? How fast must the gap be created? What slowdown rate is appropriate?

2. How are the commands transmitted to the line vehicle to begin gap creation? How are communications and coordination of motions between the pair of line vehicles and the merging vehicle managed?

3. The minimum gap required consists of a minimum forward separation and a minimum rear separation (plus the length of the merging vehicle). The merging vehicle must insert itself into this gap at the right location. Therefore, the gap must be presented in a proper relationship to the merging vehicle. How are we going to manage these logistics?
4. Merge management requires the designated following vehicle to split its allegiance between two vehicles; the merge vehicle and its previously engaged lead vehicle, which must remain engaged until the merge is completed. How do we handle such dual allegiance?

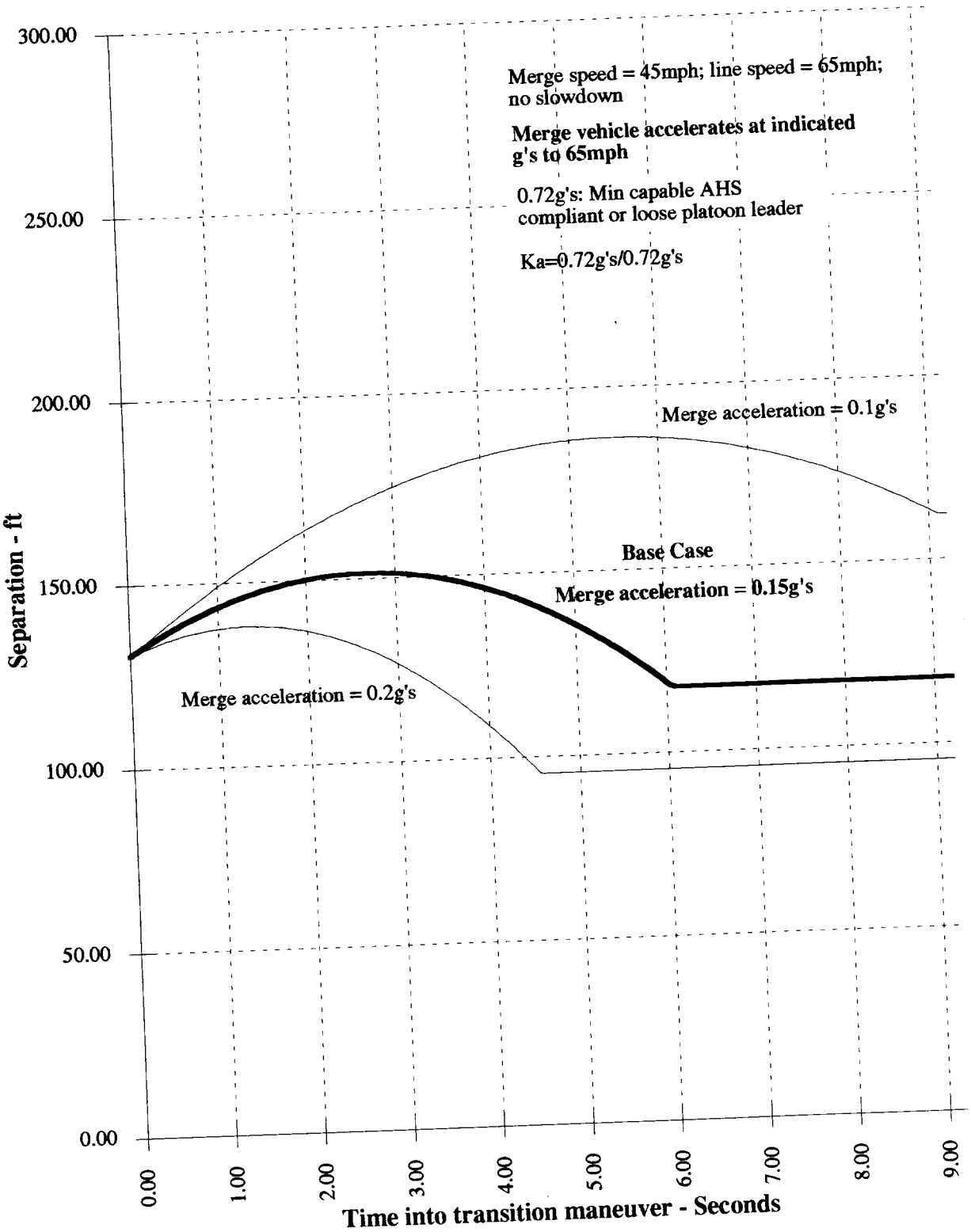


Figure 31. Stopping point differences during merge maneuver for various values of merge vehicle acceleration.

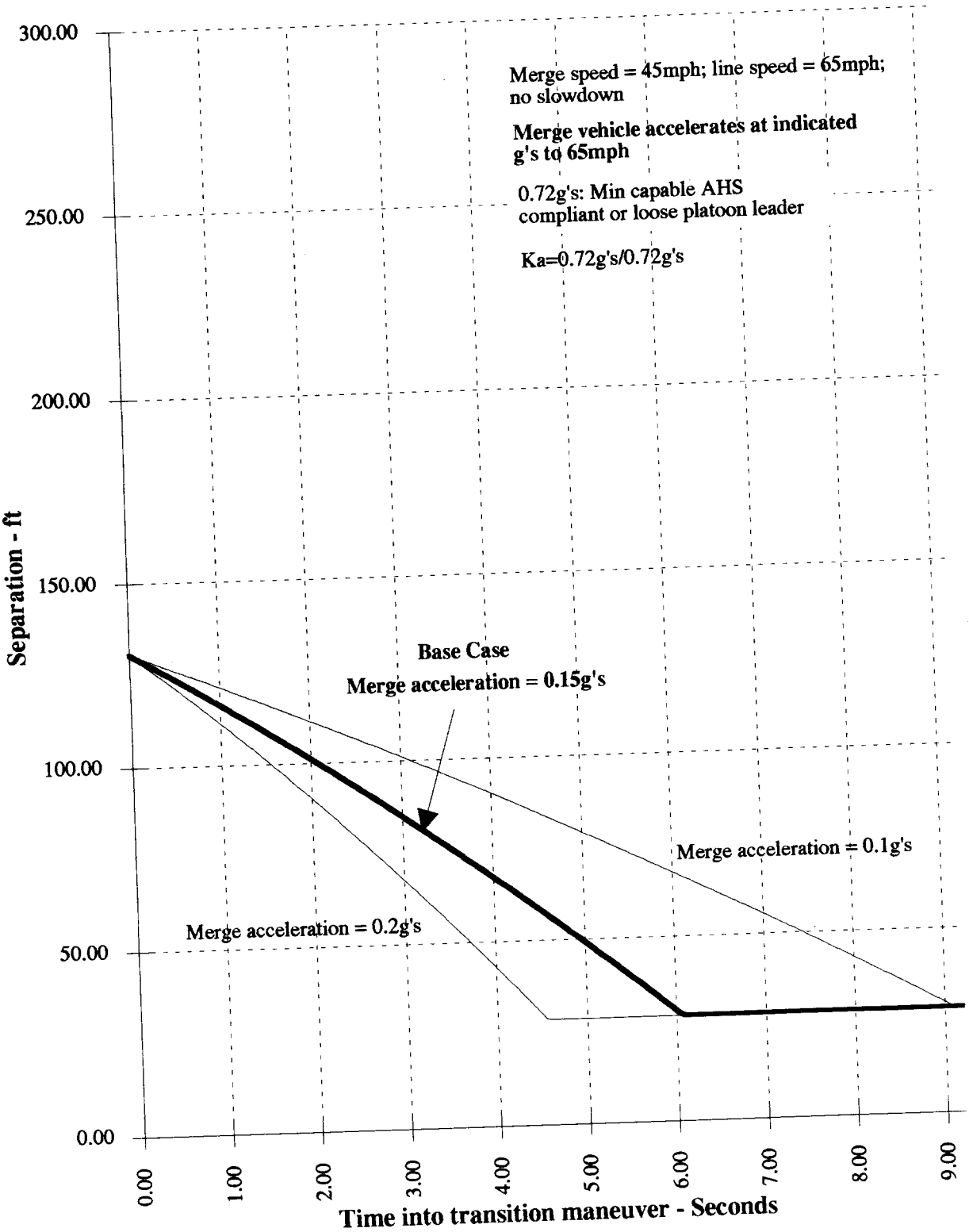


Figure 32. Stopping distance differences during merge maneuver for various values of merge vehicle acceleration.

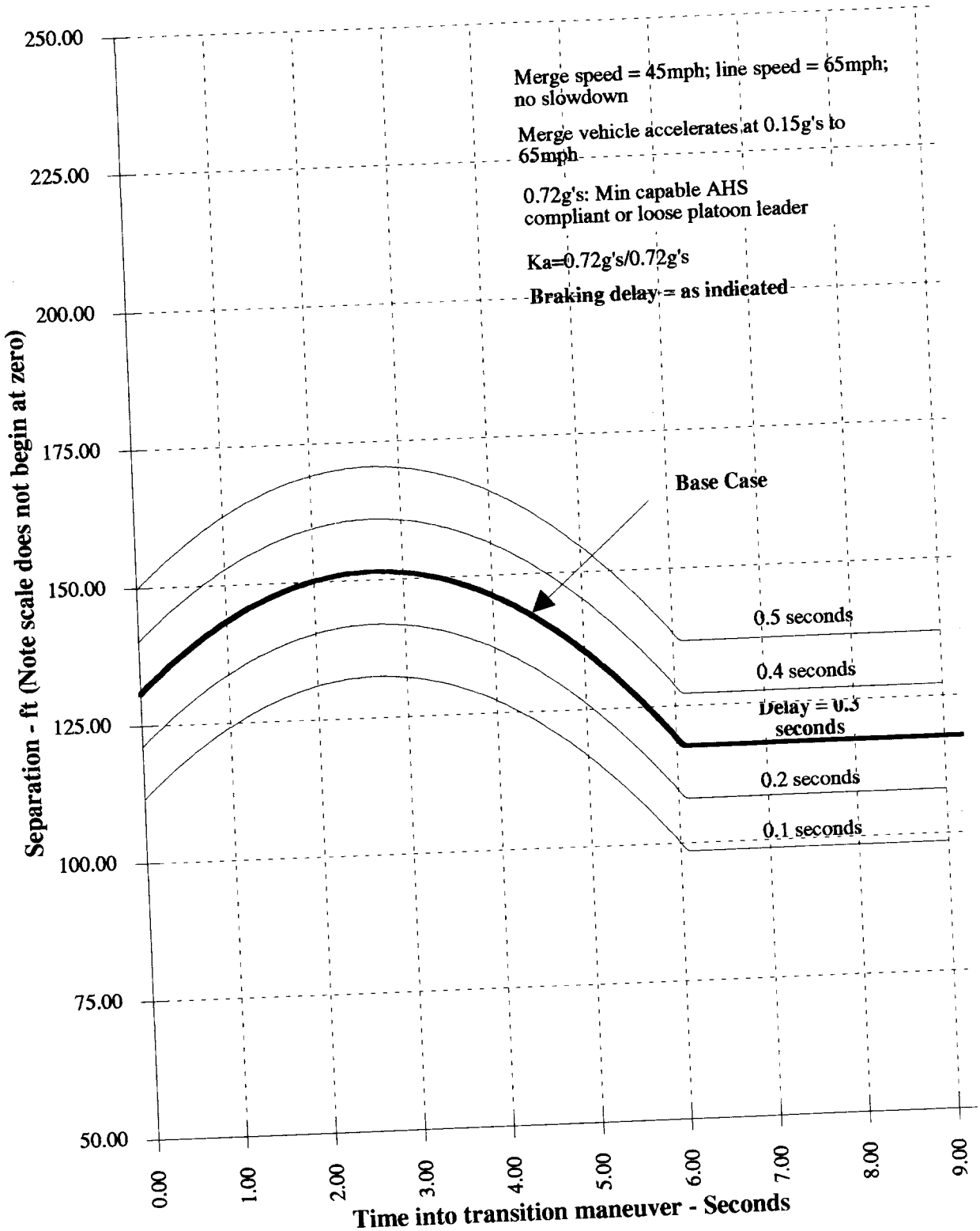


Figure 33. Stopping point differences during merge maneuver for various values of braking delay.

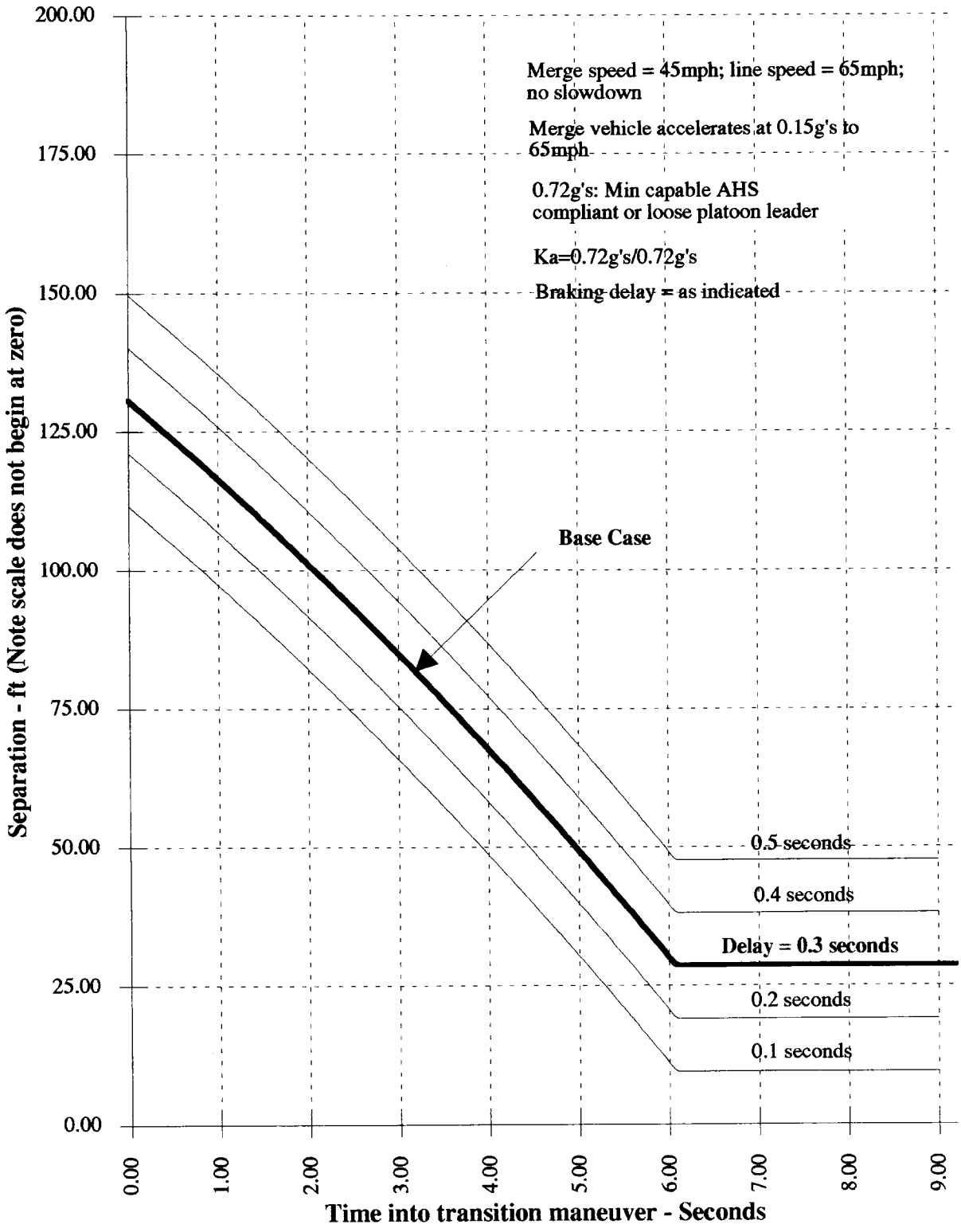


Figure 34. Stopping distance differences during merge maneuver for various values of braking delay.

5. Because the forward and rear portions of the gap are based on the merging vehicle's state when it enters the automated lane, the motions undertaken after it is on the lane, and the engagement dynamics between the merging vehicle and its partners, is there some optimum entry strategy? For example, should a merging vehicle always enter with no suppression of capabilities? This would reduce the forward separation requirements, but increase the rear requirements. Similarly, should a merge always be done at line speed? This would minimize the rear separation requirements, but maximize the forward separation requirements.

Considerations such as these suggest that merging situations may not be manageable if all vehicles are operating autonomously (except in situations where the merging lane is sufficiently large that a near steady state engagement may be established between the designated following vehicle and the merging vehicle). Especially in an urban environment, it is necessary to coordinate merging from entry facilities with some zone control capability.

If the actual merge is manually controlled with respect to longitudinal and lateral guidance, the entire process of safe gap creation and merge accommodation will be fundamentally flawed. The concept of a safe merge is based on coordinated maneuvers, which, in turn, are based on certain expectations of the merging vehicle. If any aspect of this expectation is invalid, a safe merge cannot be guaranteed.

For example, if the merging vehicle is an AHS vehicle being manually controlled (by design or chance), neither the speed nor the position of entry within the gap can be predicted. Some coordination may be possible using signal tactics to indicate the proper merge position, but without positive control, assurance of a safe merge would be lacking. If the merging vehicle is a rogue, even limited coordination is unlikely. If the entry facility is finite and dedicated, a vehicle on the automated lane may infer a merge potential simply because a vehicle is on this facility. However, no other coordination ability would exist. There would be nothing to prohibit the rogue (or the manually controlled AHS vehicle) from entering the automated lane at any opportune time. If this happened, it would have to be treated as a “sudden intrusion” threat.

If we move away from the dedicated and finite entry facility into mixed traffic, transition lanes, the merge problem is compounded. It is very difficult to conceive of an ability to treat mergers of this kind as anything other than “sudden intrusion” threats.

In-Line Transitions

The merging situations discussed above are complicated by the intrusion of another vehicle into a stable in-line engagement, necessitating a 3-way engagement until steady state conditions can be restored. In-line transitions lack this complication; however, the conflict dynamics remain the same. In this section two in-line transition situations are discussed:

1. An overtaking situation where the burdened vehicle must slow to reach a steady state engagement with the privileged vehicle.

2. A closing situation involving a change between two steady state engagement situations.

The analysis technique used is the same as that used for merge transition analysis.

Overtaking transitions: The merge transition conclusions are equally applicable to closing situations where a line speed vehicle is overtaking a slower, but accelerating vehicle. The gap referred to in the merge analyses is the counterpart to the minimum separation that will allow that encounter without slowing the line vehicle and that will provide tolerance to a worst case exposure at any point along the closing maneuver.

The closing situation presented in this section is slightly different: a fast vehicle is approaching a slower, but constant speed vehicle. In this situation, the following vehicle must slow to the lower speed and engage the slower vehicle under the new conditions. The question to be answered is where should this slowdown begin, assuming some maximum slowdown rate (SDR) is desired. As was the case with merge situations, this point is not necessarily a result of requirements based on initial conditions. Stopping point differentials must also be considered. Figures 35 and 36 show the stopping distance differential curves and the stopping point differential curves for the same vehicle combinations used for the merging analyses. The following vehicle is traveling at 65 mph and closing on the slower vehicle, traveling at 45 mph. The closing algorithm is a desired SDR of 0.15 Gs (which may be accomplished by engine braking). As shown in figure 35, the stopping point differential has virtually no influence on the minimum separation at start of slowdown, even when the faster vehicle has minimum braking capabilities. It is much less influenced by other conditions. While we did not specifically examine the influence of certain variables in this transition, it can be expected that the same behavior exhibited for merge situations would also apply for these closing situations.

Changing steady state engagement: The second type of in-line transition illustrates the influence of the closing algorithm on worst case exposure during a closing maneuver from an initial steady state loose platoon engagement to a final steady state tight platoon engagement. As for other transition situations, the goal is to accomplish the maneuver without sacrificing tolerance for a worst case maneuver by the privileged vehicle at any point along the way. Initially, the vehicles are traveling with a separation of 24 feet, with braking capability suppressed to 20 fps/sec. The desired end condition is a tight platoon engagement with a separation of four feet. The question being asked in this section is: “Is it safer to close quickly, with high accelerations and decelerations than it is to close more deliberately?” To represent these closure options, two algorithms were selected:

1. A rapid closure using five fps/sec acceleration for the first half of the closure and five fps/sec deceleration for the last half to a final separation of four feet.

2. A slower closure, with the same balanced maneuver as above, but using acceleration and deceleration rates of 1.25 fps/sec.

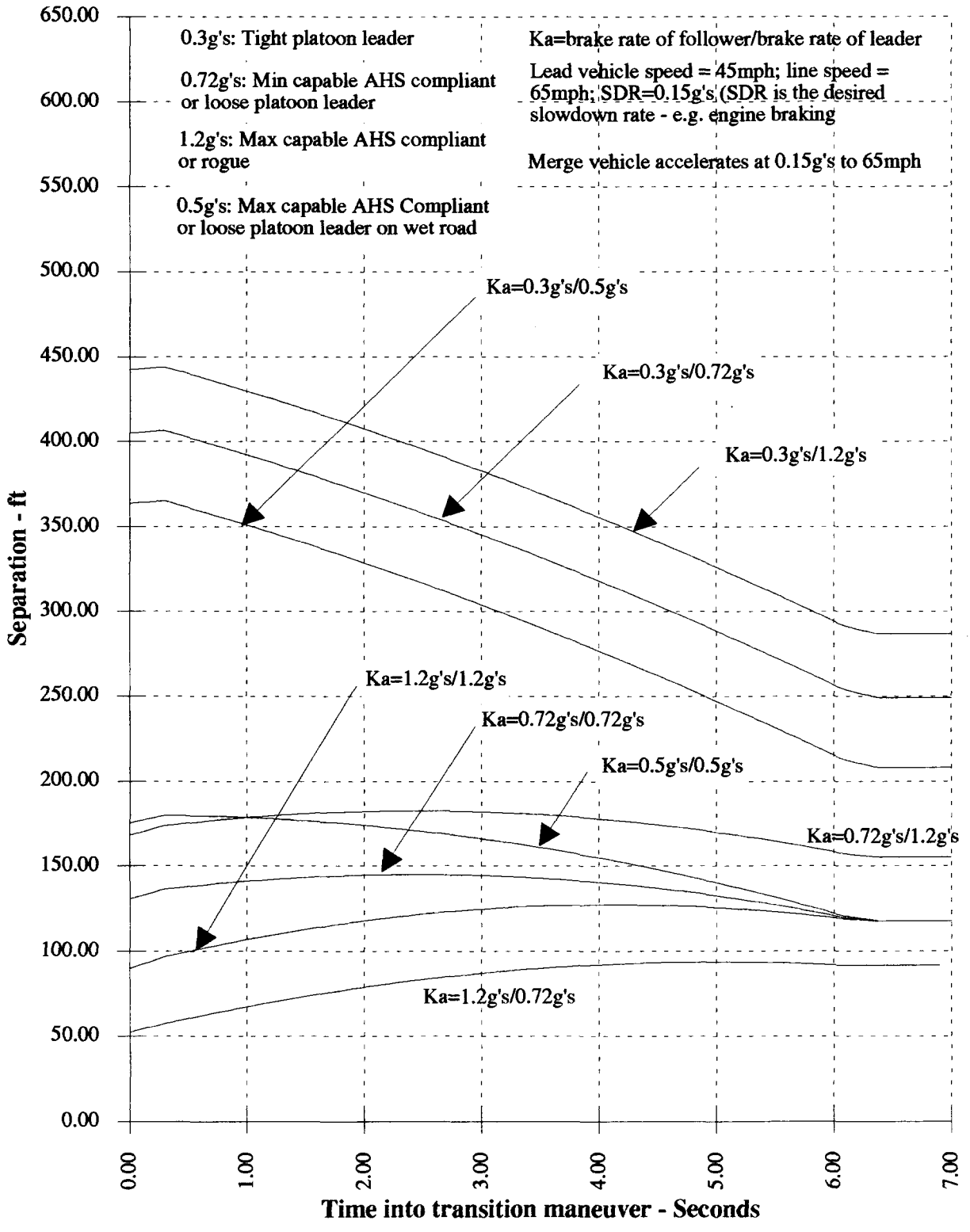


Figure 35. Stopping point differences during closing maneuver for various values of Ka.

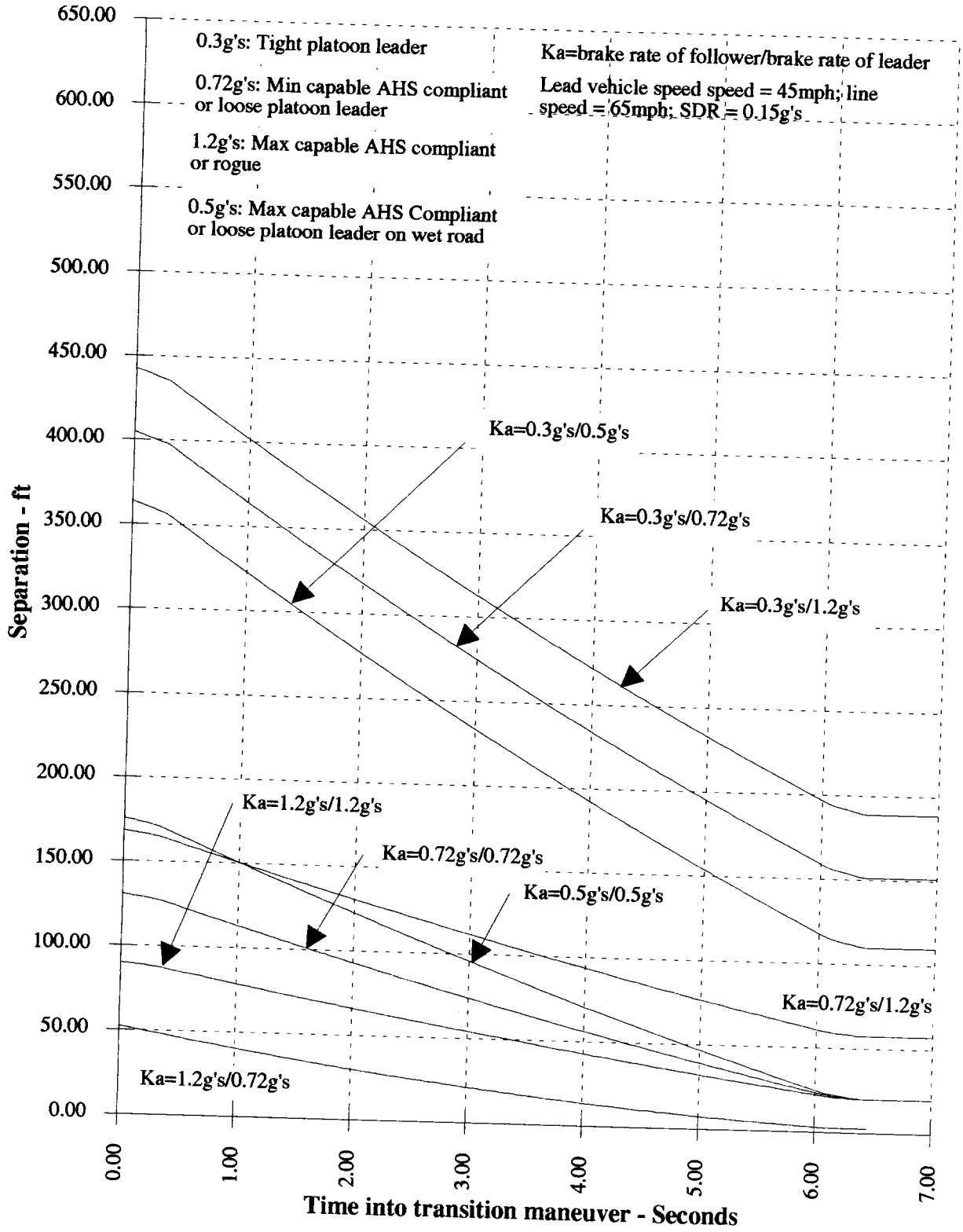


Figure 36. Stopping distance differences during closing maneuver for various values of Ka.

Figures 37 and 38 illustrate the results. The form of these displays is different from those used earlier; however, concepts and analytic procedures are identical. In each of these figures, the lower shaded curve represents the minimum separation required, based on the closing algorithm, to avoid collision under a worst case execution by the privileged vehicle at any point along the way. These curves reflect a required alteration of braking capability for the privileged vehicle. To support a final separation of four feet, the braking rate of the privileged vehicle must be suppressed to 10 fps/sec. In this analysis, it is assumed that this change was instituted at the time the burdened vehicle began its closure maneuver. This is not a necessary condition; however, if any other approach is selected, a different curve would represent minimum separations.

Figure 37 shows the results of the rapid closure algorithm. To tolerate a worst case exposure during the closure path, the actual separation curve must be everywhere above the minimum requirement. As can be seen, this requirement is not satisfied under this rapid closure algorithm. Conflict occurs during the second half of the maneuver. This means that if the privileged vehicle were to stop at 10 fps/sec during this phase of the closure, a burdened vehicle, with a braking rate of 20 fps/sec, would collide with it.

Figure 38 shows that the slower closure algorithm does not promote this exposure.

While we are hesitant to draw fundamental conclusions based on these results, it does appear that a more deliberate approach is favored. What we can forcefully conclude is that any closing situation—any transition situation—has subtle implications regarding worst case exposure during the maneuver and that these implications are primarily influenced by the closure algorithm. The analyses in this report cannot be used as a quantitative expression of these influences; however, they are valid indicators of certain qualitative aspects of influences. Much more sophisticated modeling and simulation are required, using more realistic models of separation controllers and vehicle motions.

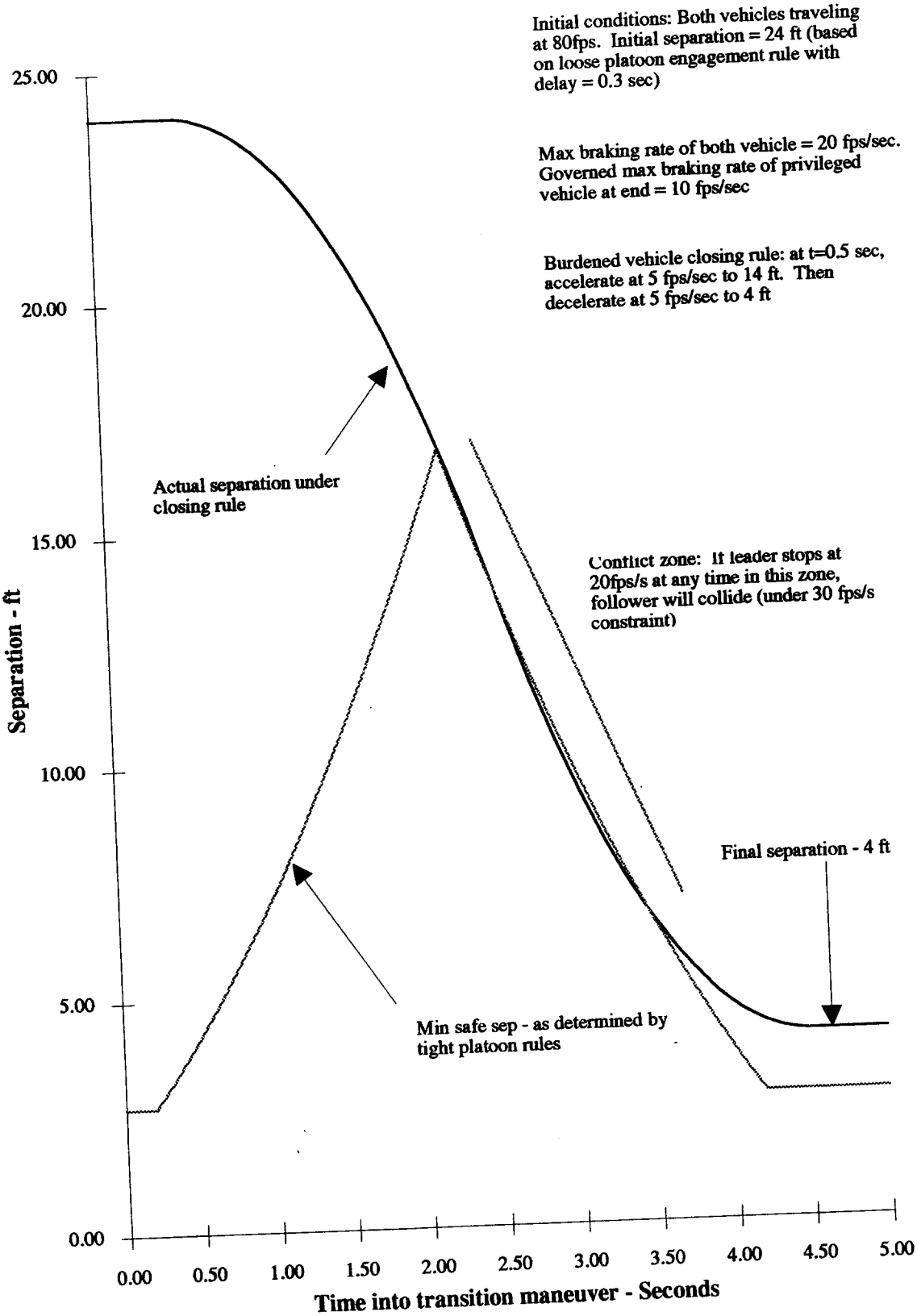


Figure 37. Separation conflict during transition from loose platoon to tight platoon under fast transition rule.

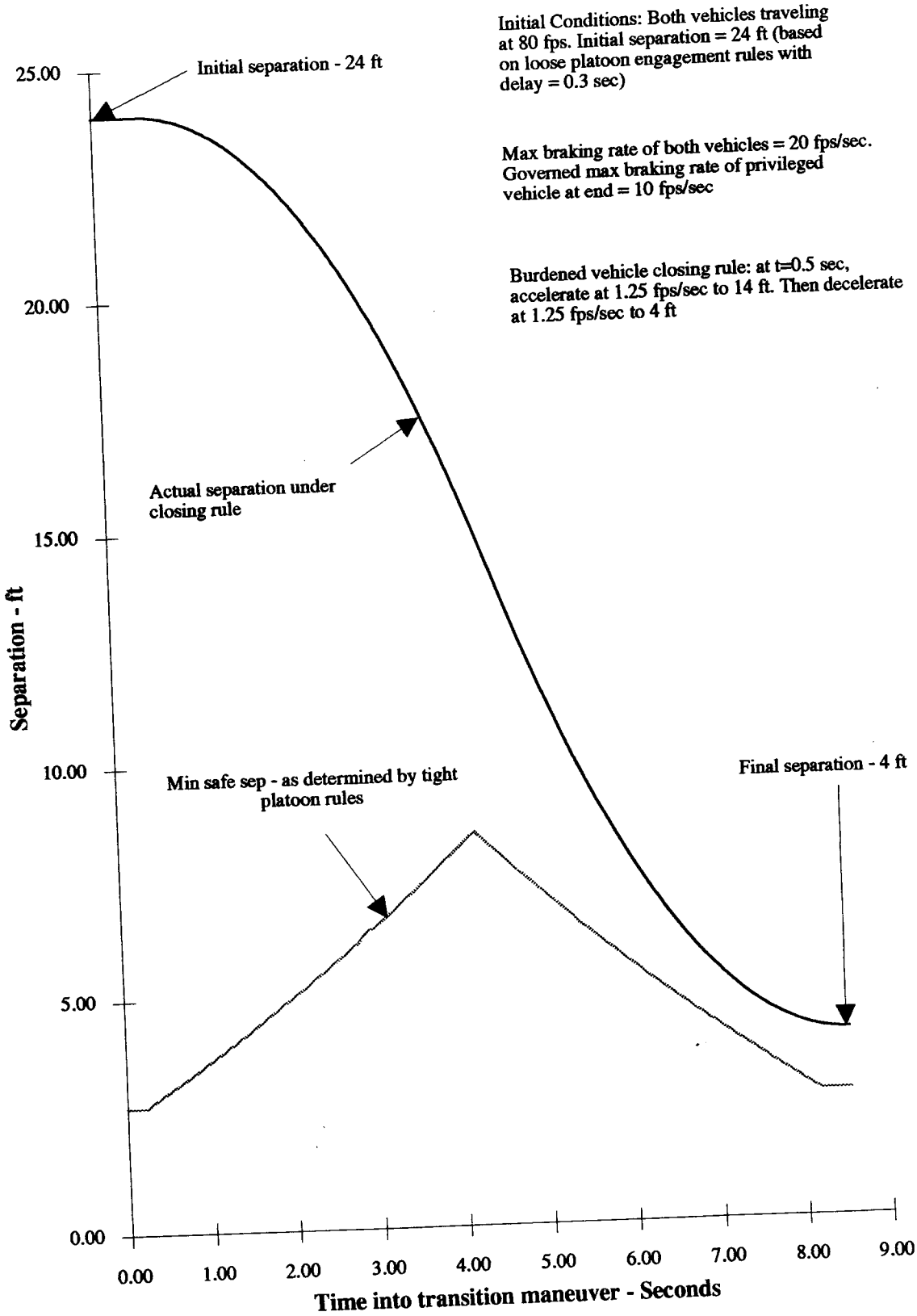


Figure 38. Separation conflict during transition from loose platoon to tight platoon under slow transition rule.

In-line transition concerns: In-line transitions are not as problematical as merging transitions—there is no gap formation or coordination requirement. Three specific concerns exist:

1. As with any transition, the problem of assuming the worst case situation to be that defined by the initial approach conditions exists. Approach strategies must account for potential conflict situations that may occur during the maneuver.

2. The analyses above were directed toward the transition to a closer engagement. Similar conditions exist for disengagement from a close engagement to a more relaxed engagement. We do not suspect the worst case shift exhibited above, but the process of sequencing actions (e.g., removing brake suppression) must be carefully established.

3. Finally, any process of transition must have the capability to abort the maneuver and return to a safe engagement. No action should be taken that places the vehicle in an untenable situation if, for any reason, the transition must be undone.

Exit Transitions

No quantitative analyses of the exit transition were performed. However, considerable thought was given to the quantitative aspects of this maneuver and concerns associated with it. Therefore, this section is devoted in its entirety to these concerns.

As difficult as the previous transitions appear, they have a common characteristic: they are controllable. The exit transition does not enjoy this privilege. It is complicated because it not only involves the physical transfer of the vehicle from the controlled confines of the AHS to the uncontrolled roadway, it also involves the transfer of control from the AHS to the vehicle operator. To accommodate these transfers, and, at the same time abide by the goal of never placing a vehicle in a situation that cannot be controlled poses a significant challenge. The requirement to adjust the vehicles in the AHS lane to accommodate the transfer simply adds to the complexity.

Prudence would seem to indicate that the physical vehicle transfer and the vehicle control transfer should not occur simultaneously. Prudence would also suggest that the transfer of control should only occur when the vehicle is in a stable steady state condition, with a velocity and forward spacing sufficient to enable manual control and to allow the reacquisition of control by the AHS if, for any reason, the control transfer does not take place. To accommodate an exit transfer, three subsystems must be prepared:

1. AHS lane preparation—specifically the actions the adjoining vehicles on the AHS lane must take to accommodate the transfer safely. These preparations include adjusting engagement calibration and/or engagement strategy to accommodate a vehicle leaving an engagement. Included in this general activity is the need to adjust the focus of the existing following vehicle to a new privileged vehicle and to establish an appropriate engagement with that

vehicle. The degree of this preparation depends on the particular exit strategy employed. The leading vehicle also is similarly affected. It must break its current trusted arrangement and establish a new one. If possible, this new engagement relationship should be established before the exiting vehicle leaves the AHS lane.

2. Exiting vehicle preparation—specifically adjusting its motions to be compatible with the control demands it will face in its new environment and the control capabilities anticipated from the vehicle operator. Also involved is the removal of any encumbrances in place; i.e., removal of brake suppression controls.

3. Operator preparation—specifically integrating the driver back into the control loop, calibrating his/her abilities to assume control, and providing sufficient situation awareness to prepare the operator for the control demands he/she will face when manual control is assumed.

By considering the alternative exit options and situations, as well as the inherent problem of control transfer, a number of desired conditions were developed:

1. The final transition from AHS facilities to an uncontrolled environment should be made under full manual control. The facilities should be sufficient to allow the vehicle operator to adjust the vehicle's velocity as he/she considers necessary to make this final transition (e.g., traffic, weather, and road conditions). This should include the option of coming to a full stop before proceeding. If this is not done, the AHS must assume responsibility for the vehicle's safety in a completely uncontrollable situation. We do not believe this to be a viable option.

2. The transfer of control should be made under completely stable and steady conditions. This means that the AHS cannot be controlling a physical transfer maneuver and, at the same time, require manual takeover of control.

3. Steering control may be transferred before longitudinal control if necessary. However, we do not see a safe scenario when longitudinal control transfer precedes steering control transfer.

4. Whenever and wherever control transfer takes place, the AHS should be capable of directing the vehicle to a stopped condition at a safe location if the expected transfer is not completed.

5. AHS control should never be relinquished under an assumption that manual control will be exercised. Control transfer should only be authorized as a result of overt action by the operator. The bias of the AHS should be to maintain control and take the vehicle to the safe place referenced above. This bias should only be interrupted by operator intervention.

6. Automatic exit into an uncontrolled environment is sufficiently problematical that it should not be considered. This specifically applies to exiting, under automatic control, into a

parallel, mixed traffic and uncontrolled facility. (Some concessions are possible for rural operations, as will be discussed later).

7. Once a vehicle exits the AHS lane, it should be denied a re-entry option.

8. If control transfer takes place on the AHS lane (that is, the exit maneuver is under manual control), we have a maximum disruption situation. This vehicle now has the characteristics of a rogue and must be reengaged as a rogue or an AHS compliant vehicle. If the pre-exit engagement is a platoon (loose or tight), the vehicles must disengage and reengage under AHS compliant rules prior to the control transfer. If the engagement is a tight platoon, this process will require establishing a large gap to accommodate the new engagement.

9. If automatic ejection of closely spaced vehicles is employed to minimize disruption, the exit facility and controllability must be sufficiently long to allow the disengagement off-line, by altering separation or reducing speed to permit existing separation adequate under manual control.

By considering these conflicting requirements, a concept for a model exit scenario emerges. To minimize disruptions to line vehicles, it is desirable to exit the AHS lane under full control. This exit facility would be an AHS subsystem, dedicated to the transition of vehicle and operator to a manual control while still on a controlled facility. This exit lane would be physically separated from the AHS lane (after the exit zone) to prohibit re-entry. It would also be separated from the adjacent manual traffic operation. After a vehicle enters this lane, it is still under AHS control, and will continue to be under AHS control to a safe bull pen if the operator does not seize control. The distance from the last opportunity to move to this bull pen must be sufficiently long to enable the operator to tailor the vehicle motions to match his/her perception of controllability (the vehicle must be under manual control before it is allowed to enter this segment).

This option is contrasted to an exit into a mixed traffic transition lane. As indicated above, this option is viable only if it is accomplished under full *manual* control. The full process of disengagement and reengagement must be performed on-line. Also, there must be some provision to reestablish AHS control if the vehicle, after the transfer to manual control, decides not to exit. This situation is certainly not as desirable as the previous one. Although we consider it to be second choice in the urban environment, it is viable in the rural operating environment, where capacity is not an issue. Furthermore, it may be a practical necessity for an economical rural application, using one lane for automatic, but not exclusive operations. In this environment, automated lane keeping and collision avoidance can be viewed more as a service option to an individual driver. As such, it would probably be used to automate that driver's function, using calibrations comfortable to him/her.

An exit transition not yet discussed is an end-of-the-line situation, if it exists. Such a situation would exist at the end of a segment of automated roadway. If the vehicle is forced to exit the lane, the exit conditions are not the same as those involving an intermediate exit. All vehicles will be exiting and the issue of disruption to line vehicles is not present. However, the same issues of control transfer and safe location bias discussed above still apply.

If the automated lane continues, without automatic control, the same principles are involved. Since the vehicles will be continuing on, the vehicle separation must be set to AHS compliant requirements before the last option for automatic vehicle management (to a safe area). This could be problematical, in an operational sense, if the traffic is heavy. The separation requirements for manual control could lead to congestion problems. Of course, if this happens, it is a clear signal of the need to extend the AHS system.

COLLISION THREAT INTERVENTION STRATEGIES

This section presents the results of activity area N intervention strategy investigations. Analyses were performed for the four collision threats analyzed in this research: normal collisions, malfunction induced collisions, sudden intrusion threat collisions, and collisions resulting from transferred threats. The character of the collision events under different collision-inducing situations is discussed. Charts illustrate the severity of the collision events in terms of the number of vehicles involved and the severity of each collision. These analyses primarily illustrate the collision transfer effects of the initial collision and the effectiveness of extremis intervention in reducing the severity. Specific quantitative analyses were not performed to illustrate the effectiveness of corrective intervention actions. The influence of these are obvious: if time is available to disengage from a bad engagement, the intervention is effective. The quantitative analyses did not allow for this time. Therefore, the analyses represent *worst* worse cases.

General Concepts of Intervention

Figure 5 illustrated the general concept of intervention. A portion of this figure is reproduced in figure 39 to further define the components of intervention capability.

Extremis Situation Intervention Strategies

The upper “AND” gate in figure 39 illustrates the positioning of extremis actions to eliminate a collision or to minimize its severity. An extremis situation exists whenever a worst case maneuver is executed by a privileged vehicle and the separation to the engaged burdened vehicle is insufficient to avoid a collision under its current braking authority. In general, extremis actions enhance the ability of the burdened vehicle to alter its stopping trajectory sufficiently to avoid the collision or reduce its severity. In an extremis situation, this is the only option available.

All collision avoidance capability is restricted to straight line maneuvers. Lane change is not considered a viable avoidance option in a design sense. Sudden lane change requirements, if a lane change is possible, would constitute an intrusion threat in the receiving lane. Seeking the shoulder should be an option for the aware driver, but this can't be considered a fundamental capability for extremis actions.

There are three fundamental approaches for extremis reactions by AHS vehicles:

1. Extremis broadcasts: triggered by the recognition of an extremis situation by one vehicle and broadcast to provide information to following vehicles, prompting their extremis maneuver capability.

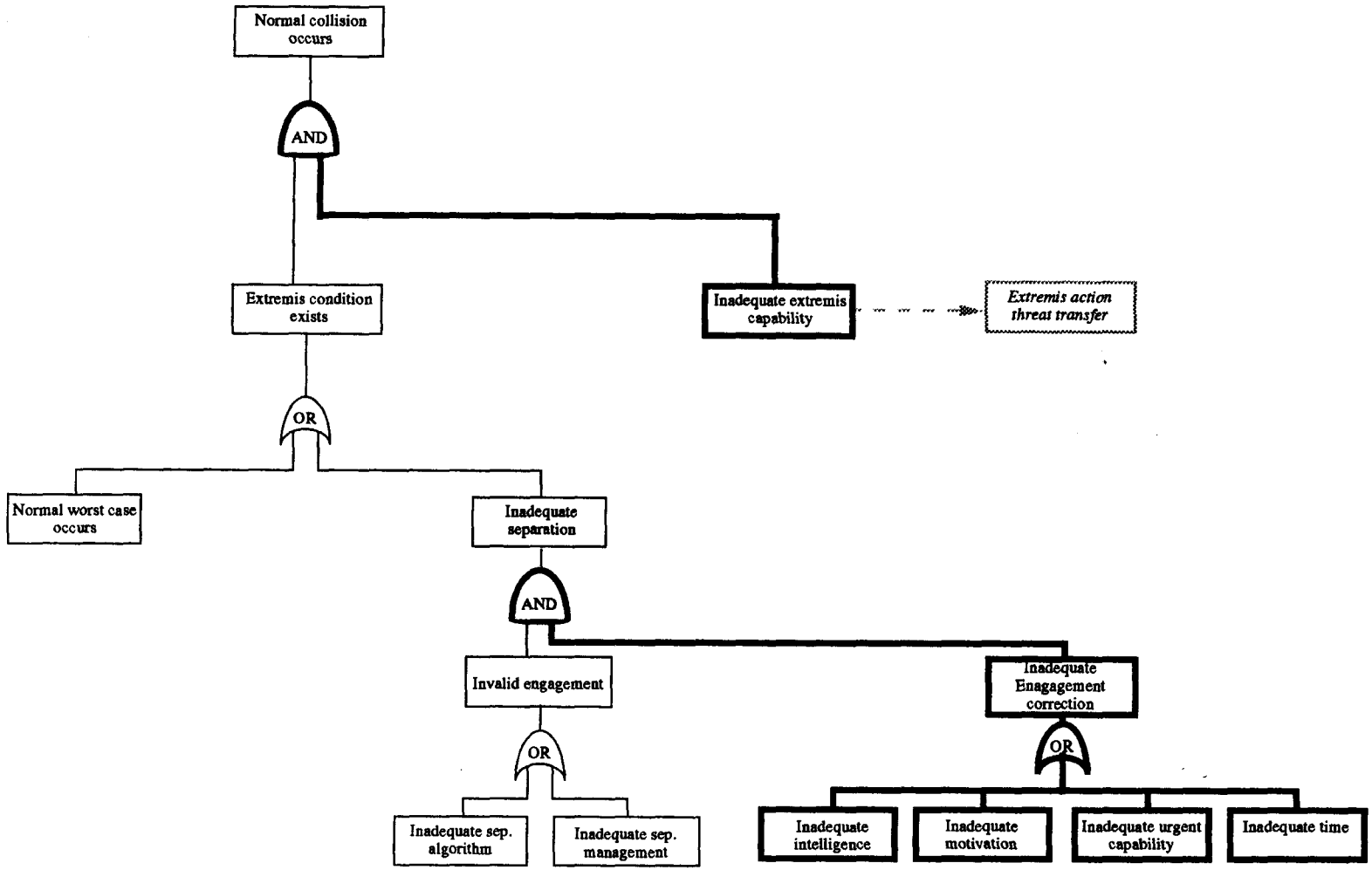


Figure 39. General fault path identifying intervention options and components.

2. Coordinated braking: a by-product of extremis broadcast, enabling all vehicles to execute extremis actions without the problems of stacked delays that are symptomatic of reacting to lead vehicle motions.

3. Extremis braking: applying the full braking capability of the following vehicles.

The first two options are possible for an AHS vehicle engaged under any of the candidate engagement strategies. The last option is, however, available only for platoon engagements. If the vehicle is currently engaged with full capability allowed (e.g., an AHS compliant engagement), no further braking capability exist; and extremis options disappear. By the same token, AHS compliant engagement would rarely be an improper engagement.

However, increasing braking capability is not an action to be taken lightly. Unleashing full braking capability to a vehicle engaged under an assumption of constrained braking rate violates the trust of that engagement and constitutes a transferred threat to following vehicles. This conflict potential suggests that an appropriate extremis action should have the goal of minimizing some overall collision severity measure, considering the number of vehicles involved and the severity of the collisions involved. Therefore, the separation manager should foresee these implications based on the current engagement and have available an appropriate strategy to accommodate an extremis situation resulting from an invalid engagement.

The options listed above are all effective tactics to deal with extremis conditions and should all be in the separation manager's control portfolio. The role they play in collision accommodation is to modify the collision bubble by decreasing its size. In some circumstances, this can be sufficient to place the current separation outside the collision bubble. In other cases, it can shorten the amount of separation increase necessary to place a vehicle outside the bubble. In no case, however, do these bubble modification approaches function as a final accommodation action. This requires corrections to the invalid engagement.

These effects are illustrated in figure 40. This figure illustrates collision bubbles that represent an increased exposure due to some inadequacy of collision prevention actions and the influence extremis capabilities may have on reducing it. Also indicated in this figure is the intended effect of separation correction intervention. The desired situation would be for these correction actions to be fully effective in adjusting separation before a worst case exposure. When this can be done, extremis options would not be required. Until these corrections have been made, however, these potential extremis actions buy time and interim protection to reach a new steady state engagement.

In the situations analyzed in the following sections, the implications of extremis actions were investigated. Extremis braking rates were considered to be available for tight platoons because of the severely suppressed braking rates used in normal operations. An extremis option for loose platoons consists of broadcast capability and coordinated braking. No reserve braking capacity was assumed. The extremis options are, by the nature of their location as an intervention when collision is imminent, relatively immune to differences based on the conditions that led to the extremis

situation. Therefore, differences in requirements or options for extremis opportunities are not relevant in these detailed analyses. Furthermore, the influence of extremis actions generally have the most effect on transferred collisions.

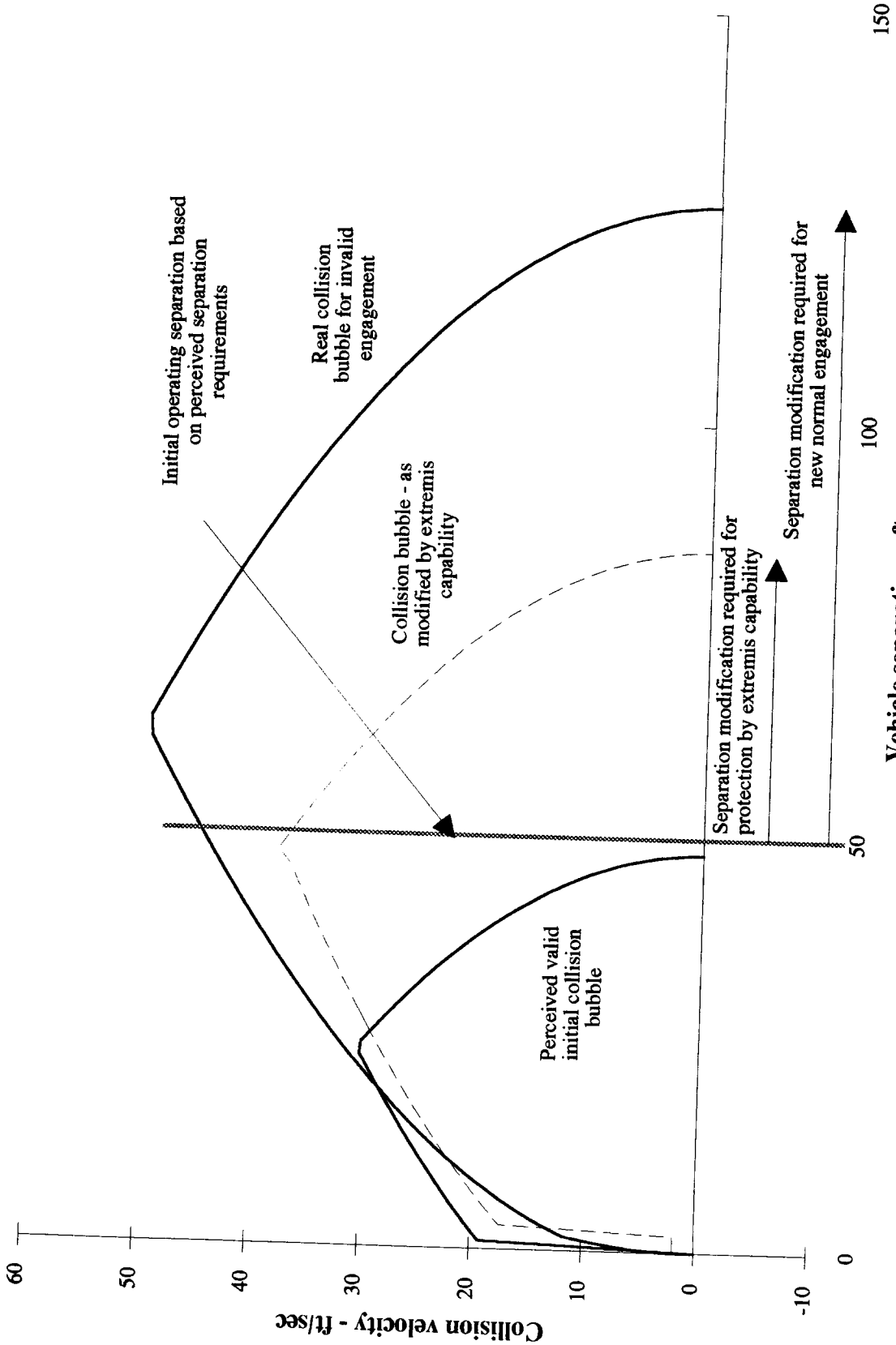


Figure 40. Graphic representation of fault intervention concepts.

Urgent Separation Adjustment Strategies

The second "AND" gate in figure 39 is positioned to enable the separation manager to intervene in the collision path allowed by an invalid engagement—to correct the invalid engagement before an extremis situation arises.

The collision threat from an invalid engagement is greater if the engagement involves small separations. Therefore, the actions taken to correct an invalid engagement are always directed toward increasing separation: the most powerful tool to minimize collision occurrence and extent is *distance*—specifically the separation before the initial collision inducing event. This translates to *time*—time to establish a more tolerant separation before the potential collision is induced. In every collision, the collision does not occur until a worst case maneuver is executed. Even seconds before a worst case maneuver is executed, valuable time is available to adjust separation to more accommodating values.

To accomplish this separation adjustment, four elements are required, as illustrated in figure 40:

1. *Intelligence* regarding the invalid engagement, before it evidences itself in an extremis situation, is the key to initiating a disengagement. The specific information is a function of the fault paths that led to the invalid engagement. To intervene in an invalid engagement resulting from a malfunction, for example, it is necessary to know that the malfunction occurred.

2. *Motivation* to effect the desired changes. An obvious motivation could be some signal suggesting a bad engagement. However, this is not a preferred method. A preferred method might be to consider any engagement "normally open, held closed," with the holding force being evidence that the key conditions of validity for that engagement exist. If any positive information is missing, the vehicle will immediately disengage and seek a more appropriate engagement state. In other words, the bias is always toward a safer state.

3. *Urgent capability* refers to the ability to take appropriate action with urgency. Urgent tactics can be employed to move away from the affected vehicle quickly. These urgent tactics may involve empowering vehicles to use more of their capabilities than are used under the steady state engagement, but less than those that might be used under an extremis situation. Once outside the influence of the invalid engagement, a more leisurely tactic can be used to continue the separation until the desired steady state engagement is reached. However, every vehicle is engaged in two directions; and the ability to take actions with respect to one engagement is constrained by responsibilities to the other engagement. For example, a vehicle engaged as a leader of a tight platoon, with suppressed braking capability, cannot arbitrarily use full unlimited braking capability responding to a forward threat without considering the effects that this action will transfer to the following vehicles in the platoon.

4. *Time* ties these elements together and is an uncontrolled variable, which underscores the need to take all accommodating actions with a sense of urgency. This translates into *preparation*

to take action. Therefore, as with extremis action planning above, urgent action possibilities should be planned by the separation manager before they are required, based on the constraints imposed by the existing engagement. Contingency plans should be available at all times, with due consideration of existing engagement obligations.

Unlike extremis intervention, the requirements for separation correction intervention are dependent on the reason the engagement is invalid. This directly influences the type of intelligence required under 1) above. Therefore, in the details that follow, these differing requirements are discussed.

Normal Collision Threat Intervention

This section examines the implications of errors in establishing running separation for normal engagements—everything is operating as expected. The view is to steady state engagement errors. As was indicated earlier, transition interactions and the development of collision bubbles for these involve establishing such a contrived set of conditions that, the simple models used in this investigation would yield similarly contrived results. The dynamics and collision implications for transition maneuvers require sophisticated simulation tools and should be examined in the context of any specific concept and control law. However, the results probably will not alter the inferences that can be drawn on the basis of these simpler analyses.

Figure 41 is a high level fault-tree representation of the fault paths leading to a normal collision. This figure also illustrates the placement of intervention options to counter errors in establishing running separation.

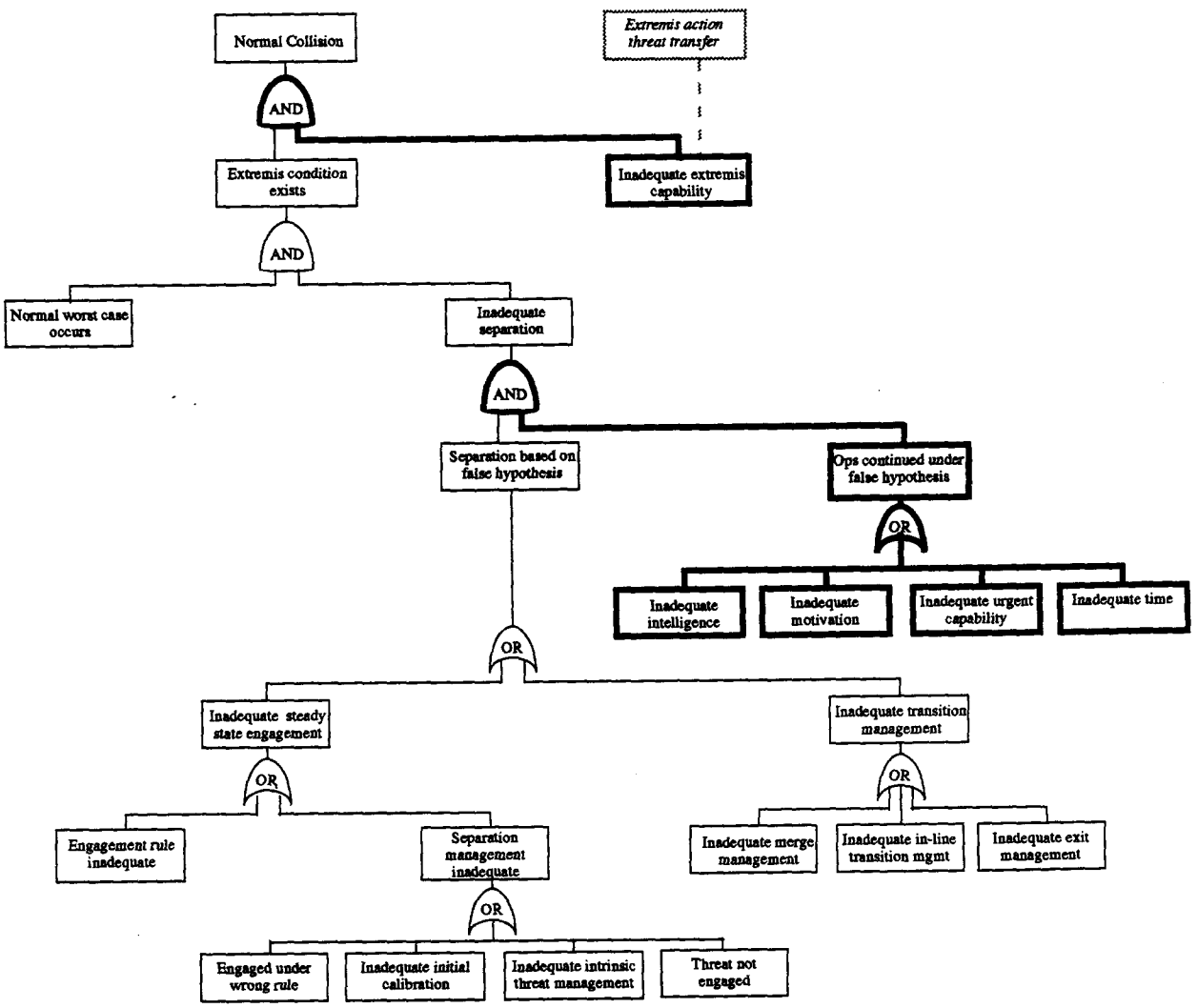


Figure 41. General fault path identifying corrections to faults leading to normal collision.

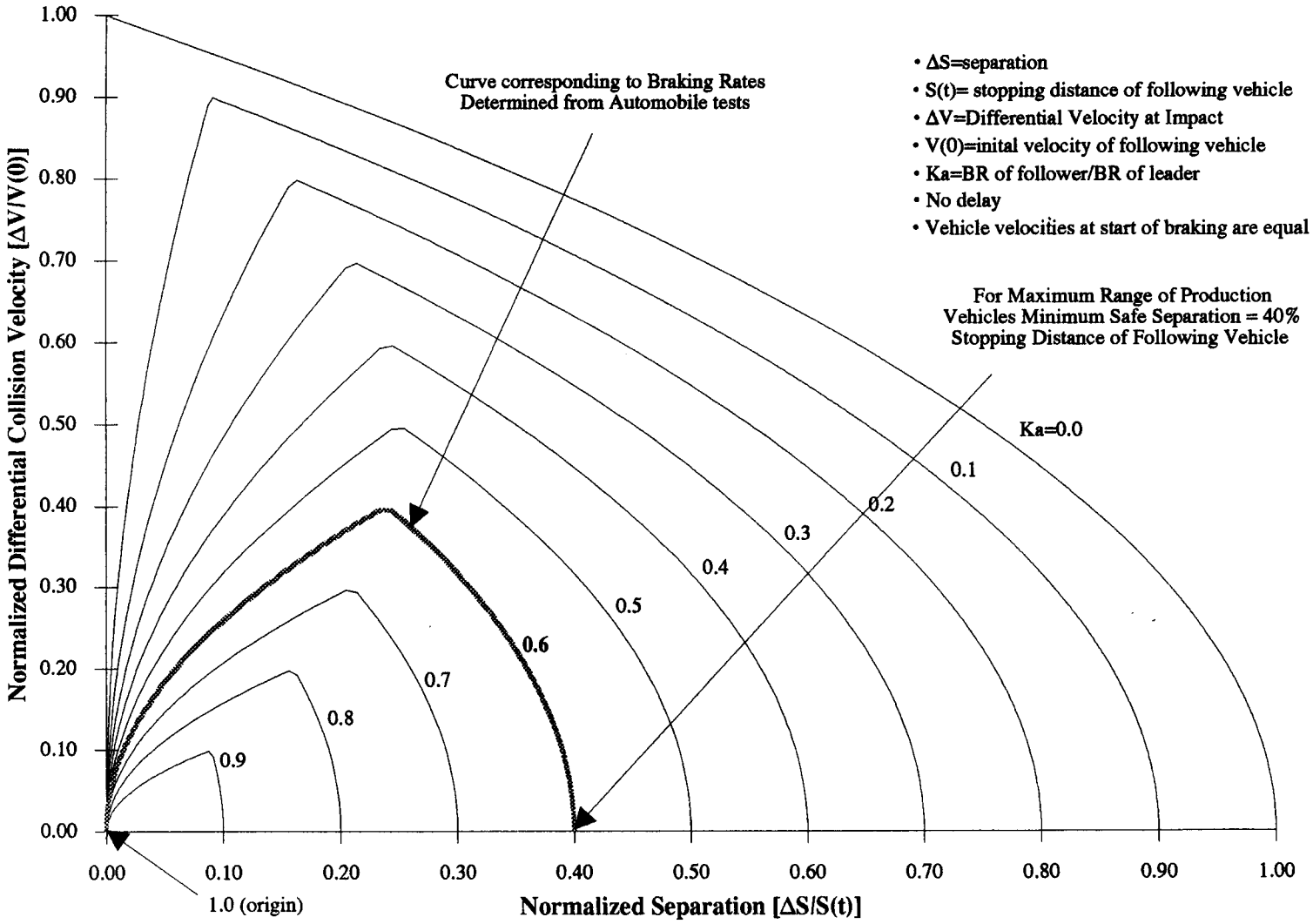


Figure 42. Normalized collision bubbles for various braking ratios.

Characterization of Normal Collisions

Figure 42 displays minimum safe separation requirements under varying ratios of stopping distances between vehicles. The format is in the form of normalized collision bubbles. In addition to illustrating the no-collision separation, (values that lie along the abscissa), these bubbles show the implications of operating at less than this minimum. The abscissa is normalized to a ratio of separation to stopping distance of the following vehicle. The ordinate, which shows the collision velocity if a collision occurs, is normalized to the velocity of the following vehicle.

Figure 42 displays separation requirements for the case where there is no response delay in brake actuation in the following vehicle. Both vehicles are traveling at identical nominal velocity, and there are no transient deviations around this nominal velocity. The bold curve represents the braking rate range exhibited in late model production vehicles. The outer bubble represents a fixed object, while the zero point represents a theoretical zero separation. This latter only exists because of the above assumptions. Figure 43 adds some realism to the situation by including a delay time of 0.3 seconds and a velocity deviation (Kv) of 1.05 (this means the following vehicle may be traveling at five percent above the nominal value at the time the leader imposes its worst case stopping trajectory). As noted in a previous section, the influence of slight deviations about a set point are most influential in small separations. The small separation area shows the required similar braking rates if small separations are to be safely supported—as in operational strategies using platooning.

This form of display is useful to determine the implications of changes in separation influencing variables. The implications of deploying extremis actions to modify the collision bubbles were not examined. The expected response is similar to that developed for malfunction induced collisions.

As illustrated in figure 41, the fault paths that permit separations less than the minimum safe requirements reflect flaws in the fidelity of the separation rule. A major portion of appendices A and B is devoted to specific identification of faults that can lead to inadequacies that cause such flaws. If inadequate separation is a result of these fundamental flaws, the ability to provide intervention at a corrective level is probably nonexistent, or, at best, of limited value. We would probably have no basis to question the engagement validity: the same flawed capabilities would be judging the wisdom of a previous decision. We probably would not be aware that the separation was inadequate until it was demonstrated in a collision—the same problem we face in the current highway system. This reflects concerns expressed earlier that designing for fundamental adequacy in separation strategies and management capability, which includes the knowledge of limits of validity and the ability to sense when those limits are being approached, is a critical requirement for an AHS.

These basic flaws, however, are not the only factors that permit an invalid engagement. The decision processes involved require capabilities in situation awareness to provide data to drive the

decision process. The initial engagement strategy and calibration require assimilation of signals from many sources. An important part of the separation manager's task will be to sort out

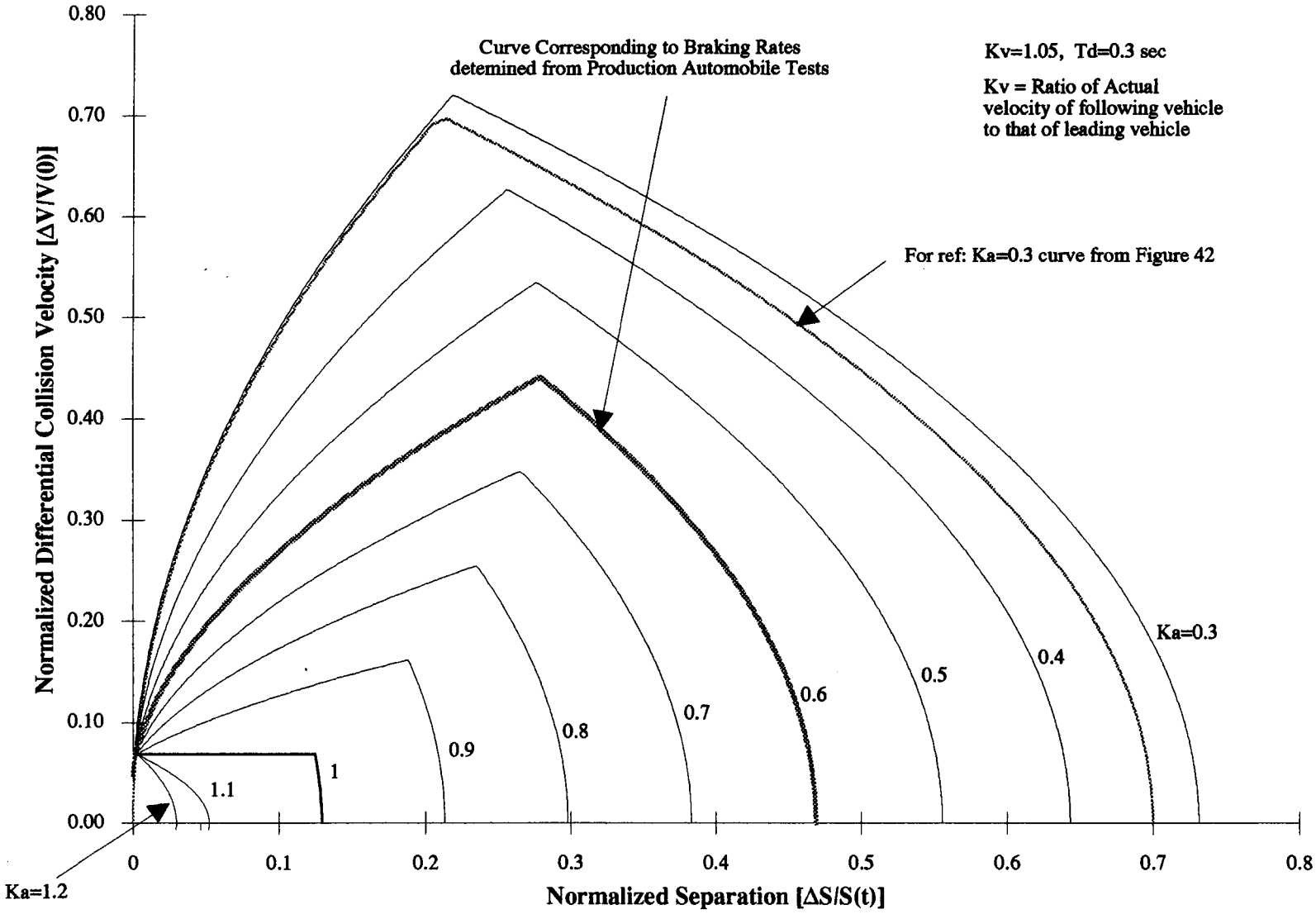


Figure 43. Normalized collision bubbles for various braking ratios with a reaction time and Kv influence.

the significant data and provide the correct response. This is not a trivial process, and some errors in judgment may result in invalid initial separations.

However, a more likely fault path involves the failure to respond to situation changes. This can result in the invalidation of an initially valid separation strategy. This controllability degradation is an intrinsic threat and is illustrated in figure 41 as inadequate intrinsic threat management. Engagement strategies that depend on precise values of braking capability are more sensitive to intrinsic threats. Changes in road conditions, such as rain or snow, must be monitored and reflected in the existing separation or, if the situation warrants, in changes in the basic engagement strategy.

This monitor-and-react capability is further complicated by the necessity to react *before* the situation is encountered. Providing this capability will present a significant challenge to an AHS. It will be most difficult for concepts that base separation control capability in the vehicle. Infrastructure capabilities for roadway conditions may have to be incorporated into the AHS. However, in rural operations, where separation management must be vehicle-based, the capability to monitor roadway conditions and effect appropriate alterations in separation must be vehicle-based.

Engagement Correction Intervention Implications

To initiate an intervention action, the separation manager must be aware that an invalid engagement exists. This requires the separation manager to constantly challenge its own wisdom regarding previous decisions. An existing separation strategy should be considered as "momentary," based on the best information available at the time; and the process of establishing and calibrating an engagement must be a continuing process. The separation manager must continually monitor relevant data and reexecute the decision algorithm.

Information that suggests that a separation manager is not completely "healthy" should render any previous decision suspect. Because of the critical role played by the separation manager, constant self health appraisals are essential, coupled with appropriate strategies for safely managing the vehicle if the separation manager is impaired. The observed behavior of the another vehicle sharing an engagement strategy may also indicate a need for intervention. Actions that suggest that a vehicle is not playing according to the rules believed to be in effect are indicators of an invalid engagement.

If, for any reason, the conditions required for establishing the validity of an existing engagement are not present, a safer engagement should be sought that is consistent with the newly formed situation hypothesis. The separation management function must be capable of forming hypotheses and establishing rules to assure valid engagements.

Malfunction Threat Intervention

The majority of this investigation was concerned with the implications of various operational strategies for safe separations. As stated earlier, the perspective was adopted that an "unfailed"

(innocent) vehicle would be isolated from malfunctions elsewhere. Full success in this approach would, ideally, make a passenger in an unfailed vehicle oblivious to malfunctions that affect vehicles around it. Such a lofty goal is unlikely, but possible, within the capabilities of a separation management function to safely engage malfunctions that may occur.

Figure 44 is a high level fault tree representing malfunction accommodation options. However, even though adequate capabilities may be available to accommodate a malfunction, these options should never be used in lieu of taking reasonable steps to eliminate the malfunction.

The implications of four malfunction situations are discussed below to illustrate potential collision consequences and collision transfer mechanisms and to test the influence of some severity reducing techniques. Following this discussion, requirements for separation correction intervention are presented.

Characterization of Malfunction-Induced Collisions

A malfunction is defined as an occurrence that destroys the validity of an existing engagement. Therefore, the malfunction exposure of a specific vehicle is derived from both the vehicle itself and the vehicles with which it is engaged. As will be discussed later, the purpose of malfunction accommodation is to deal with these malfunctions before collisions occur. Once a collision occurs, we are in a threat transfer situation where our concern shifts to minimizing the extent of the collision. As a result, the collision analyses in this section are not much different from those analyzed under the threat transfer investigation. However, the possible methods of accommodation are sufficiently different to warrant a conceptual separation.

The analyses in this section are particularly concerned with the more intimate engagement strategies: loose platoons and tight platoons. These engagement strategies have the common characteristic of operating under a suppressed capability. As a result, they are prone to a potentially severe failure mode that is not characteristic of other engagement strategies; failures that lead to a vehicle braking too fast—setting up a more severe worst case situation for all following vehicles.

Situation 1: Loose platoon, brake suppression control failure: The first situation simulates a condition where a vehicle suffers a malfunction in the brake suppression control device, which results in a leading vehicle stopping too fast. This failure results in a vehicle having its maximum braking capability available—in this situation assumed to be 1.2 Gs (a maximum capable vehicle). This vehicle can no longer discharge its responsibility, as a privileged vehicle, to “present a consistent and predictable worst case maneuver” to a trailing vehicle. The loose platoon steady state conditions are as follows:

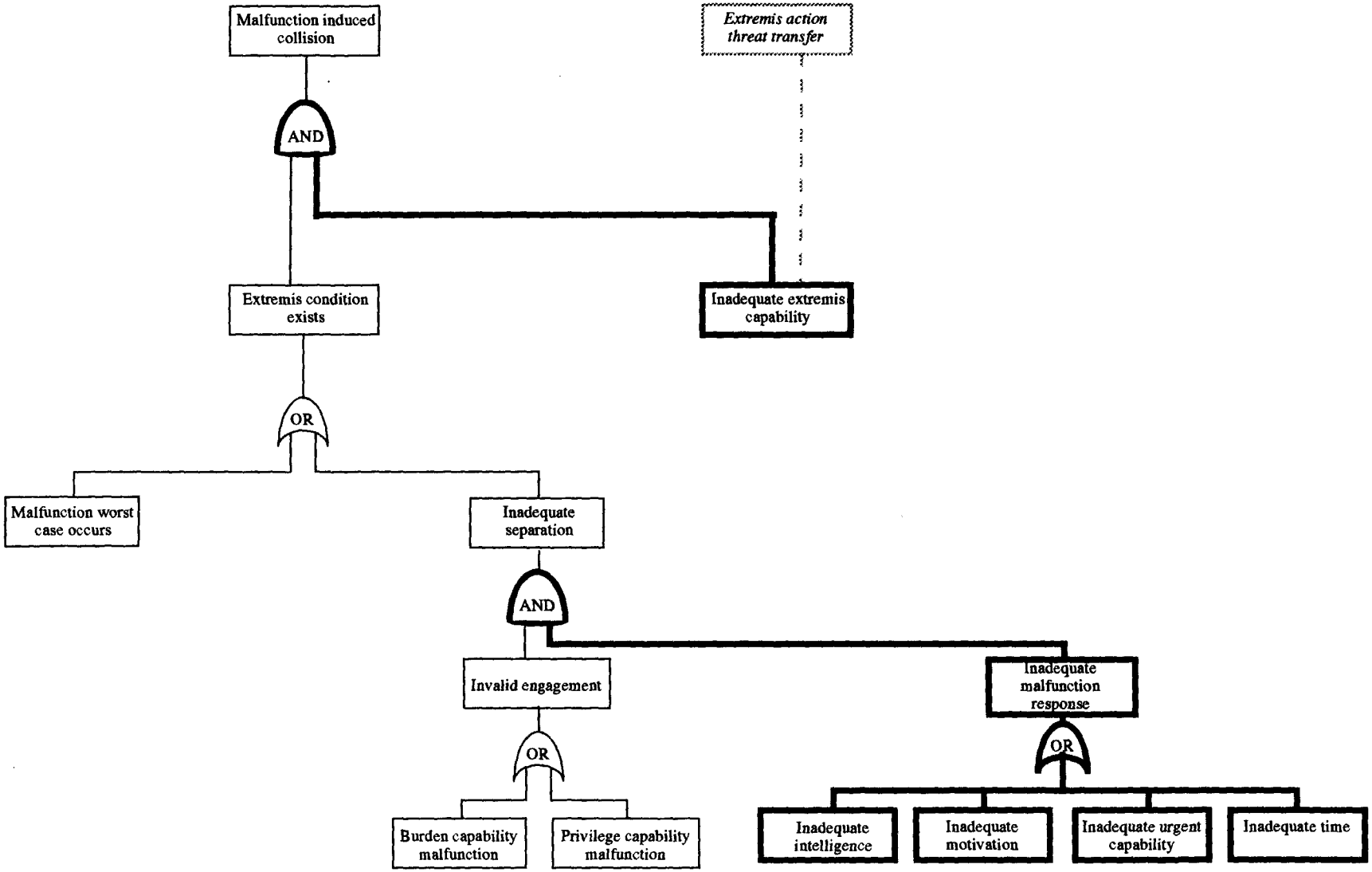


Figure 44. General fault path identifying malfunction accommodation options.

- Platoon speed = 60 mph.
- Intra-platoon spacing = 26.4 ft.
- Response time = 0.3 secs.
- Platoon regulated braking rate = 0.6 Gs.

The collision event was initiated by a 1.2 G stop by the leading vehicle. There was no knowledge of the malfunction until the beginning of the failed vehicle brake application. The failed vehicle was capable of detecting this and broadcasting an "extremis" (collision imminent) alert to the following vehicles. Their response time was reduced to lag the failed vehicle by only 0.1 second behind the second vehicle and perfectly coordinated braking among all vehicles following vehicle 2 was invoked. The second vehicle still retained a delay of 0.3 second behind the failed vehicle.

In developing the collision response, the following assumptions were made regarding the multiple collision effects:

1. A collision "pack" is formed by the colliding vehicles. This pack stays together. As other vehicles collide with this pack, they add to its mass. All vehicles have the same mass.
2. Between collisions, this pack continues movement under a deceleration of 1.0 Gs.
3. An individual collision event (one collision) is completed in 0.05 second.
4. All individual collision events occur in a front to rear manner, with no rotations.
5. Vehicle crush is a linear function of the difference in velocity (immediately prior to collision) between the colliding vehicles. The conversion factor used is one foot of crush/20 fps ΔV. This crush was added to the initial vehicle separations as it represents additional distance available to a following vehicle to act before it collides with the pack.
6. The maximum ΔV of the colliding vehicle was computed by allocating the collision velocity on the basis of the relative masses of the colliding vehicle and the pack. In this context, ΔV is the velocity of change the colliding vehicle suffers during the collision. Thus it is a measure of the collision severity.

Figure 45 shows, in collision bubble form, the results of the collisions induced under this malfunction situation. As shown, in addition to the initial collision, there are collisions involving the vehicles 3 and 4. Subsequent vehicles have the capability to stop before collision.

Figure 46 shows a different view of the collision sequence. This figure shows the velocity profile of the involved vehicles as they approach the pack, collide, and then continue on as part of the pack.

As illustrated in this figure, the colliding vehicle suffers an increasing ΔV as the mass of the collision pack increases, even though the overall ΔV between the colliding objects is decreasing.

Situation 2: Loose platoon, partial brake failure: The second simulated situation is a partial failure of a vehicle that reduces its braking capability by 50 percent—from a loose platoon value of 0.6 Gs to 0.3 Gs. This vehicle can no longer discharge its responsibility, as a burdened vehicle, to "keep clear" of the leading vehicle under the latter's worst case maneuver. The loose platoon steady state conditions are the same as those for situation 1, including the extremis broadcast and coordinated braking. Figure 47 shows the collision bubbles for this situation. As can be seen, there are no secondary collisions. This suggests that malfunctions that increase a worst case presentation are more severe than those that decrease controllability, further suggesting a priority for efforts to minimize these worst case enhancing malfunctions.

Figure 48 shows the velocity profiles for the vehicles involved in this collision sequence.

Situation 3: Tight platoon, brake suppression control failure: This malfunction, as well as the next, examines the same malfunction used in situation 1, except that the brake suppression control failure occurs on a vehicle in a tight platoon engagement. The tight platoon steady state conditions are as follows:

- Platoon speed = 60 mph.
- Intra-platoon spacing = 4.4 ft.
- Response time = 0.3 second.
- Platoon regulated braking rate = 0.3 Gs.

The same extremis broadcast and coordinated braking capabilities exist as for the loose platoon situations.

Figure 49 shows the collision bubbles for this situation. As would be expected, the close spacing of a tight platoon will involve many more vehicles in the collision. The analyses was only carried to 11 vehicles. The velocity curves in figure 50 show that even with only 11 vehicles, the collision severity on subsequent vehicles is still rising. Furthermore, these are not small ΔV collisions. This behavior is unacceptable, and suggests that the malfunction management strategy for tight platoons must be biased toward very reliable systems.

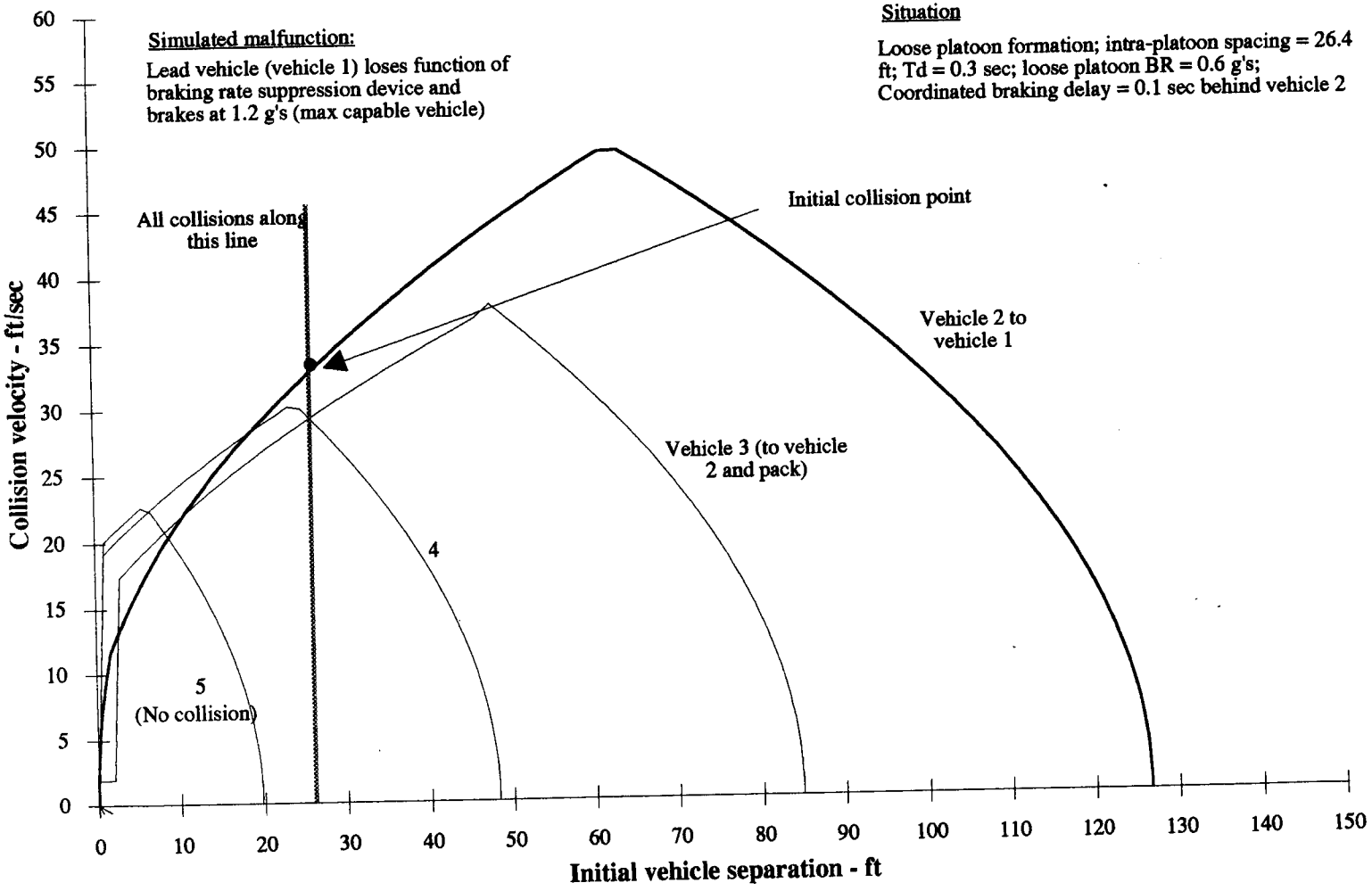


Figure 45. Collision bubbles for simulated malfunction—privileged vehicle brake control failure.

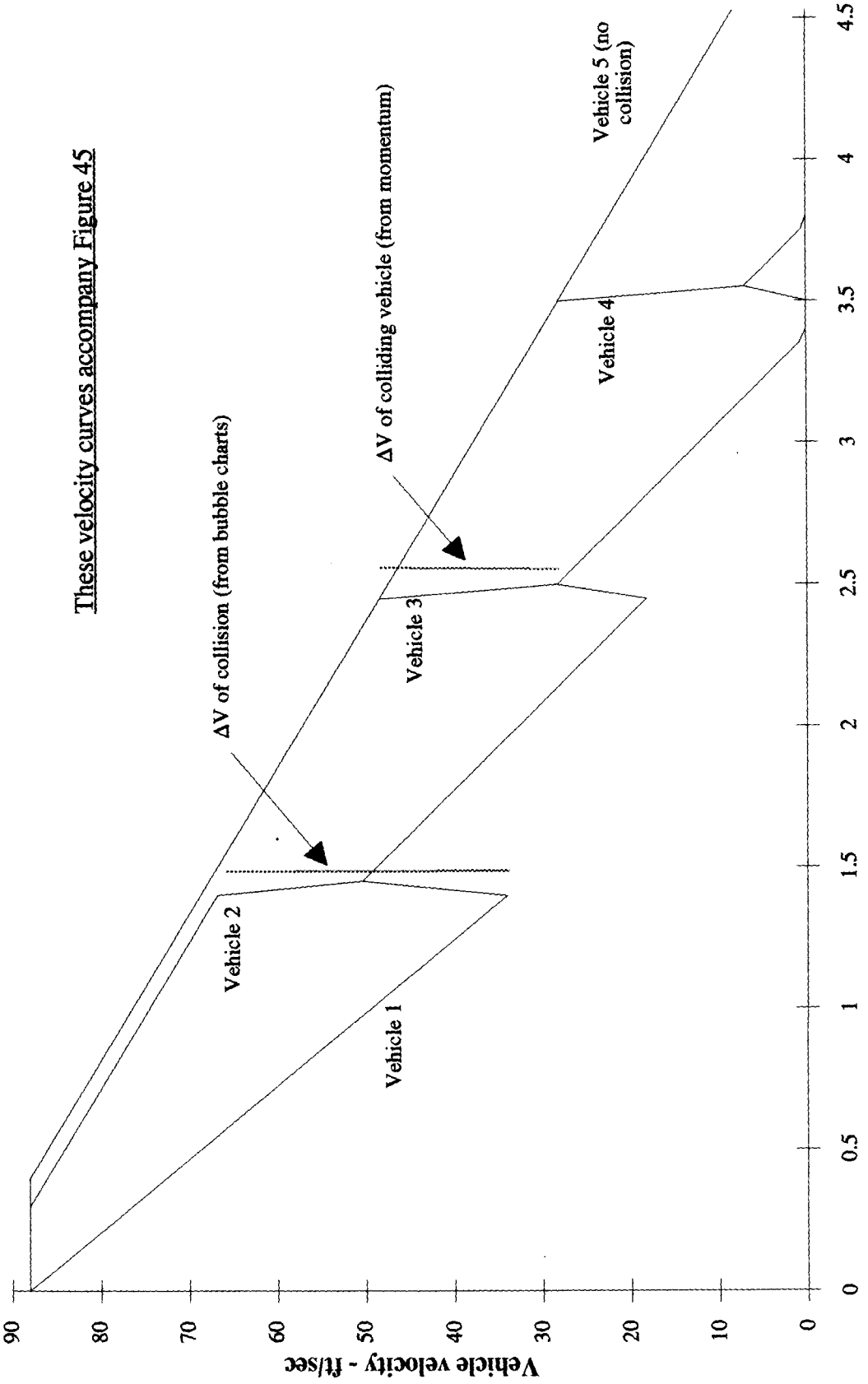


Figure 46. Vehicle velocity curves during collision event.

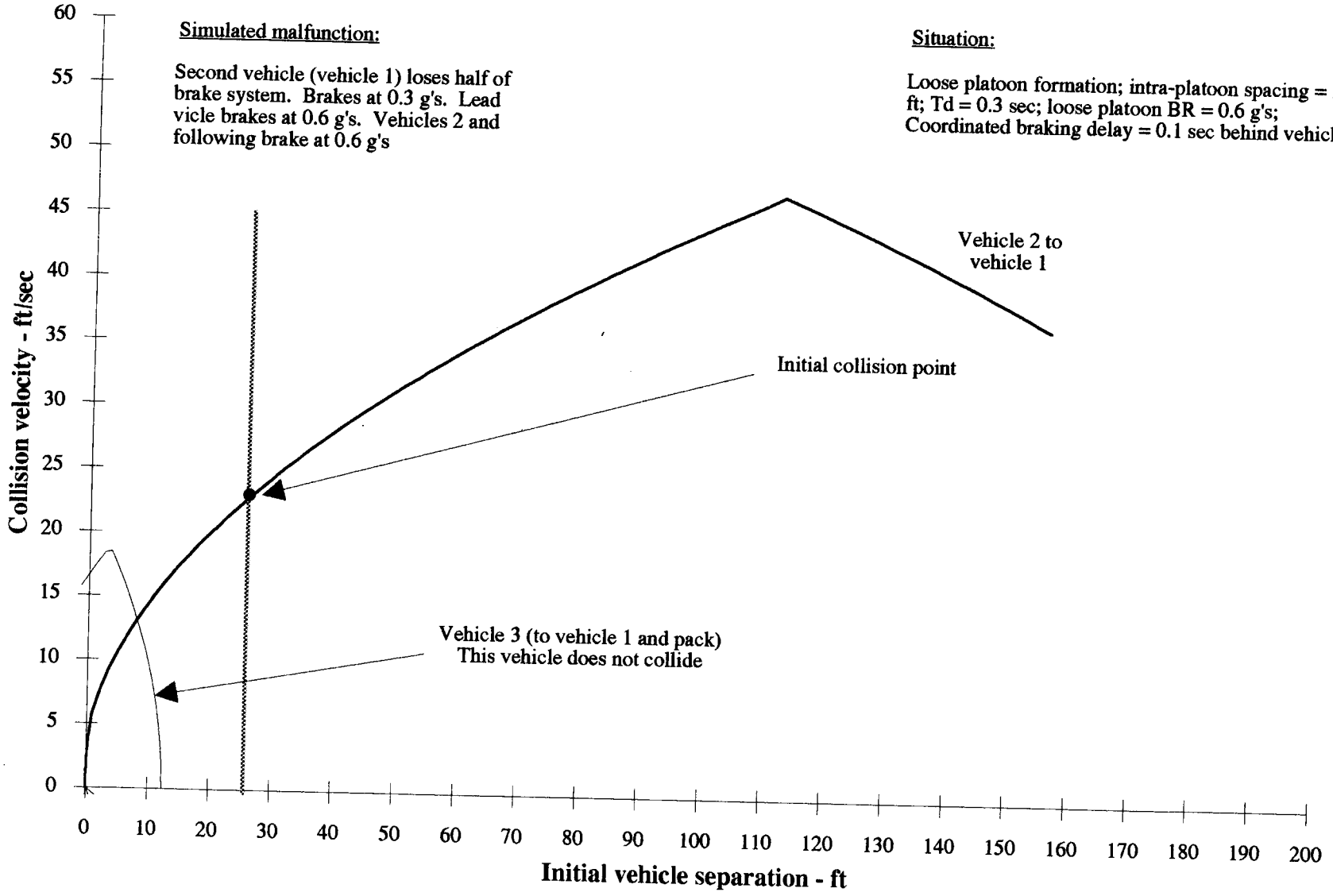


Figure 47. Collision bubbles for simulated malfunction—burdened vehicle brake failure.

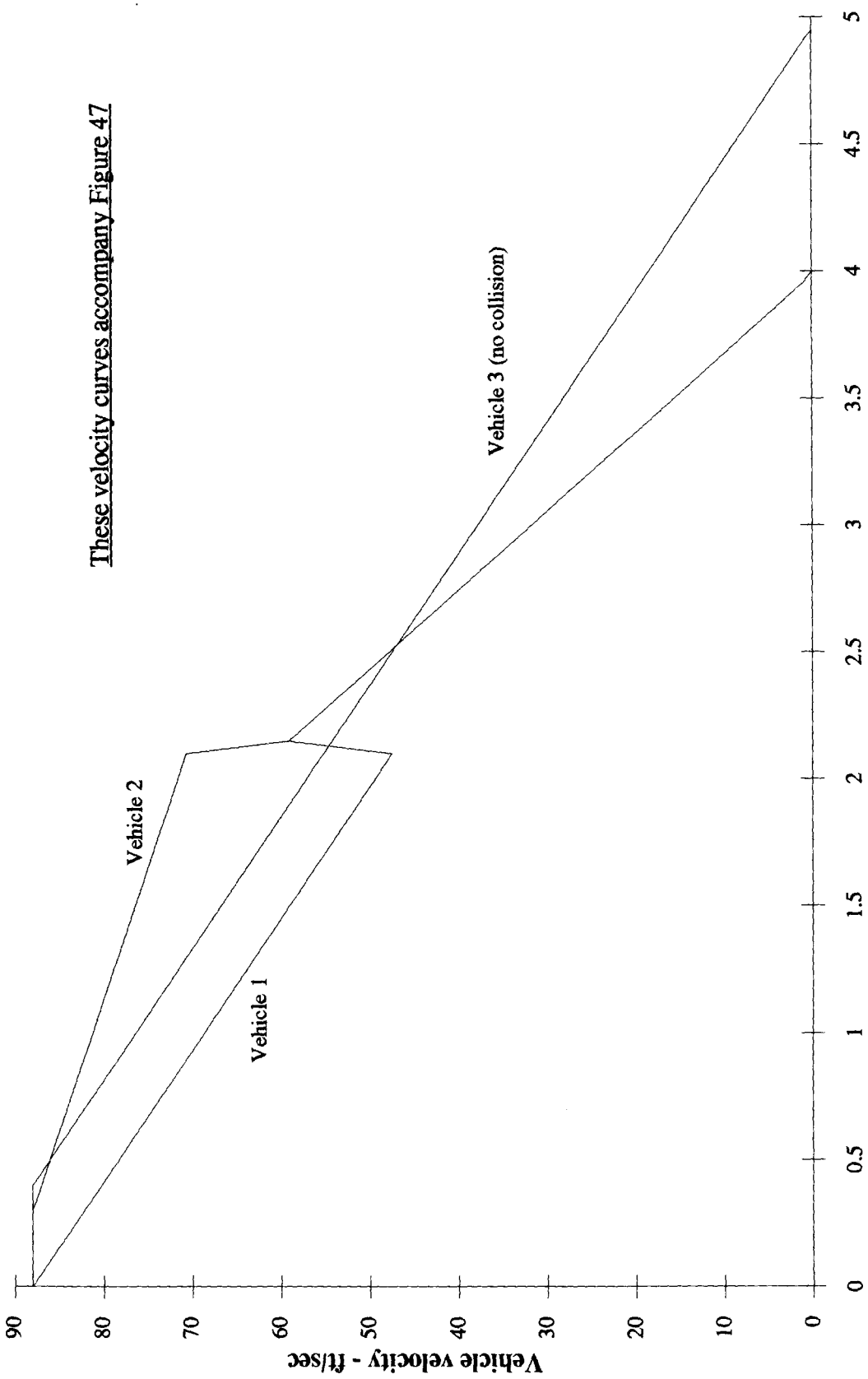


Figure 48. Vehicle velocity curves during collision event.

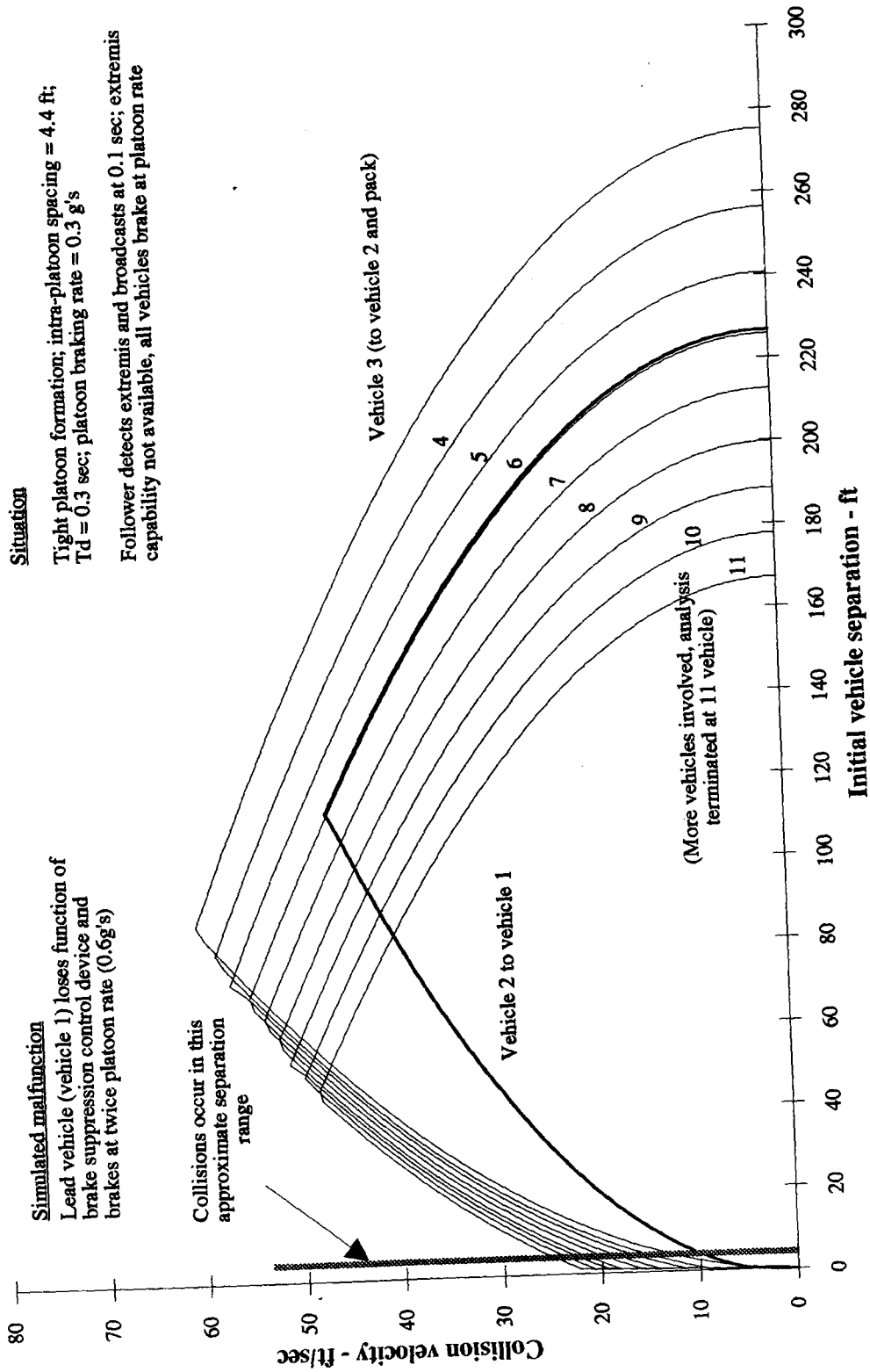


Figure 49. Collision bubbles for simulated malfunction—privileged vehicle brake control failure, tight platoon, no extreme capability.

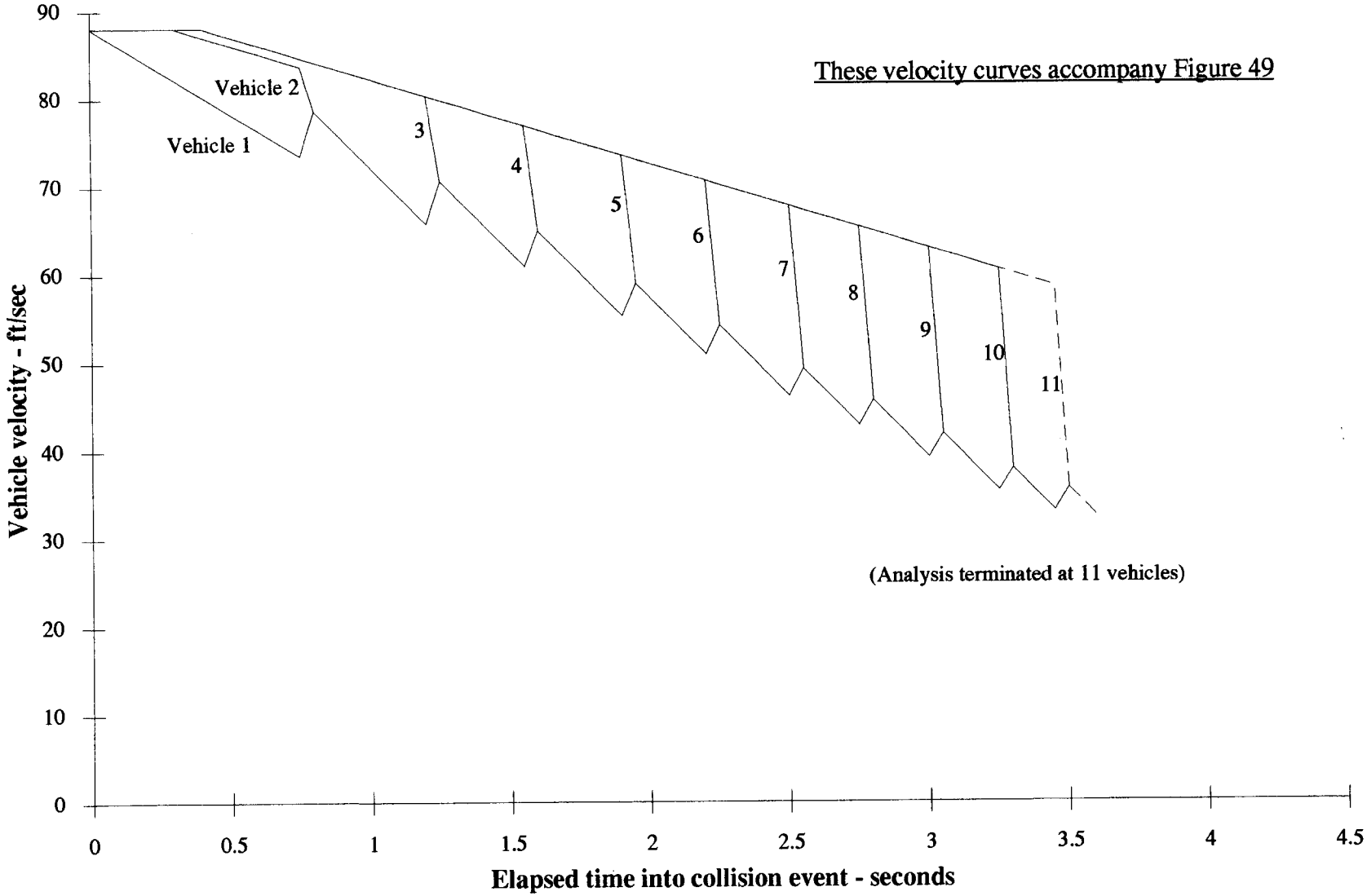


Figure 50. Vehicle velocity curves during collision event.

Situation 4: Loose platoon, brake suppression control failure, extremis braking: This last situation examines a possible means to help alleviate the extensive chain collision exhibited in situation 3. Raising the suppression level to more nearly coincide with the available braking capacity could be used in extremis situations. This capability would remove the low braking rate that was the major contributor of the long chain collision in situation 3. Therefore, with this new capability, when vehicle 2 senses the extremis situation and broadcasts to the rest of the platoon, the platoon constrained braking rate is changed to a higher level, in this example to 0.6 G.

Figure 51 shows the effect of this strategy. There is a considerable improvement over that in situation 3. Figure 52 shows the velocity profiles of the affected vehicles. The collision event only involves 11 vehicles, and the severity for each vehicle is significantly reduced.

Severity Summary

The relative severity of the collision sequences discussed in the previous sections is shown in figure 53. The values depicted are the maximum ΔV of the colliding vehicle.

These results indicate that:

1. A given collision occurring with a small separation operating strategy involves more vehicles than are involved with a larger separation strategy.

2. However, the relatively few vehicles involved with the larger separation strategy are subjected to a more severe collision than their direct counterparts in a small separation system.

3. Subsequent participants in the collision, for small separation systems, see an increasingly severe collision, perhaps exceeding those of the vehicles involved in a larger separation system.

As a generalization, it appears that as we decrease separation, we increase the susceptibility to malfunctions that destroy the validity of an engagement. Furthermore, the more we control the worst case ability of vehicles, a necessary condition to support small separation strategies, the more susceptible we are to malfunctions that alter that ability. The potential collisions resulting from increased worst case maneuvers appear to be significantly more severe than malfunctions influencing decreased stopping capability.

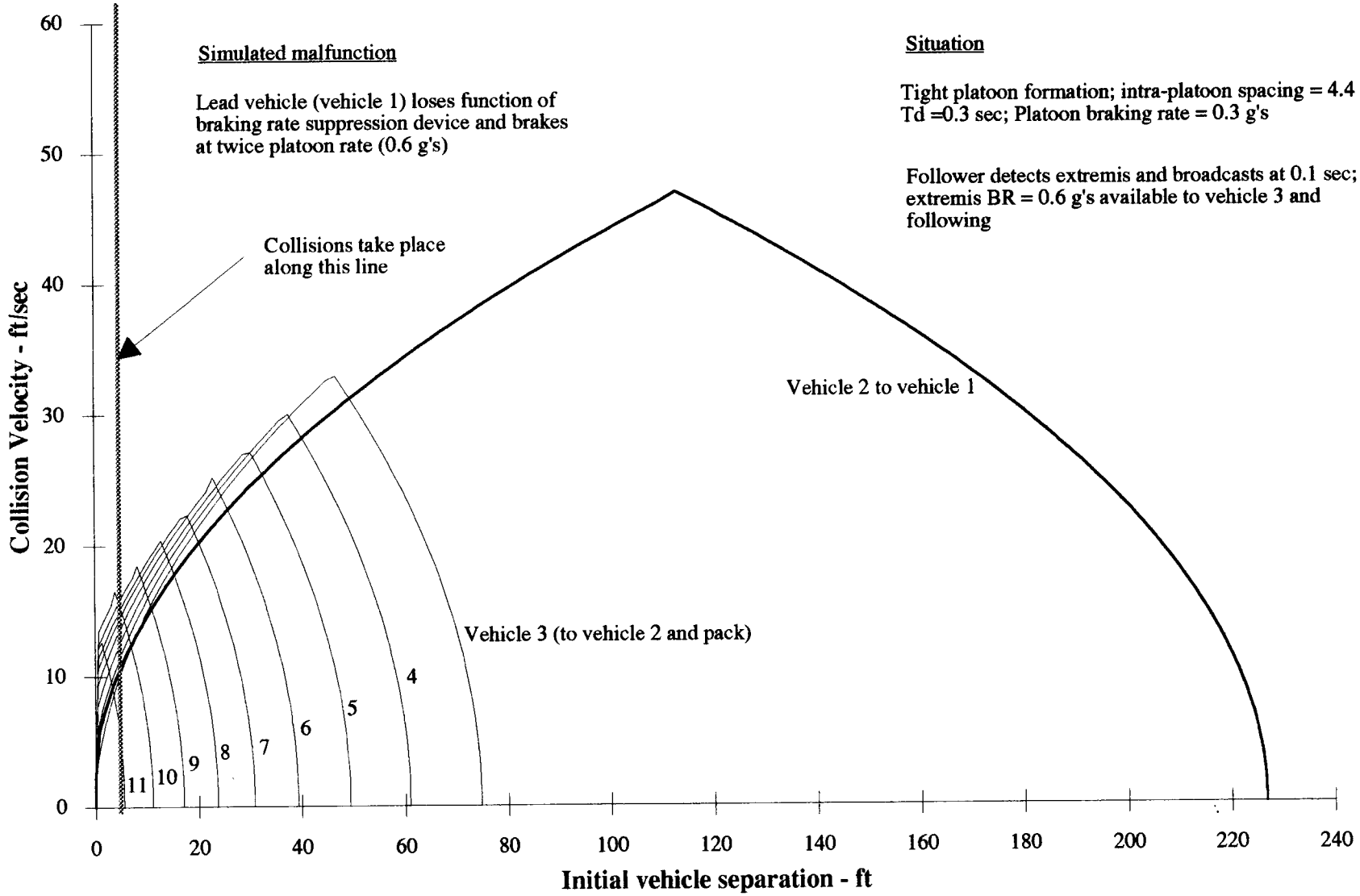


Figure 51. Collision bubbles for simulated malfunction—privileged vehicle brake control failure, tight platoon.

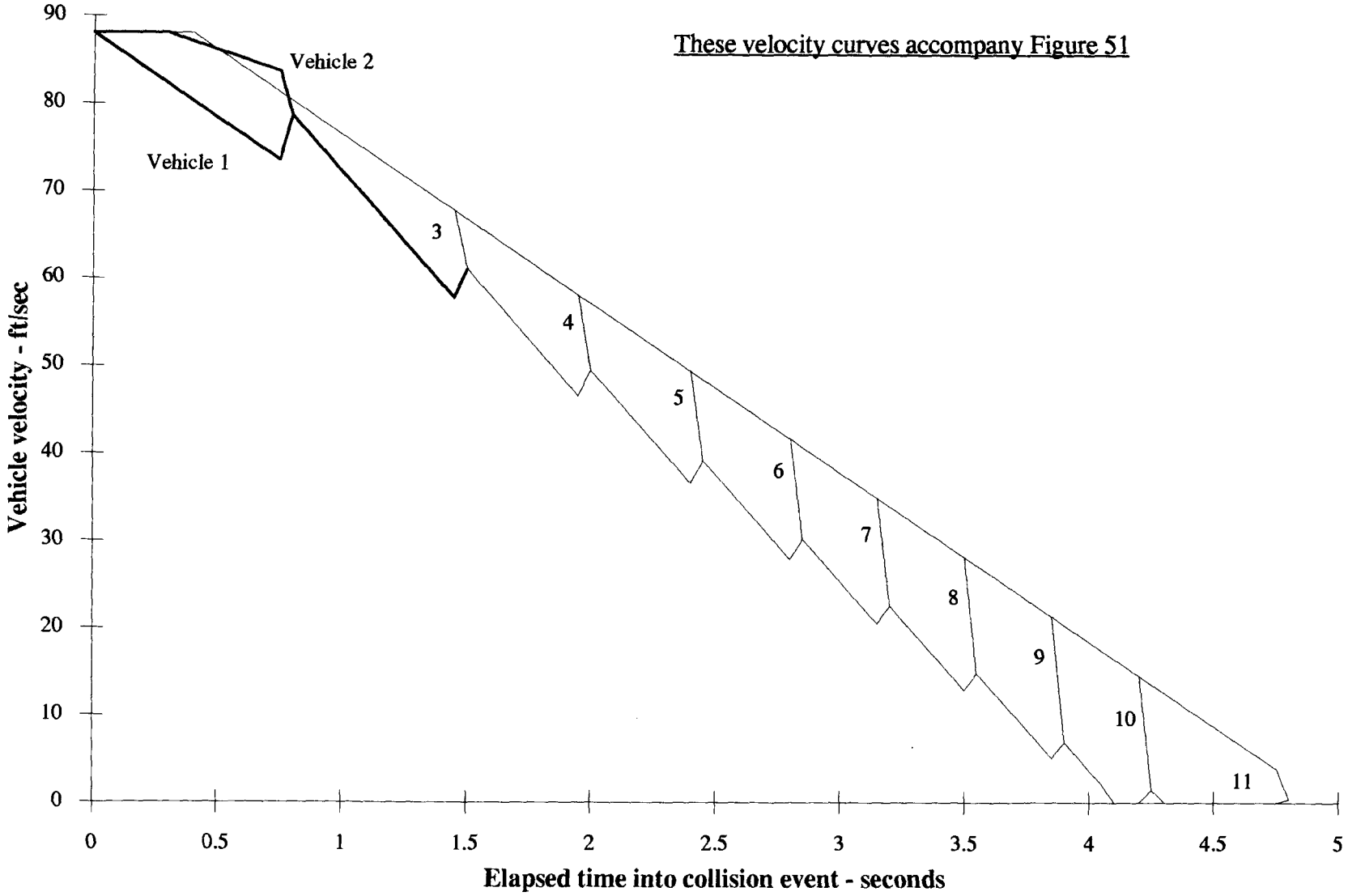


Figure 52. Vehicle velocity curves during collision event.

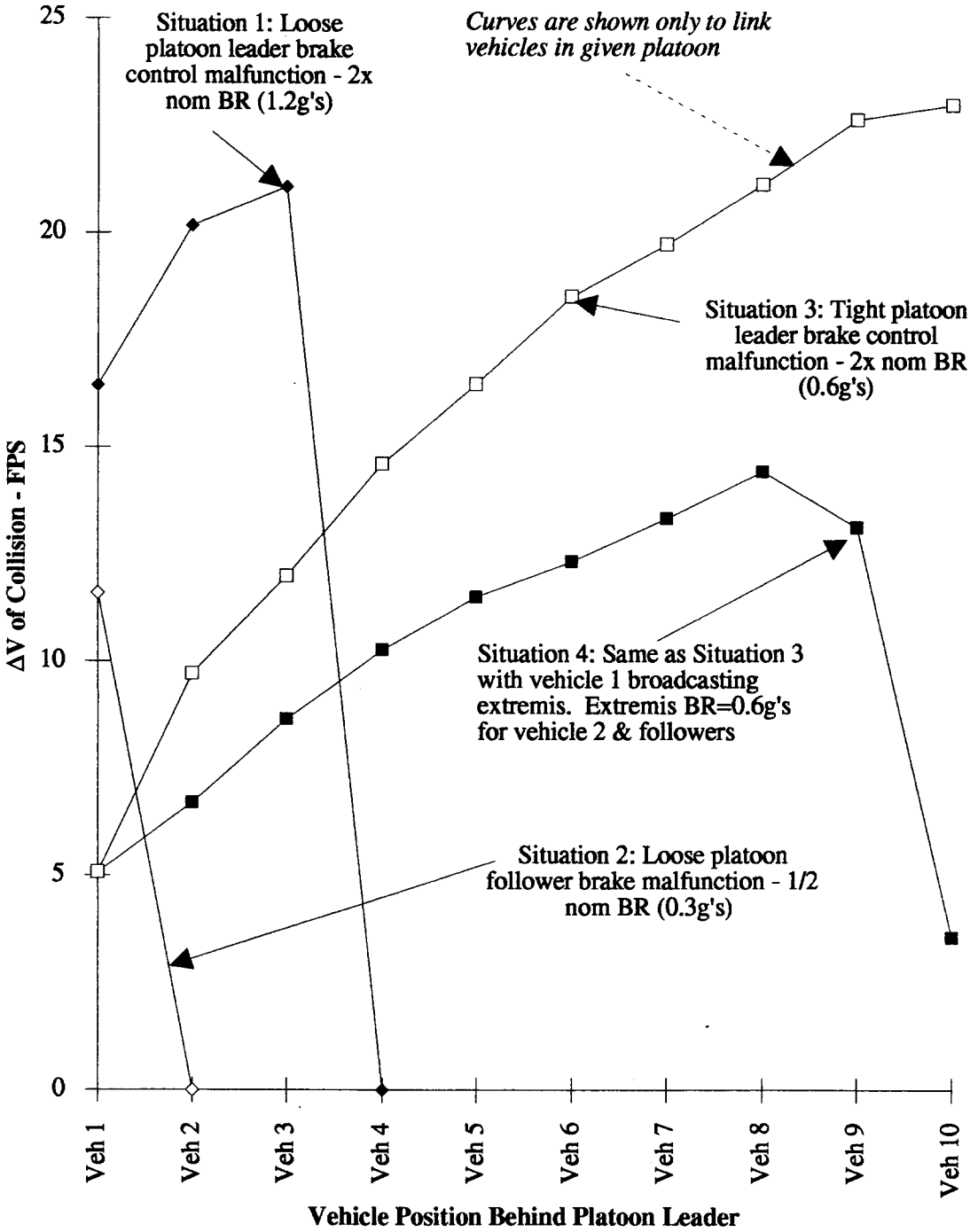


Figure 53. Maximum ΔV for colliding vehicle for selected malfunction studies.

Malfunction Accommodation Implications

To facilitate an intervention to adjust an unsafe separation, the separation manager must have information regarding the health of the engaged vehicle as well as its own health. Therefore, there is a need for sophisticated health monitoring capabilities of the functions critical to the validity of a particular engagement. The intelligence required is an indication that the engaged vehicle is healthy, implying the need for health information sharing. In a fail-safe environment, this implies the need for wellness indicators as part of the "hold close" conditions of an engagement. It is not necessary to know the specific malfunction. Again, from a fail-safe perspective, any unhealthy indicator is reason to suspect an engagement problem.

Because the engagement strategies considered are necessary to accommodate the range of conditions expected for an AHS, most malfunction situations can be safely engaged. In every situation analyzed, the failed vehicle could have been placed in another already existing threat category, with an already existing safe steady-state engagement strategy. For example, a vehicle that loses brake suppression control is the functional equivalent of a rogue vehicle and could be engaged as such without concern for the malfunction. If we knew the new braking limit, it could be engaged under AHS compliant rules. A malfunction in one vehicle in an engaged pair invalidates that engagement, but not necessarily all engagements with that vehicle. If, before a collision, we could back away from the invalid engagement to one that tolerates the failed vehicle as another threat agent, no collision would result.

Ideally, the separation error caused by a malfunction of a vehicle would be corrected by such simple tactics as changing the engagement rule, adjusting separation as necessary to comply with the new rule. However, as was discussed earlier, a malfunctioning vehicle can no longer be considered capable of any engagement with responsibility, it can never be a burdened vehicle. Therefore, knowledge of the malfunction must be communicated to the vehicle now placed in the burdened role. This is the vehicle that must take action. If this vehicle was previously the privileged vehicle in the engagement, we have a rear engagement situation which is problematic. However, this problem is considerably less of a problem than continuing operations under an invalid engagement rule.

A vehicle's separation management capability should accommodate awareness of its potential malfunction exposure, and have appropriate escape plans selected and calibrated to as-is conditions, including any constraints imposed by its dual responsibility. These plans should include options for extremis actions in the event of an imminent collision, as well as an urgent tactic profile to enable the vehicles to separate under more severe conditions than allowed by the current engagement strategy.

"Sudden Intrusion" Fault Intervention

The previous sections examined threat management implications from engaged threat agents; that is, threat agents acquired and engaged under some separation strategy. Such concerns are related to the validity of the initial engagement and engagements that may have been valid, but become invalid—

through inadequate management of intrinsic threats or a malfunction. Another collision potential arises from threats that cannot be engaged through normal strategies. These threats result from the sudden appearance of a threat agent ahead of a vehicle at a distance that is less than that required to allow normal engagement. Included are leading vehicles not engaged at a proper range, rogue vehicles that merge into an AHS lane, AHS vehicles under manual control for merging into the AHS lane, dropped objects, animals crossing the roadway, and accident spillover from adjacent lanes, including vehicles, objects, or vapor threats.

Figure 54 is a high level fault-tree representation of the paths leading to a sudden intrusion collision. This figure also illustrates the placement of intervention options to counter errors in establishing running separations.

Characterization of Sudden Intrusion Collisions

No specific analyses were conducted to examine the collision implications of this threat. The character of initial collisions with sudden intruders is basically the same as for normal transitions. A sudden intrusion imposes the maximum requirements for effective transition management.

While initial collisions are a concern, a more significant concern is the domino effect they will create. This effect can be very significant and is subject to a degree of control by using extremis intervention. The next section, dealing with transferred threats, contains several analyses illustrating the quantitative aspects of such collision events.

"Sudden Intrusion" Fault Intervention

In general, corrective intervention effectiveness depends on how far away the threat is detected. If it is detected close to the AHS vehicle, the situation may be immediately extremis. If detected further away, an urgent maneuver may be possible to avoid the collision or reduce its severity.

If the threat agent is a moving vehicle, there is a chance of using urgent maneuvers to arrive at an acceptable engagement. If the threat agent is not a moving vehicle, the situation is extremis at the time the agent is detected. In either case, reactive control options are important.

For non-vehicle threat agents, however, most of the avoidance capability must be placed on eliminating the sudden intrusion threat. If the threat is present, collision is likely and focus should be shifted to transferred threat management.

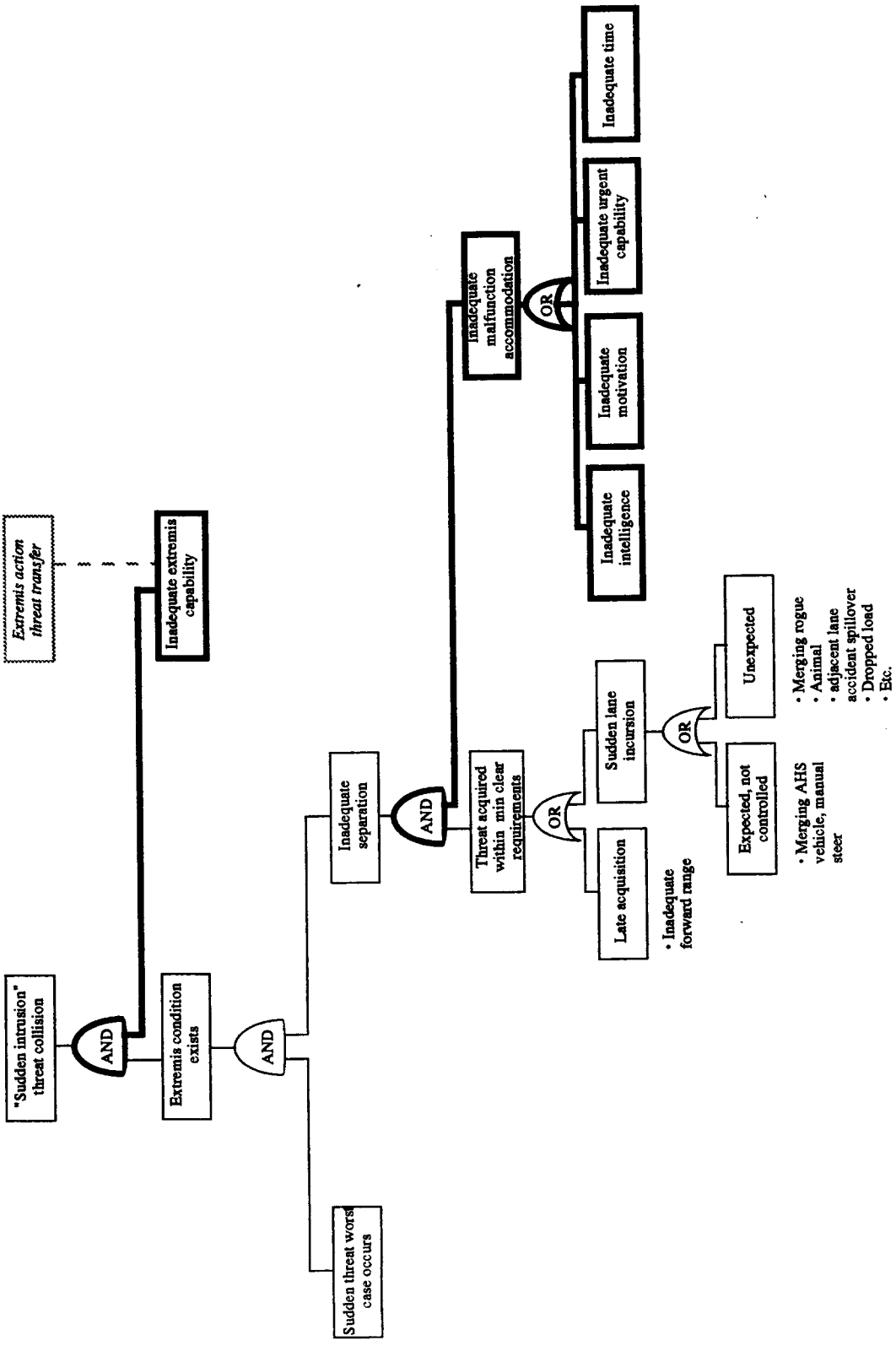


Figure 54. General fault path illustrating sudden intrusion intervention options.

Transferred Threat Fault Intervention Implications

Any engagement between two vehicles involves trust that each vehicle will execute its responsibilities according to the roles they play regarding that engagement. A malfunction, as presented in a previous section, involves the loss of this trust. However, an engagement also involves another trust: trust that each vehicle in the engaged pair will execute their *other* roles adequately. For example, when we close to a few feet to another vehicle, we are trusting that vehicle to not do anything unexpected. We are also trusting that vehicle to maintain adequate and safe relationships with vehicles or objects in front of it. The smaller the separation, the more significant this implied trust becomes. In placing this trust, a burdened vehicle is expanding the role of its engaged privileged vehicle. It is specifically asking it to *not* become involved in a collision.

Figure 55 is a high-level representation of the fault paths leading to a collision involvement of an innocent vehicle, as well as the placement of intervention points. As illustrated, the worst case presentation to an innocent vehicle is a collision involving a leading vehicle, from any cause.

Transferred Threat Collision Characterization

While the malfunction threat intervention discussion focused on malfunction induced collisions involving a pair of engaged vehicles, the analyses clearly extended beyond this boundary and illustrated the influence such collisions may have on vehicles following this pair. These secondary collisions, involving innocent vehicles, occurred simply because these vehicles were in close proximity to the initial collision—a proximity that was established by the AHS operating strategy. This potential for innocent vehicle involvement may well be the most significant influencer of any negative public perception of AHS safety. If for no other reason, this negative perception is sufficient to elevate threat transfer management to a very high priority in the design and operation of an AHS.

The malfunction threat examples illustrated the threat transfer effects of an initial collision between two engaged vehicles as a result of a malfunction in one of these vehicles. Recognizing this provides clues to possible control options to be discussed later. A more difficult situation to control is the effect of sudden intrusions. The nature of the collision transfers resulting from this threat is discussed in the following sections. These analyses examine the susceptibility of platoon engagements to sudden intrusion threats, provide some insight into extremis action influences, and illustrate the effects of some capabilities to provide control before an extremis situation is reached.

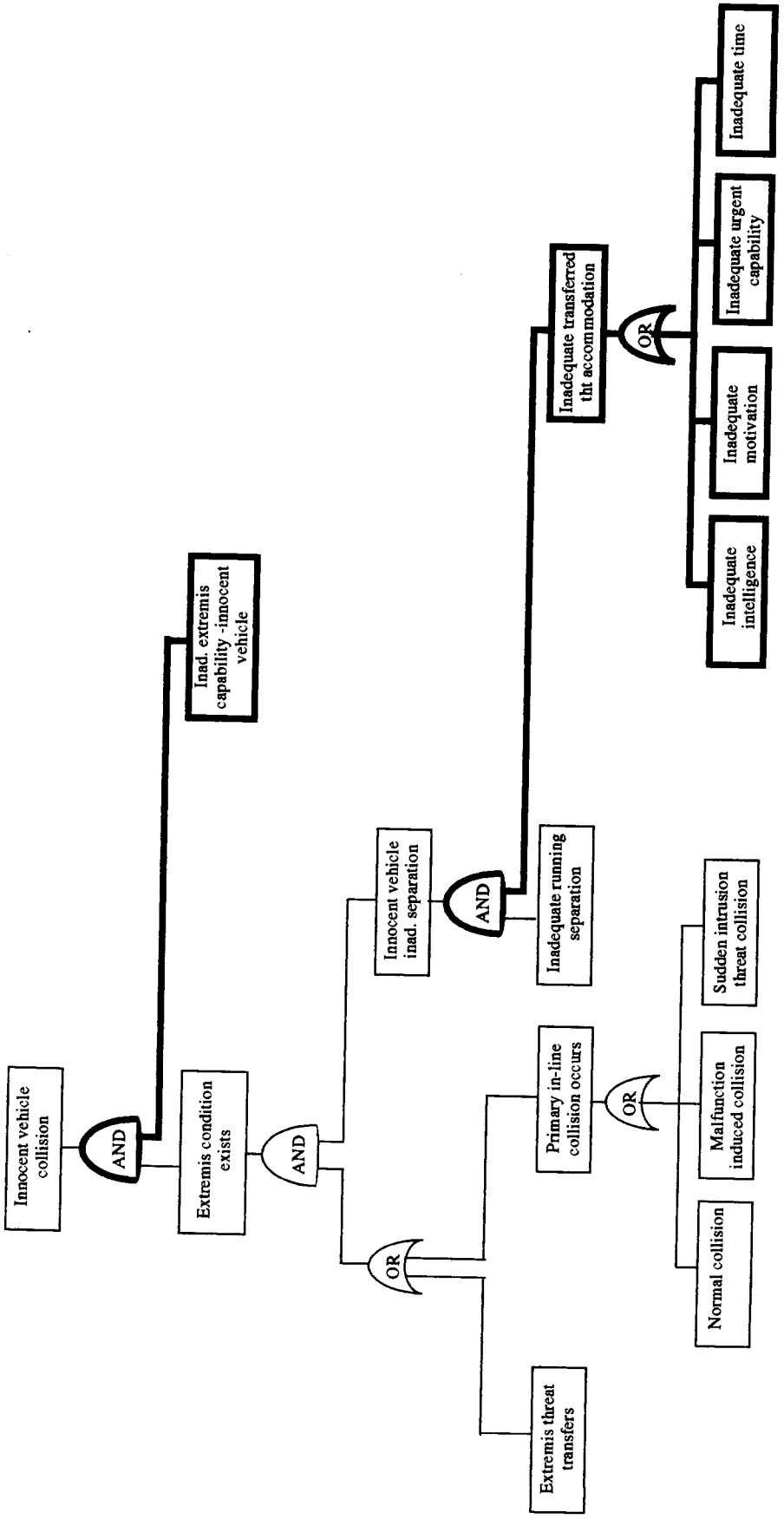


Figure 55. General fault path illustrating threat transfer situation.

The specific analyses presented all deal with the same threat situation, characterized as the intrusion into an AHS lane by a rogue vehicle, at line speed, 30 feet ahead of the platoon leader. Immediately upon entry, this vehicle executes a maximum capable stopping maneuver (1.2 Gs). Line speed for all situations is 60 mph. Six situations are presented. The first two involve a loose platoon engagement and illustrate the influence of extremis broadcast and coordinated braking. The next two repeat these situations for a tight platoon engagement, with the added enhancement of extremis braking capability. The last two address a slight variant of these latter situations.

The analysis procedure used for these situations was the same as that used for malfunction threats; i.e., the same collision characteristics of pack formation and behavior, allowance for vehicle crush, etc. The format for presentation of results also duplicates that of the malfunction threat discussion; i.e., the use of collision bubbles and vehicle velocity profiles to present results.

Situation 1—Loose Platoon, No Coordinated Braking: In this situation, a loose platoon, with an intra-platoon spacing of 26.4 feet and a suppressed braking rate of 0.7 Gs encounters the intruding threat agent. The platoon does not have coordinated braking capability (all delays are additive). Also, because the nominal suppressed braking rate is the lower bound of vehicle capability, it was assumed that no extremis braking capability was available. Figure 56 shows the collision bubbles for the resulting collision event. Figure 57 shows the companion vehicle velocity profiles. As illustrated in these figures, this is a severe collision situation in terms of both number of vehicles involved and the severity of their involvement.

The maximum pre-collision velocity differential shared by the pack and a colliding vehicle occurs when the fifth vehicle collides with the pack. This collision is also the most severe (maximum ΔV) for any colliding vehicle. The analysis was stopped at 12 vehicles; but it can be seen that the collision event is far from over. At least another 10 vehicles would be involved if they were members of the platoon.

Situation 2—Loose Platoon, Coordinated Braking: This situation duplicates situation 1 with the addition of extremis broadcasting to enable coordinated braking. Again, no extremis braking rate was assumed to be available. The algorithm for coordinated braking is the same as that used for malfunction threats: the lead vehicle senses an extremis situation and broadcasts the extremis message to all followers at 0.1 second after it senses the situation. All following vehicles brake in unison with a delay relative to the leader of 0.1 second.

Figures 58 and 59 show the results of this collision event. As can be seen, the results are remarkable. Only the first two vehicles are involved and the severity of the second vehicle collision is reduced compared to situation 1.

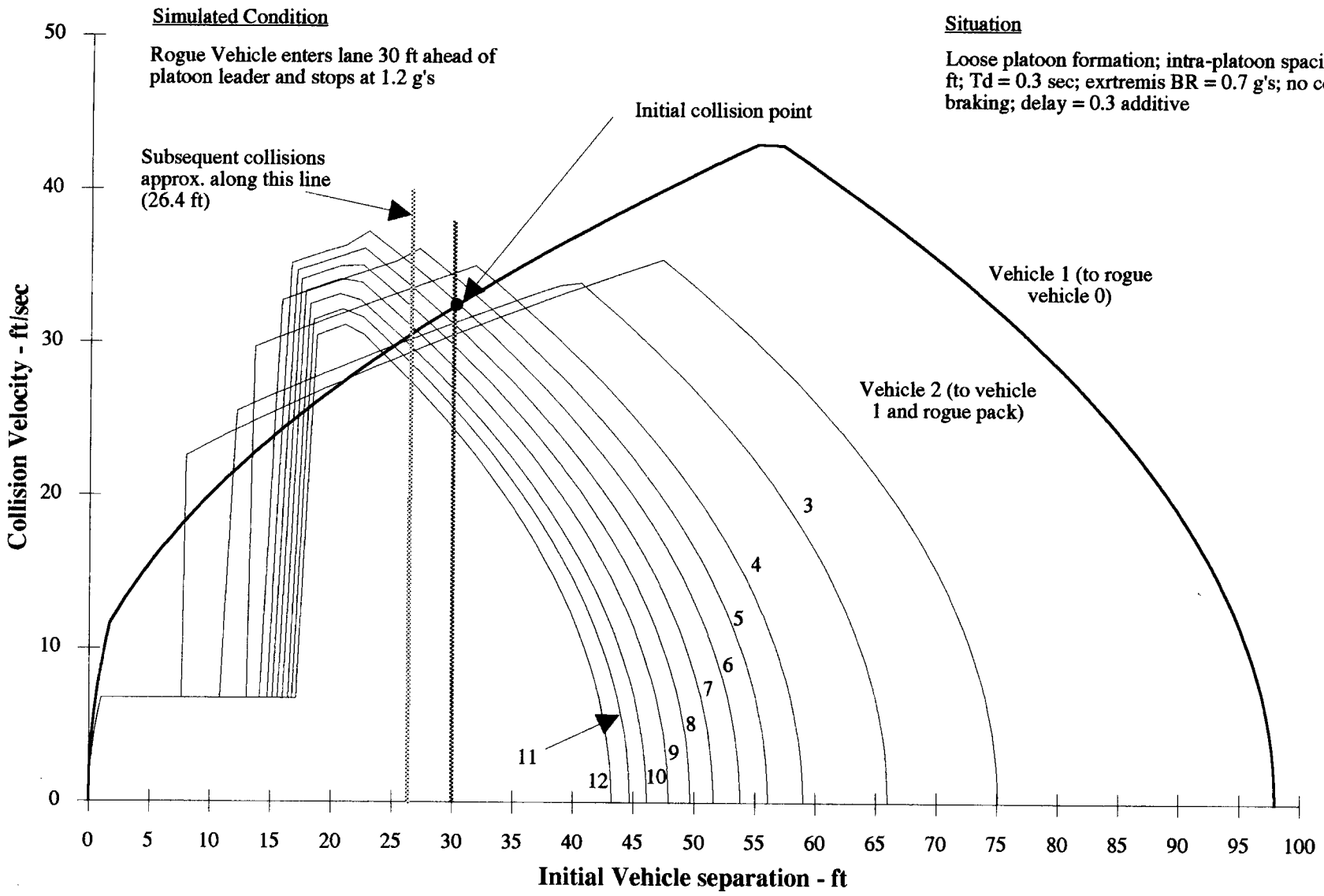


Figure 56. Collision bubbles for simulated threat transfer condition—sudden intrusion, loose platoon, additive delay.

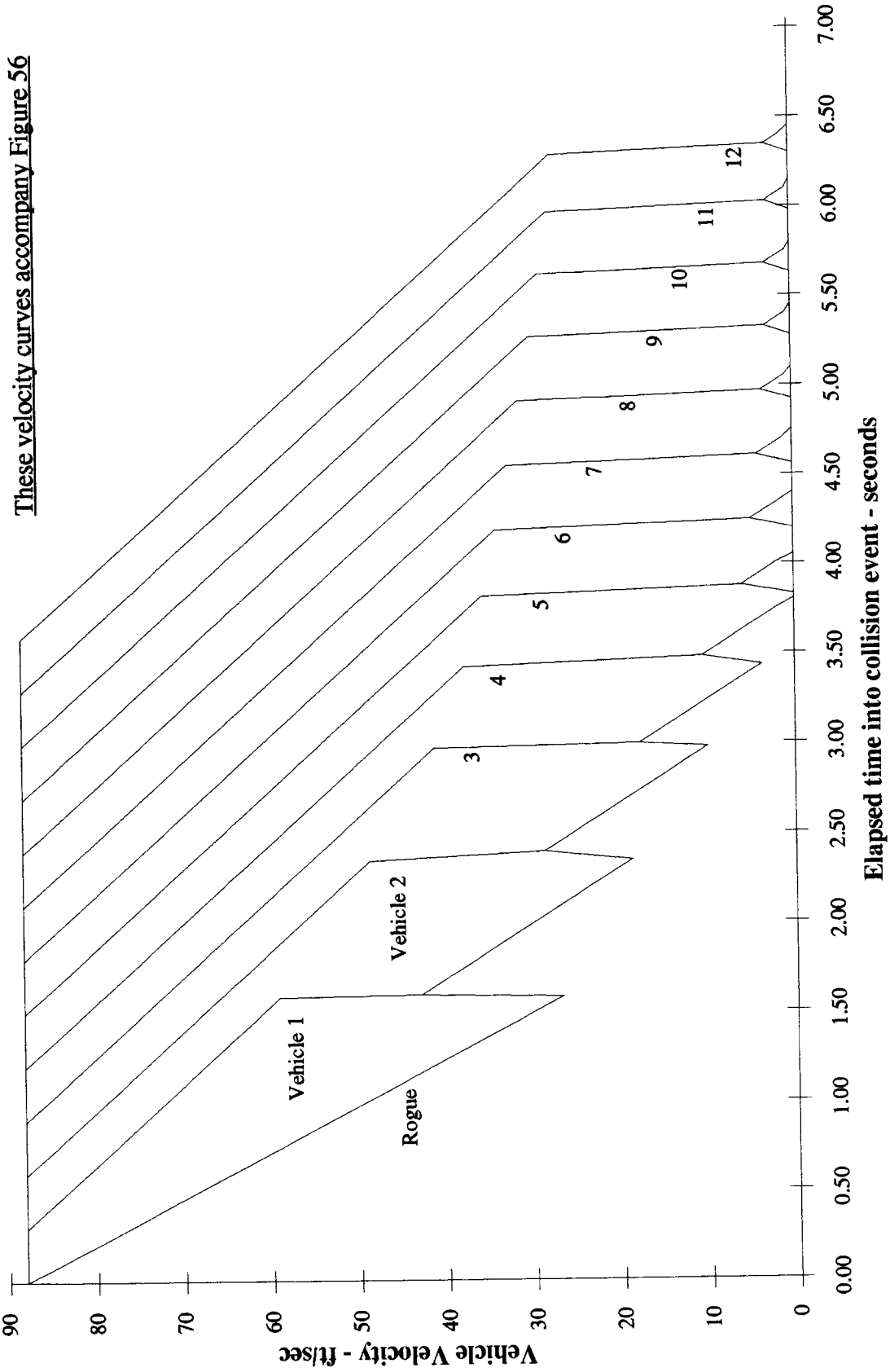


Figure 57. Vehicle velocity curves during collision event.

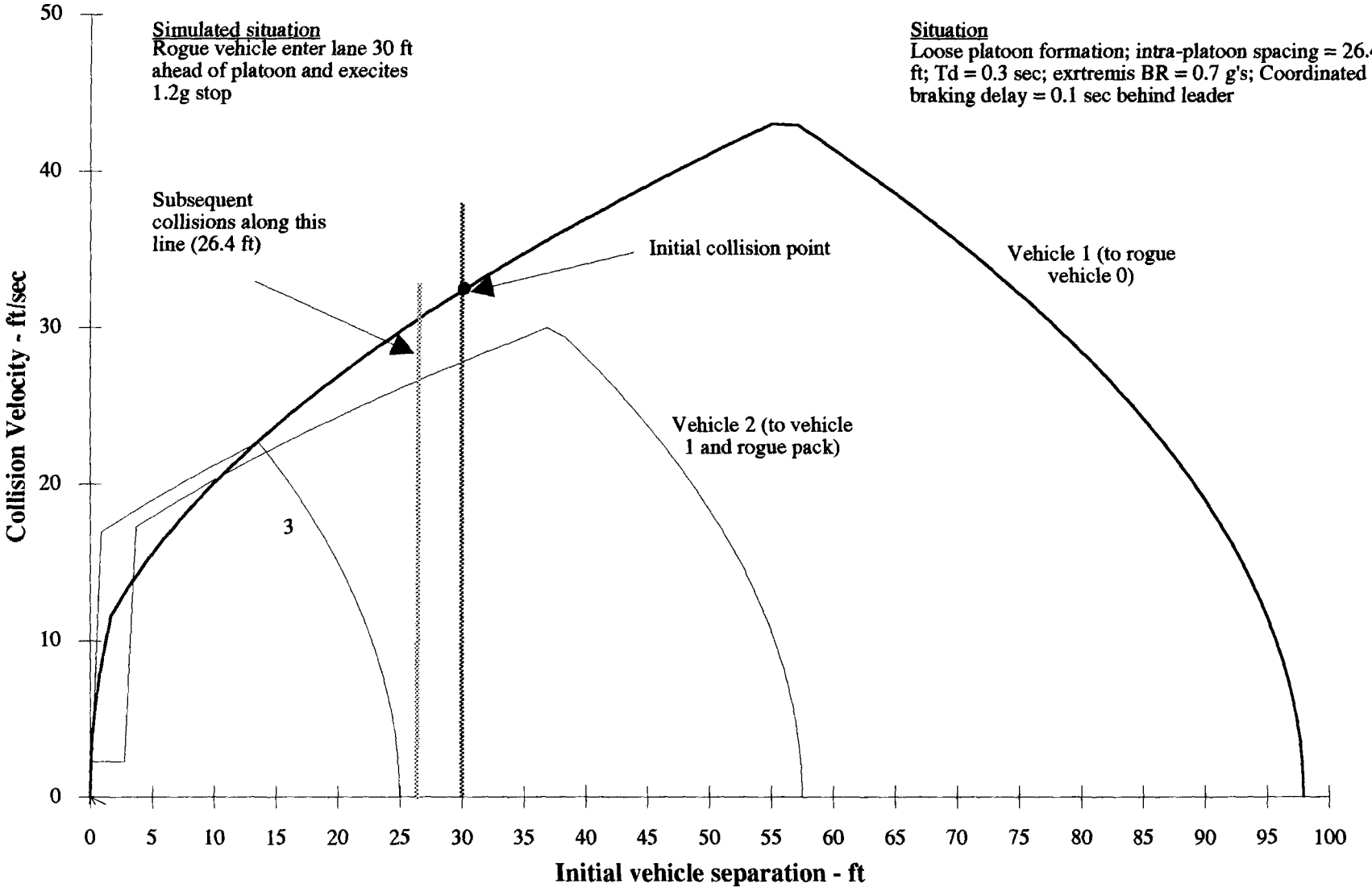


Figure 58. Collision bubbles for simulated threat transfer situation—sudden intrusion, loose platoon.

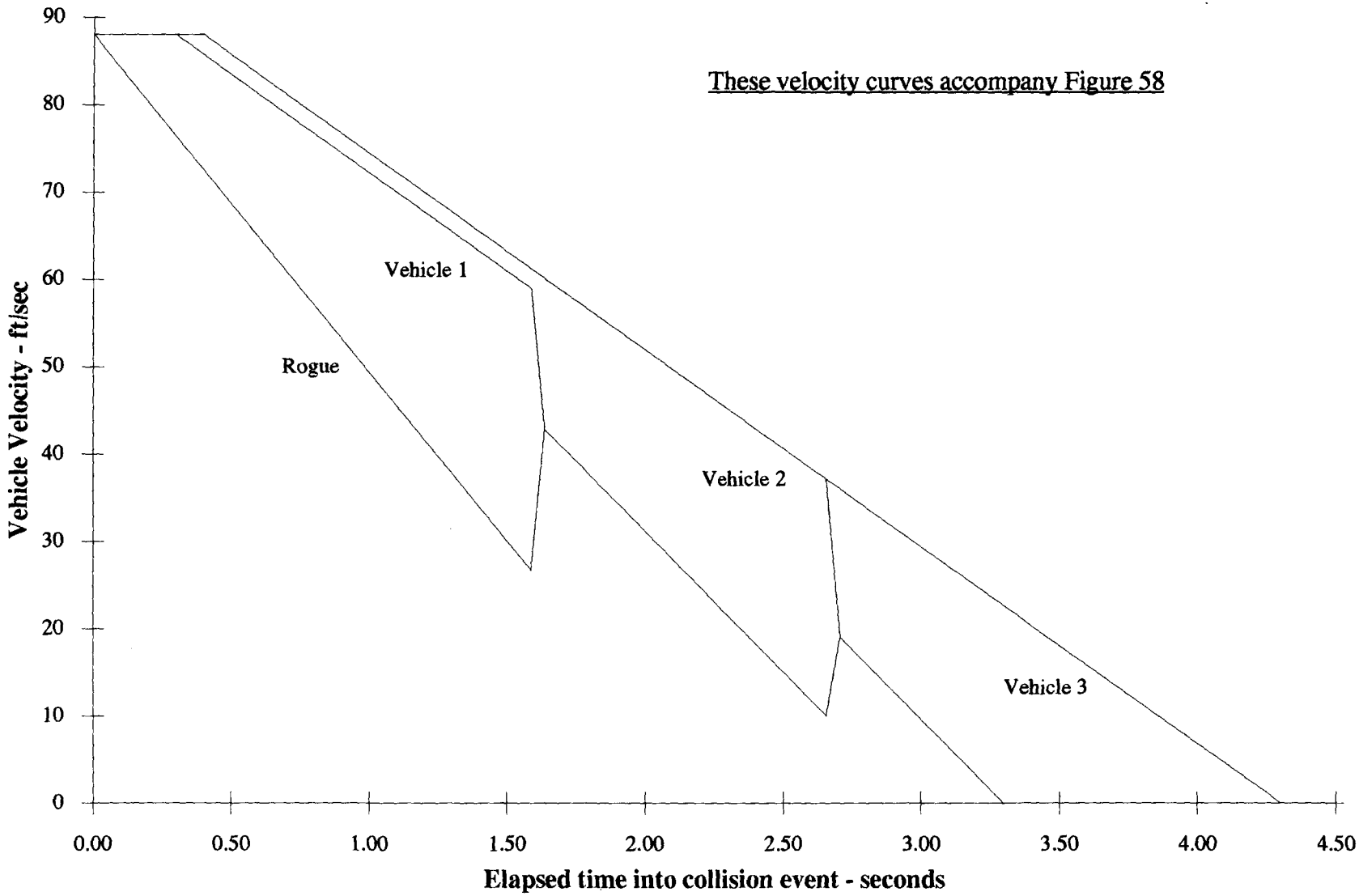


Figure 59. Vehicle velocity curves during collision event.

Situation 3—Tight Platoon, No Coordinated Braking: This situation duplicates situation 1 for a tight platoon, with the added feature of extremis broadcast to permit an extremis braking rate, but not coordinated braking. The nominal intra-platoon spacing is 4.4 feet and the nominal suppressed braking rate of the platoon leader is 0.3 Gs. The extremis braking rate is assumed to be 0.7 Gs. Figures 60 and 61 illustrate the results of this collision event. As can be seen, this is a very severe situation. The severity of each collision increases for each collision and the number of vehicles involved far exceeds the number used in these analyses. It is reasonable to expect that, unless platoon length were limited, a colliding vehicle could reach the maximum theoretical limit of severity, experiencing a ΔV approaching line velocity.

There is an anomaly that exists in this situation. The first three vehicles experience a collision with each other before the intruder is contacted. (This illustrates the influence of extremis actions as threat transfer agents). The effect of these initial collisions is to create a large mass pack under low ΔV conditions. When this pack collides with the intruder, the intruder absorbs a greater share of the collision ΔV. The result is a lower severity on the first three vehicle than they experience under coordinated braking, illustrated in the next situation. However, vehicles after these three suffer greater severity than those under coordinated braking. Inferences that can be drawn from this observation are discussed under transfer threat intervention.

Situation 4—Tight Platoon, Coordinated Braking: This situation duplicates situation 3, with the addition of an extremis braking capability of 0.7 Gs. Figures 62 and 63 illustrate the resulting collision event. As was observed for loose platoons, the influence of coordinated braking is significant. Not only is the number of vehicles involved reduced from situation 3, but the severity is also reduced—with the exception of the first three vehicles, as discussed in the previous section.

Situation 5—Tight Platoon, Leader Vision Failure: In this variant of situation 4, the leader fails to "see" the intruder and continues at full line velocity to collision. The second vehicle infers extremis from this initial collision and broadcasts to enable coordinated braking at the extremis rate. Figures 64 and 65 illustrate the results of this event, which is a more severe collision. Not only is the number of vehicles involved increased from situation 4, but the severity of each collision is consistently higher.

Situation 6—Tight Platoon, Leader Vision Failure, Look-ahead Option: This situation duplicates situation 5 with the added capability for the second vehicle to "look ahead" and see the intruder and act accordingly. This vehicle, independent of the leader vehicle actions, determines the extremis situation and is the source of an extremis broadcast, enabling all of its followers to brake in unison at the extremis rate. An additional enhancement used in this situation was that all vehicles act in unison with the second vehicle.

Figures 66 and 67 illustrate the results of this collision, which are very significant. However, compared to other tight platoon situations, this situations results in the minimum number of vehicles involved, as well as a consistently lower severity. This demonstrates the benefits that can accrue with vision capabilities that look ahead of a lead vehicle.

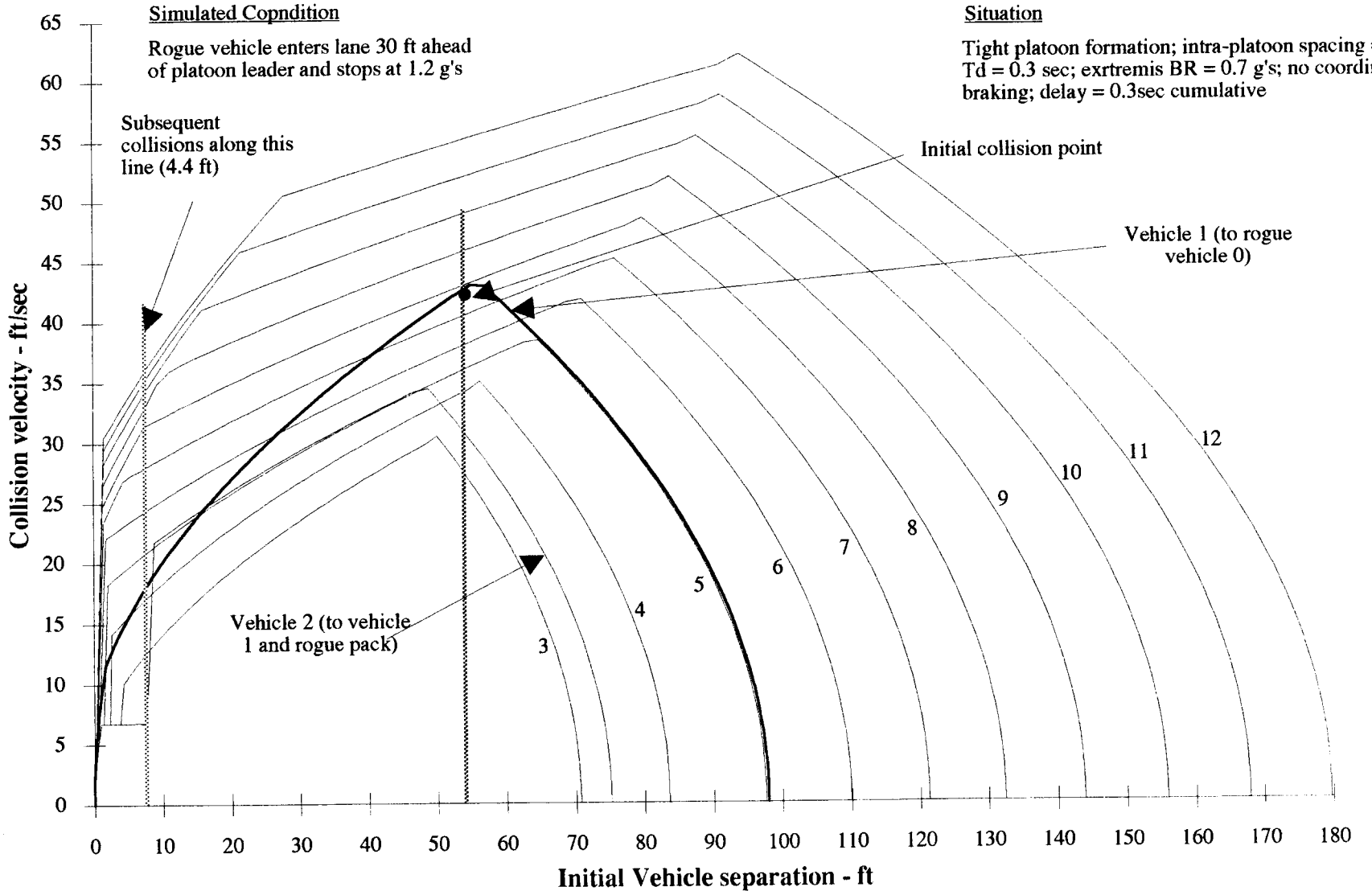


Figure 60. Collision bubbles for simulated threat transfer situation—sudden intrusion, extremis braking, additive delay, tight platoon.

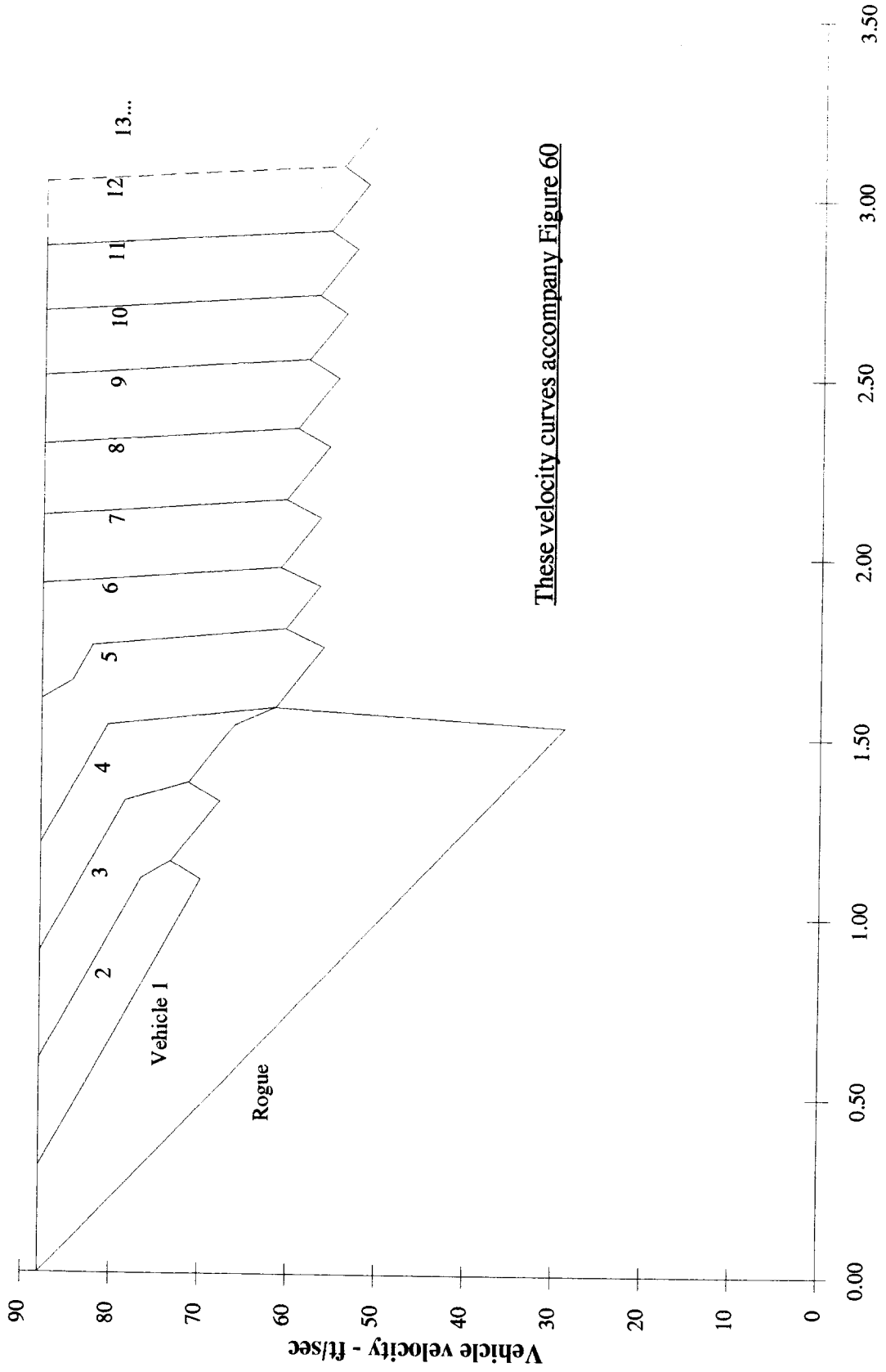


Figure 6.1. Vehicle velocity curves during collision event.

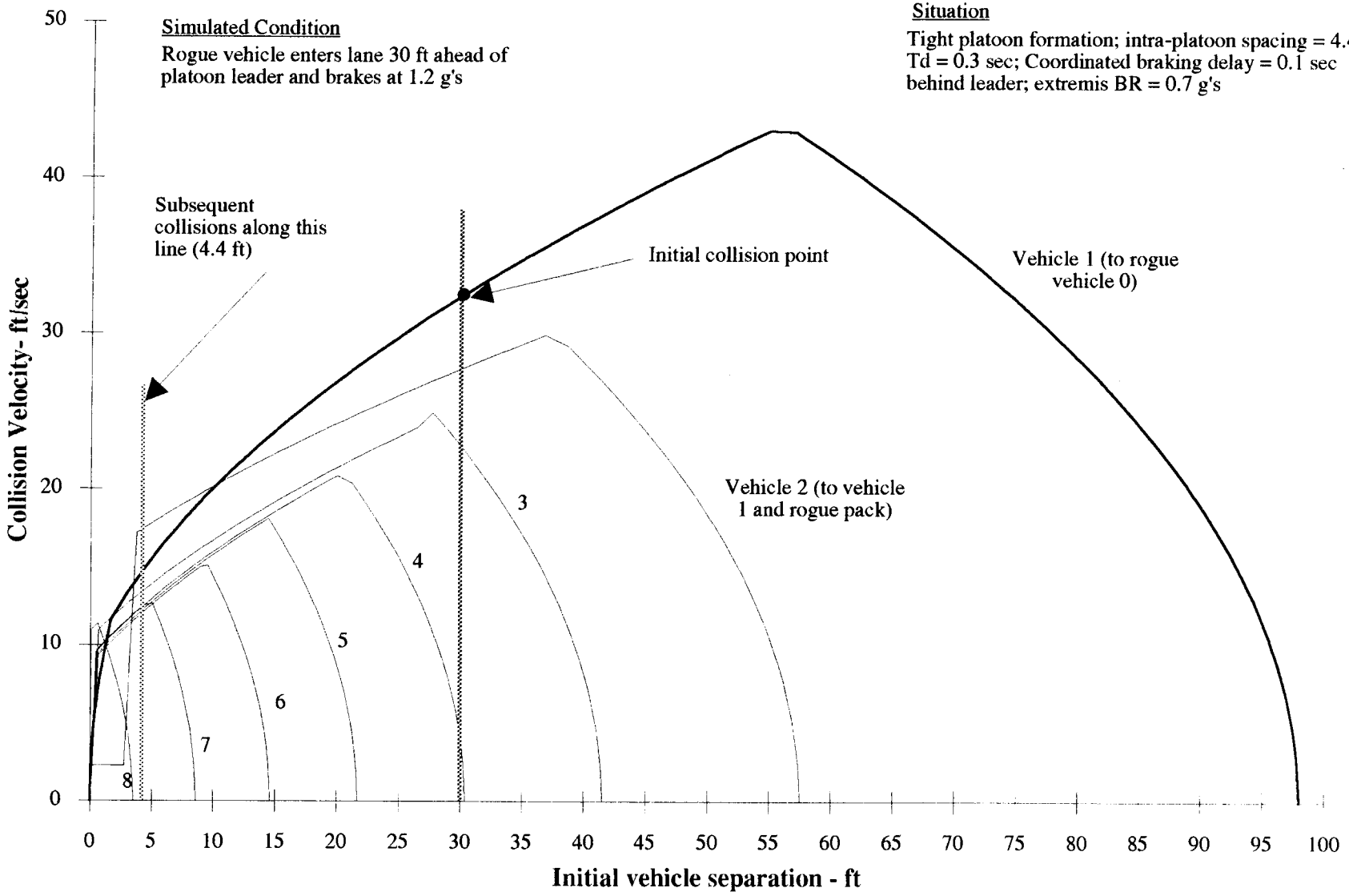


Figure 62. Collision bubbles for simulated threat transfer situation—sudden intrusion, extremis braking, tight platoon.

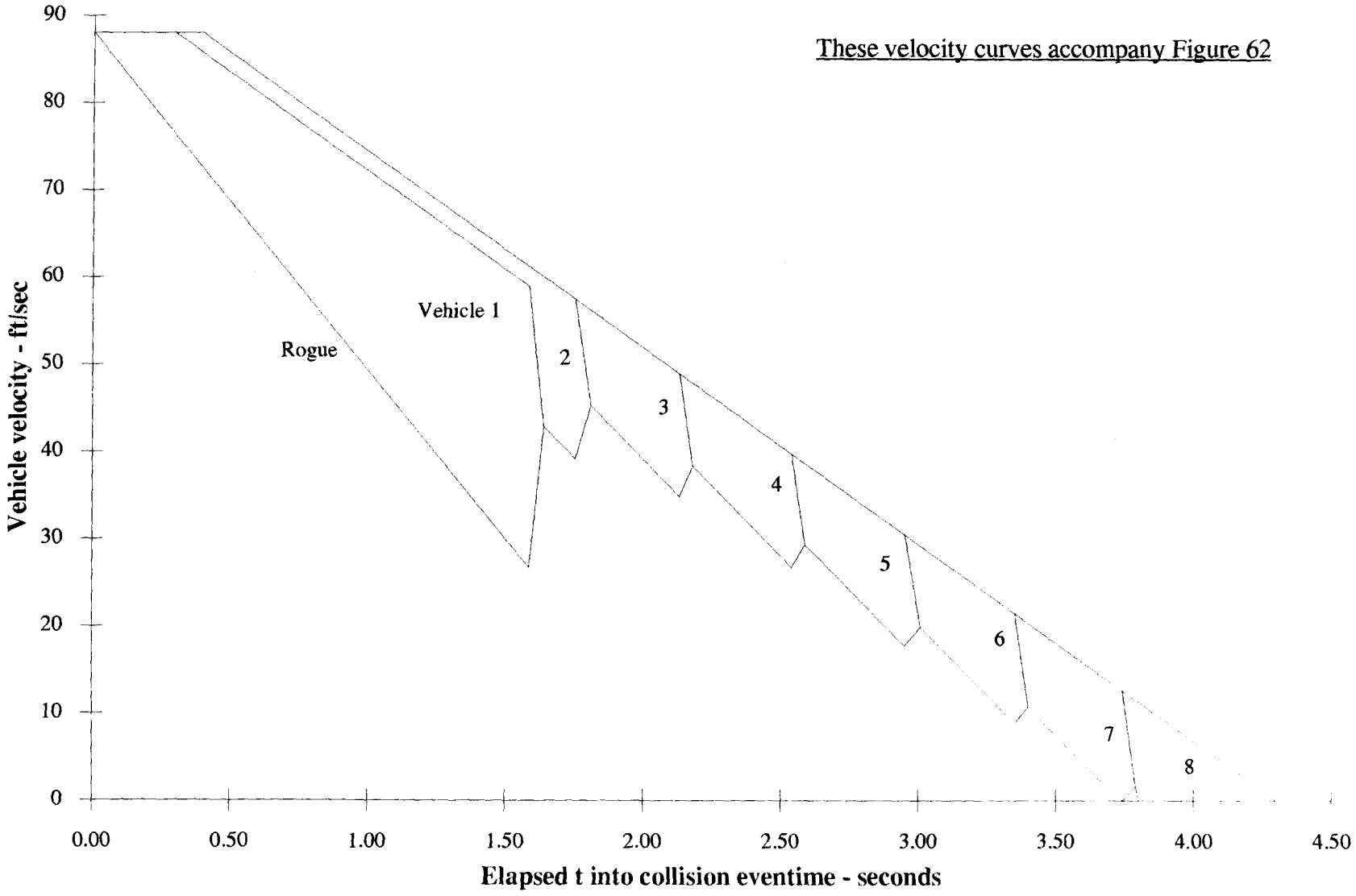


Figure 63. Vehicle velocity curves during collision event.

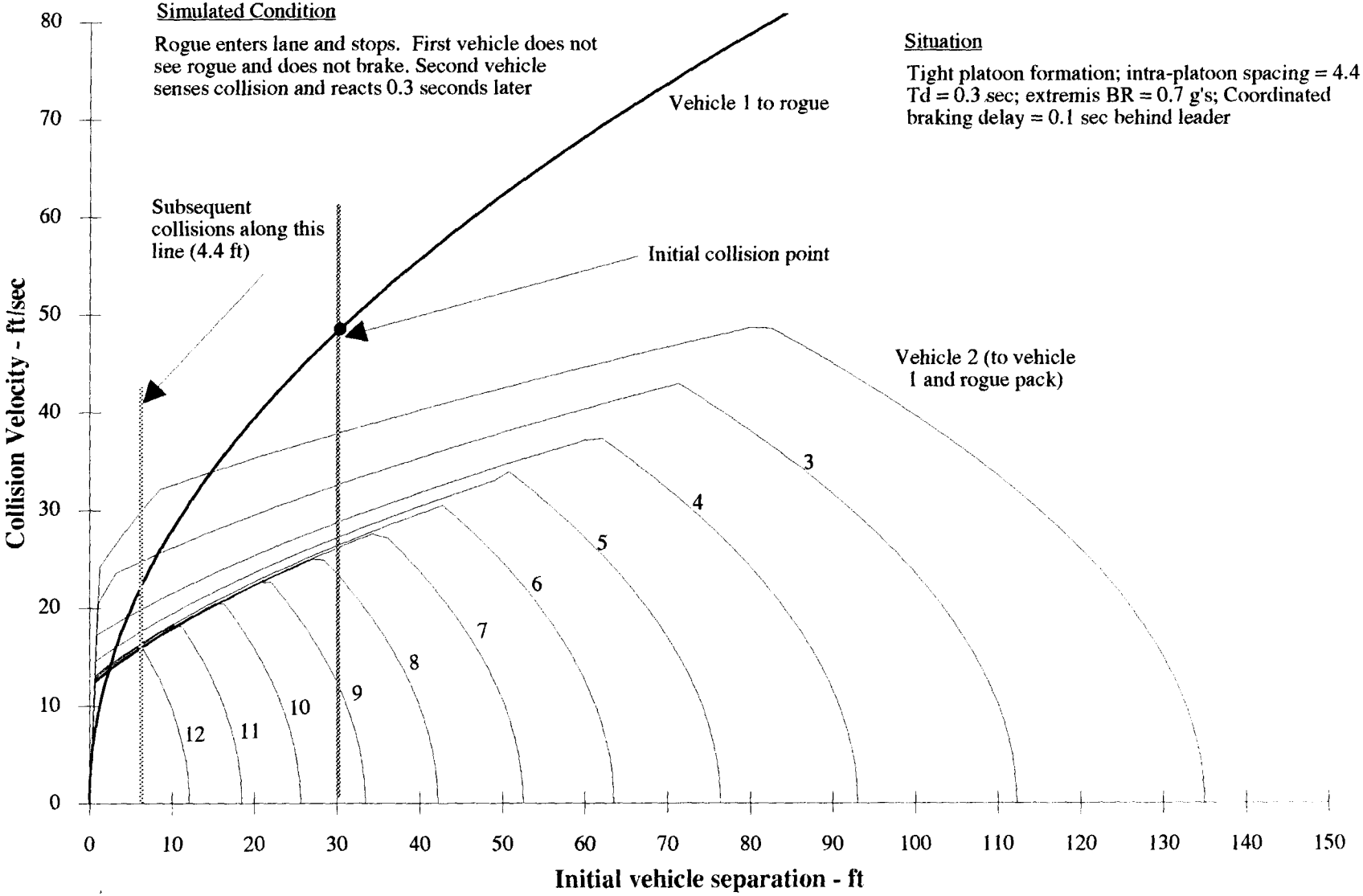


Figure 64. Collision bubbles for simulated threat transfer situation—sudden intrusion, leader fails to detect, extremis braking, tight platoon.

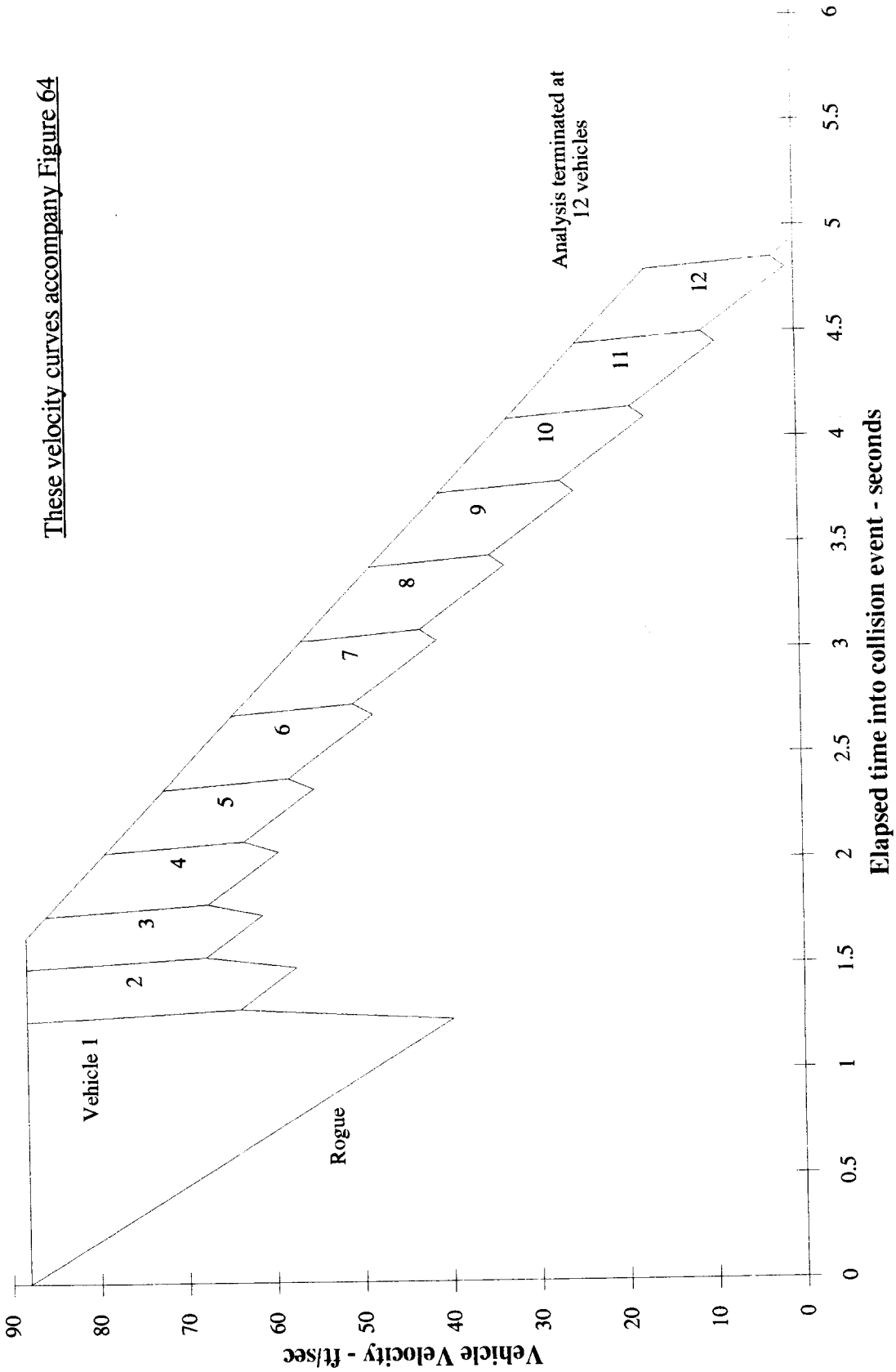


Figure 65. Vehicle velocity curves during collision event.

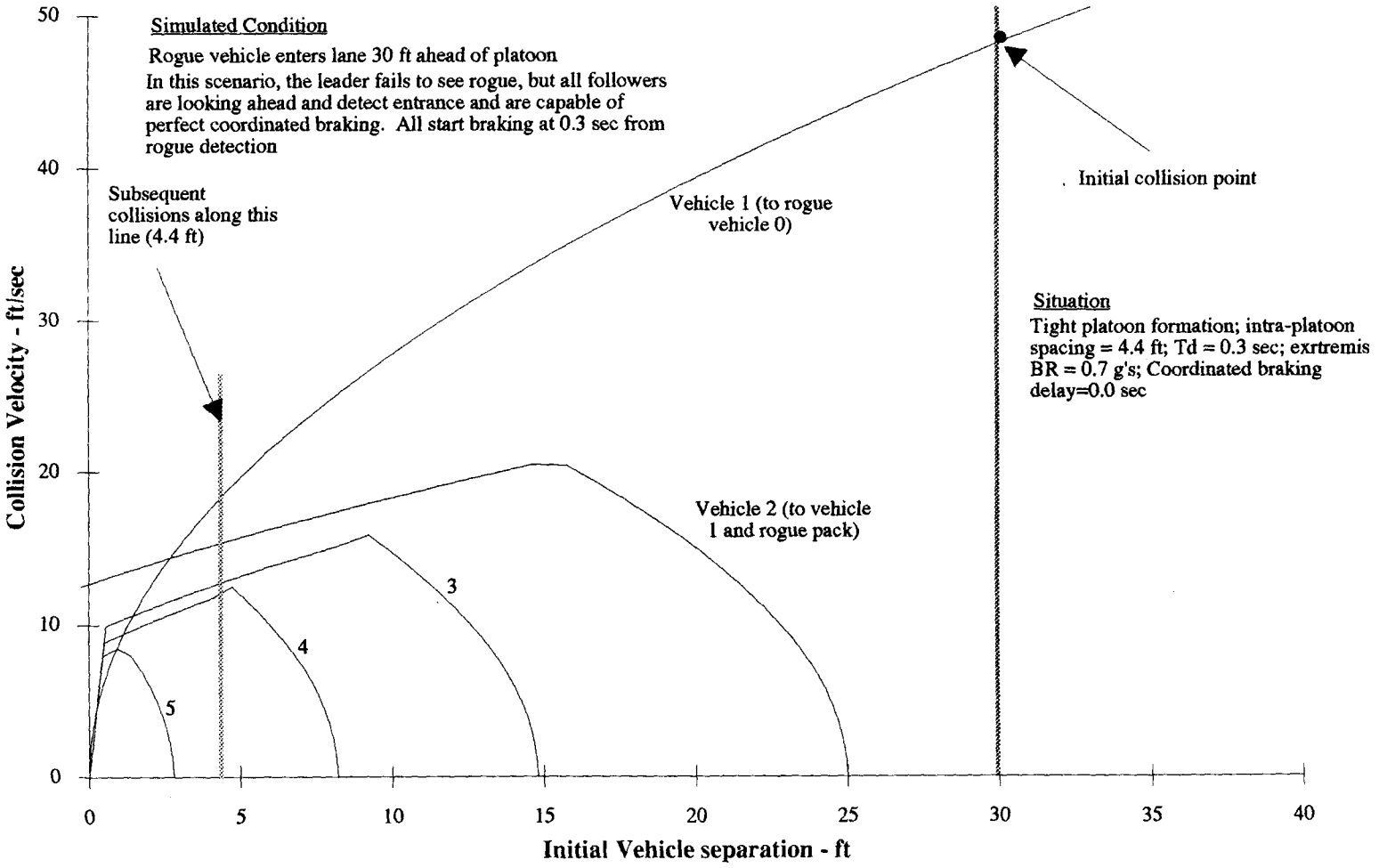


Figure 66. Collision bubbles for simulated threat transfer situation—sudden intrusion, leader fails to detect, followers look ahead, perfect coordinated extremis braking.

These velocity curves accompany Figure 66

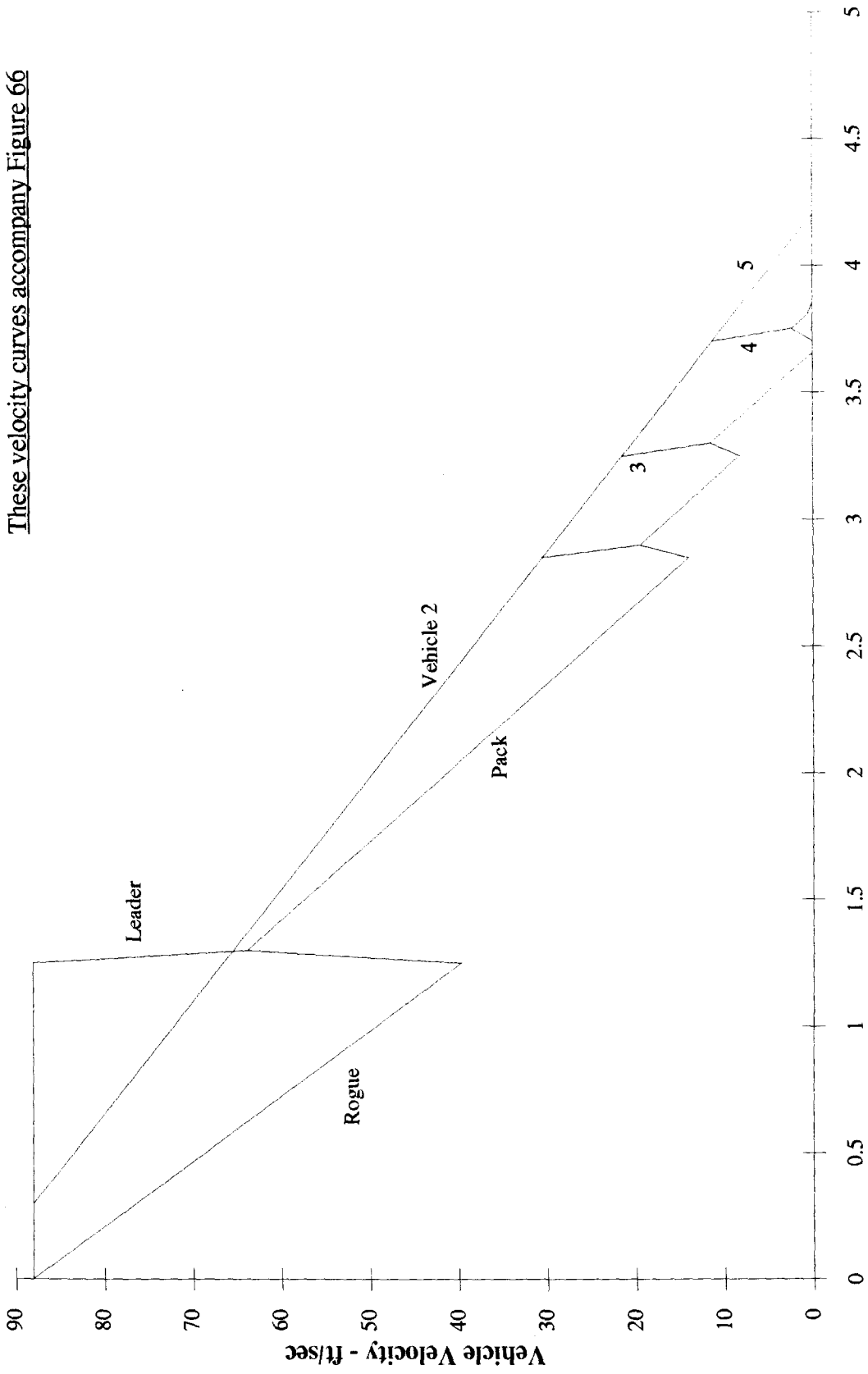


Figure 67. Vehicle velocity curves during collision event.

Severity Summary

The relative severity of the collision situations analyzed above is shown in figure 68. As in the malfunction induced collision, the severity measure is the maximum ΔV endured by the colliding vehicle. These data illustrate the following results, which are totally consistent with the results of the malfunction induced collision investigation:

1. The rather obvious observation that, facing the same threat conditions, a tight platoon will involve more vehicles in the collision event than looser strategies. Again, this points to distance as the most important weapon for collision avoidance.

2. However, the relatively few vehicles involved with the larger separation strategy are subjected to more severe collisions than their direct counterparts in a small separation system.

3. Subsequent participants in the collision, for small separation systems, see increasingly severe collisions, perhaps exceeding those of the vehicles involved in a larger separation system.

Transferred Threat Intervention

These analyses clearly indicate the positive influence of coordinated braking and other extremis intervention actions. In addition, one concept for improving extremis effectiveness was illustrated in situation 6—the capability of a vehicle to "look ahead" of the leading vehicle and recognize that it is in an extremis situation, without receiving its cues from the initial collision.

This concept of early intelligence is also a key ingredient of effective corrective actions. Basically this implies the need for a vehicle to be aware of the situation its engaged privileged vehicle is facing. All corrective intervention options available for influencing a specific threat situation are equally valuable for following vehicles. For example, a vehicle could gain an advantage from knowing the health of the vehicle two positions ahead of it, as this will influence the likelihood that the vehicle immediately ahead will be involved in a collision. Such knowledge could serve to initiate corrective intervention actions to avoid any secondary involvement.

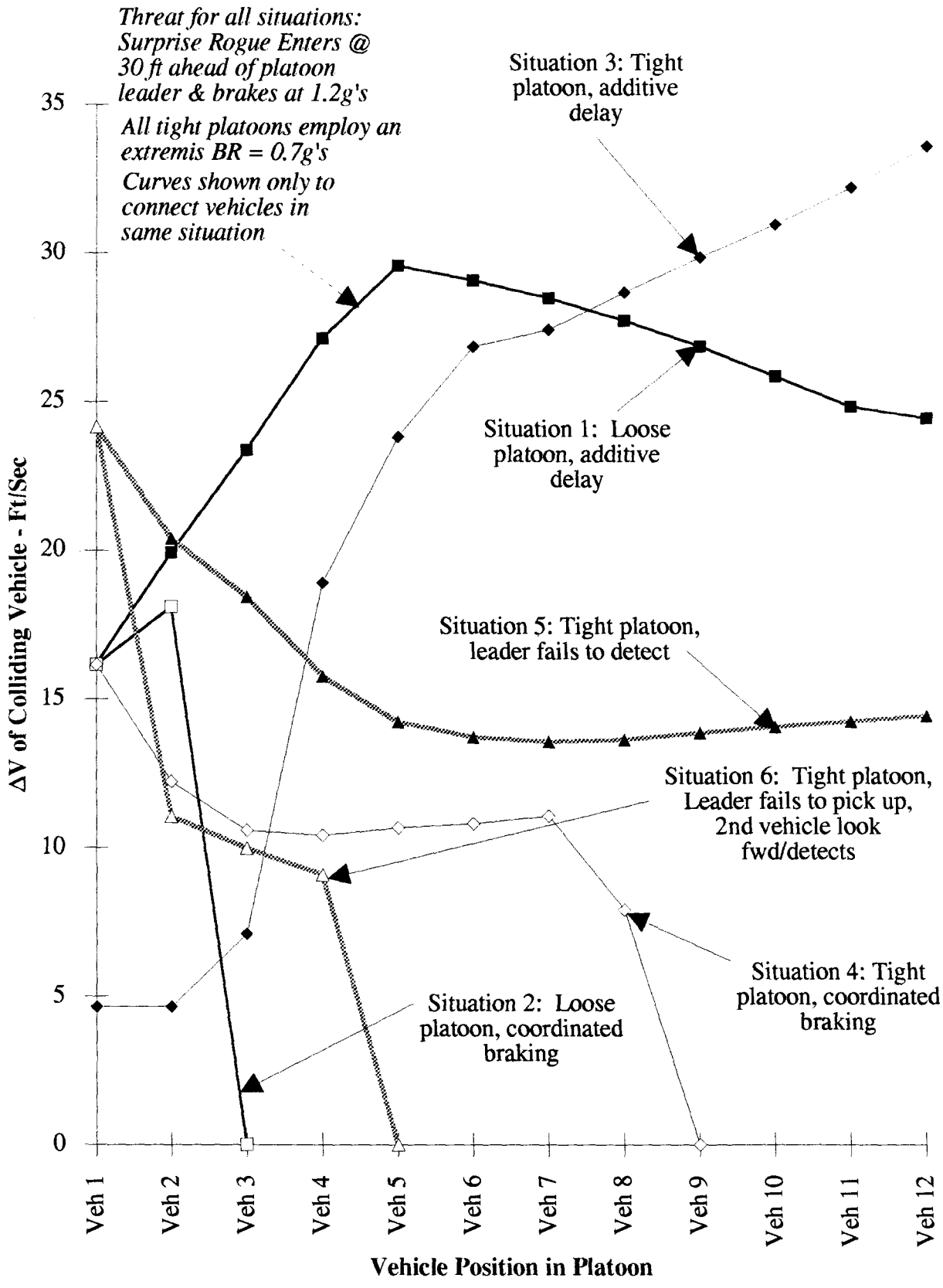


Figure 68. Maximum ΔV for colliding vehicle for selected threat transfer situations.

Similarly, relying on a leading vehicle to safely function as the “eyes” for a following vehicle is not safe. It would be better to see the road ahead of the immediate leading vehicle to verify this trust and initiate corrective action.

Again, adequate corrective and extremis intervention capabilities add to the responsibility of the separation manager. In addition to protecting itself, a vehicle recognizes that its safety is, to a great extent, dependent on the safety of the engaged vehicle. Any intelligence about the latter can be factored into a separation strategy in a timely manner.

SEPARATION MANAGER IMPLICATIONS

The previous sections, together with appendices A and B, collectively present concerns, implications, and requirements for an adequate separation manager function; periodically imputing capability and responsibility to its definition. These implicit and explicit concerns were generally focused on required capabilities to perform a function—knowledge required to determine what constitutes safe separation under many different conditions. Little emphasis was placed on the operational aspects of managing safe separation.

Figure 69 summarizes the separation management problem (this figure is a copy of figure 22 with the addition of ordinate descriptors to reflect the intervention concerns discussed in collision threat intervention strategies). As illustrated, almost every separation management problem increases as vehicle separation decreases. If there was no demand for a high level of roadway lane capacity, the separation manager would have a strong bias to large separations. The demand for capacity, however, is always seeking small separations. If there was no demand for a high level of safety, this capacity manager would have a strong bias toward small values of separation.

These different biases illustrate the classic adversarial relationship between safety demands and capacity demands. Satisfaction of both views requires negotiation. In this negotiation, safety should *never* be the loser. Furthermore, it would be out of character for the safety manager to initiate a move toward operations with smaller separations. It defers to the capacity manager for this motivation. In return, the safety manager reserves the right and the responsibility to establish the conditions under which this operation can be permitted without compromising the standards of safety. In addition to ensuring that vehicles will not be allowed to operate at small separations unless certain conditions exist, this authority is continuing—to force these vehicles to retreat to larger separations if any of the required conditions change. Furthermore, the separation manager reserves the right to seek a more relaxed separation if the demand for capacity is removed.

This simplified representation of tasks defines, in very general terms, *what* must be accomplished by the safety manager; the end result of its efforts. In the sections that follow, we focus on the procedural implications to *do* it.

Throughout this investigation, an image of a concept of operations evolved that provides the functional capabilities necessary to enable the demand for capacity and the demand for safety to coexist. This section adds definition to this image.

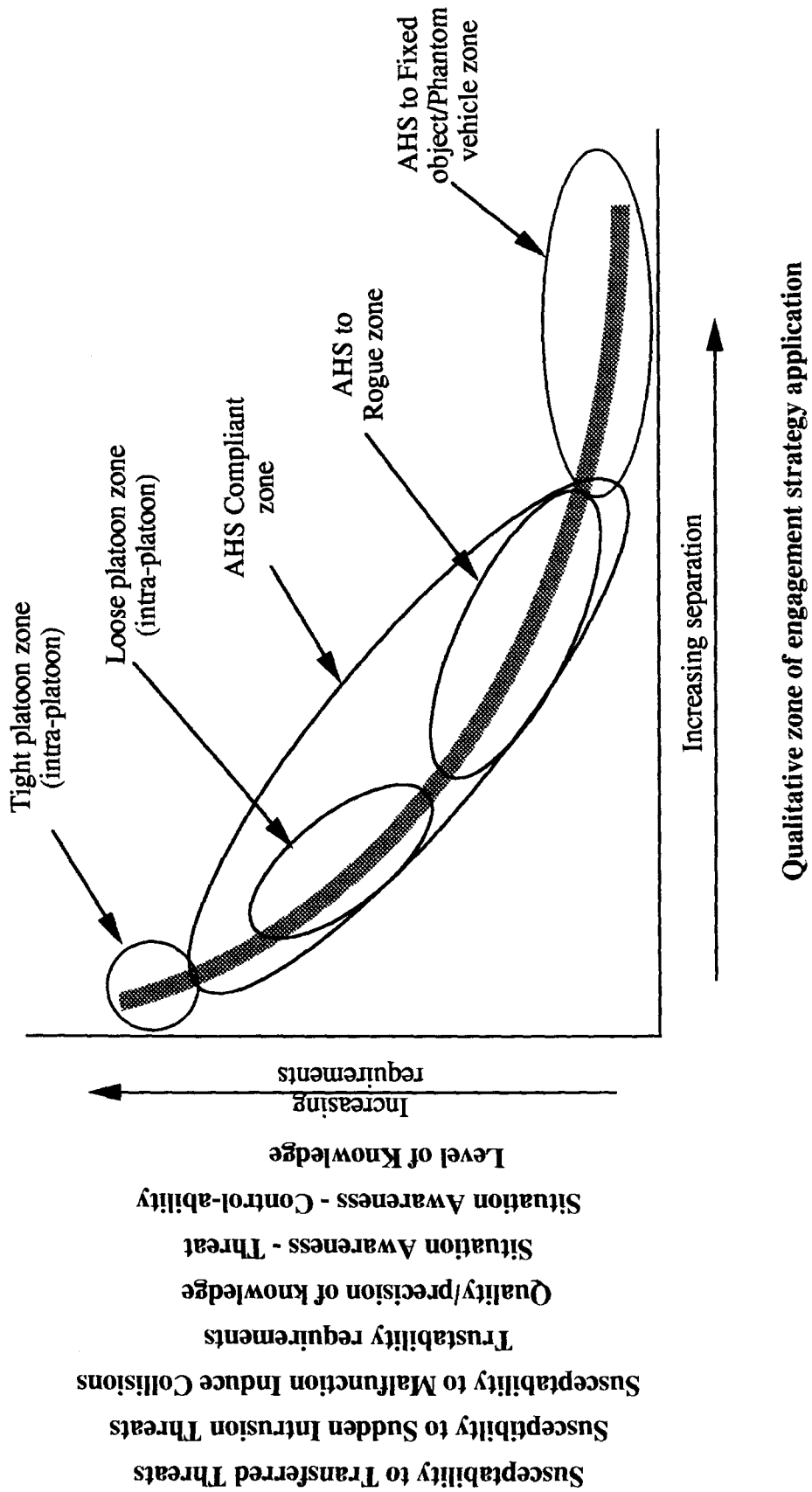


Figure 69. Qualitative relationship between selected engagement strategies and separation control complicating factors.

To formulate the concept, elements were borrowed from other transportation modes, such as:

- Concepts of “fail-safe.”
- Concepts of “authority, agreement, and permission” to coordinate vehicle movements relative to one another.
- Concepts of “privilege” and “burden” to establish relative responsibility for collision avoidance.
- Concepts of “restrictive state” management to lessen the possibility that vehicles will establish engagements that are not safe.

These terms will be defined in their context with AHS operations as they occur. The following section discusses the basis for this operation concept. In the section covering procedural implications the operational concept is developed.

Conceptual Basis

Basic Threat Control Options

The activity area N posture was that all threat agents that may appear on an AHS lane must be addressed by the AHS. This posture reflects system safety analyses that require deliberately treating all possible threats. System safety concepts allow three methods of treatment:

1. Threat engagement: a strategy for maintaining separation between an AHS vehicle and other threat agents on the roadway.
2. Threat exclusion: a strategy for eliminating the need for engagement by controlling access to the AHS lane.
3. Threat acceptance: a considered decision that some threats are simply not reasonably controllable by exclusion or engagement (e.g., the bullet, the 747, and the bowling ball). This option is reserved for very low probability threat situations.

This investigation focused on the first two options: engage or exclude. Unfortunately, the relationship between these is circular:

- If a threat cannot be safely engaged, it must be absolutely excluded; and,
- If a threat cannot be absolutely excluded, it must be safely engaged.

A fail-safe perspective resolves this logic: we assume that exclusion techniques will not be 100 percent effective. Therefore, strategies must be developed to safely engage all threats that approach the boundary of an AHS. This stance does not diminish the desirability and benefits of exclusion; but it does remove the demand for absolute exclusion as a condition of AHS safety.

In addition to this fail-safe consideration, two additional factors influence our position:

1. Even if the exclusion provisions were 100 percent effective, conditions can change on-line, by a malfunction (real or perceived) or other means.

2. Even if the above line changes did not occur, multiple engagement strategies must exist to manage, for example, transition maneuvers or intra-platoon spacing as opposed to inter-platoon spacing.

As a result, five engagement strategies were developed, based primarily on the characteristics of the threat agent to which an AHS vehicle may be exposed. It is the role of the separation manager to apply these strategies as appropriate. To accomplish this, the separation manager uses the same principles of exclusion used for controlling access to the AHS—except in this situation, exclusion is used to control access to engagement strategies. Figure 70 is a schematic diagram illustrating this concept. The top illustrates the exclusion applied at the boundary of an AHS. At the entry to each lower level, all vehicles that do not satisfy the conditions required to safely participate in the engagements at the next lower level are restricted from passing to that level.

This schematic is ordered (top to bottom) to reflect increasing capability requirements. To generalize this concept, each engagement strategy can be thought of as a “restrictive state;” that is, a vehicle is restricted from entering unless it possesses all the capabilities required to participate at that level. The term “restriction” can be considered a restriction on ability to close on another vehicle, or, more generally, on another threat agent. Later in this section, the phrase “seek a more restrictive state” will be used. This means move to an engagement level that is higher in the hierarchy depicted in figure 70. In previous sections of this report, reference was made on several occasions to a capability to move to a safer state. This is tantamount to moving to a more restrictive state.

The Use of “Authority” to Manage Engagements

The separation manager will not allow an engagement between two vehicles unless all the conditions required for this to be safe are fulfilled. If these conditions exist, the separation manager will authorize the maneuver to engage. Authority is the approval to move between restrictive states. This final authority actually has three components:

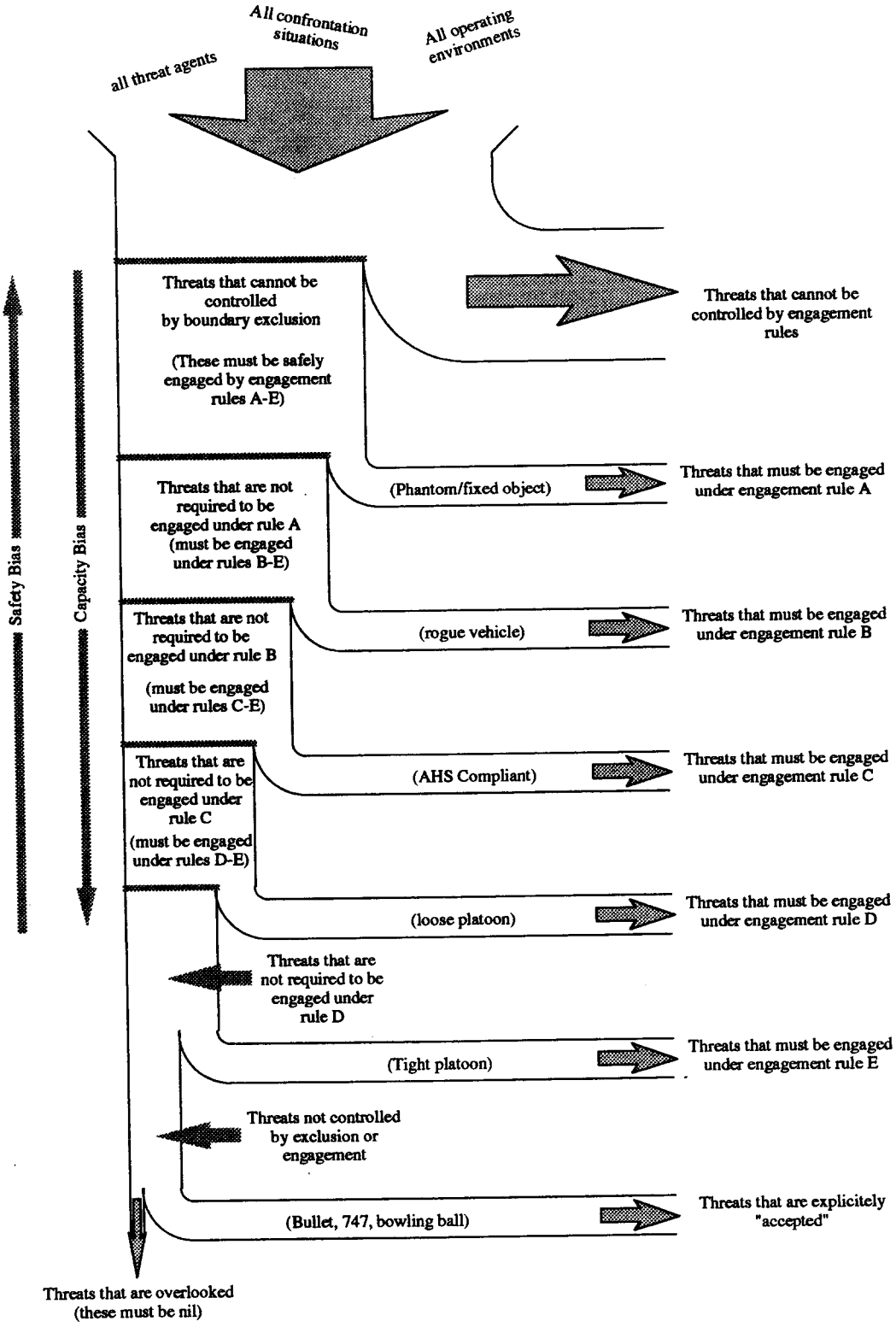


Figure 70. Threat control flow analogy.

1. The “as-is, where-is” capability of the vehicle. The real-time capability to adequately execute its responsibilities in a particular engagement. Variations between vehicles may exist as a result of malfunction (vehicle health) degraded performance, stage of AHS evolution, road condition influences, and, as will be introduced later, potential operator intervention. We have termed this “functional” authority. Functional authority determines how far down we can move in figure 70.

2. Authority restrictions imposed by a system-level operations supervisory function. For example, such limits may be imposed because of traffic problems elsewhere in the system or weather conditions that suggest that more restrictive states are in order. There may also be conditions for minimum capabilities. For example, during rush hours, it may be desirable to operate at maximum lane density—tight platoon engagements. Establishing this requirement would invoke controls at the AHS boundary to exclude all vehicles not capable of participating in this restrictive state. We have termed authority criteria generated by a system function “ruling” authority.

3. The final, and most important, authority component is permission from the privileged vehicle. A burdened vehicle cannot autonomously change the rules under which it and its paired privileged vehicle operate. The privileged vehicle may have to adjust its relationship to the vehicle ahead of it because of its obligations as a burdened vehicle in that relationship. Furthermore, platoon engagements may require the privileged vehicle to adjust its capability (e.g., engage brake suppression) before it can allow the engagement. Therefore, before a privileged vehicle can grant permission for a follower to close, it has certain housekeeping chores that must be completed prior to allowing the following vehicle to close. We have termed this “conditional” authority.

The same authority concepts apply to merge situations, but two-way simultaneous authority must be obtained because, until the merge is executed, the on-line vehicles that are developing the merge gap are both privileged with respect to the merging vehicle. This is the reason we suggest, when possible, entry options that allow a vehicle to reach a pseudo steady state engagement with the line vehicles before the merge maneuver.

The use of authority to manage the navigation among various restrictive states also applies in reverse, and is a key element of fail-safety. Authority is granted under exacting conditions that indicate that both vehicles are capable of participation. Furthermore, this authority is granted for a very short period of time, after which the separation manager will seek a more restrictive state—unless the authority is revalidated. This represents the “normally open, held closed” concept of engagement referred to in earlier sections of this report. The holding force is authority. If any change in condition results in a nonaffirmation of authority, it is assumed it is withdrawn and the trailing vehicle seeks a more restrictive state.

A perhaps subtle implication of the process illustrated in figure 70 is that functional authority has a “cumulative” attribute: as we move down through the restrictive levels, additional capabilities are

required. This means that a vehicle that is capable of operating in a specified restrictive state must also be capable of operating at all *more* restrictive states. If it is not, it would have been restricted at the level corresponding to this higher restriction. This may not appear significant, but it is fundamental to the concept of operations discussed in the next section.

Procedural Implications

A concept of separation manager operations for managing navigation among these various restrictive states is represented by the logic diagram in figure 71. This figure illustrates a sequential process of engaging threats (underscoring the need for "sequential" capability referred to above). This process is very deliberate; authorizing closures to less restrictive states only when the required conditions are satisfied. This implies a movement between sequential steady states (no "leapfrogging"). There are a number of reasons why this approach would be desirable, not the least of which is to allow a resolution of one transition maneuver and the establishment of the next before the latter is initiated. However, we do not have any technical reason to suggest such a limitation. We see no reason that an AHS vehicle could not be allowed to close directly from an AHS compliant engagement to a tight platoon in one transition, as long as there is compliance with the rules of authority and transition management.

This figure illustrates the feedback loops for maintaining engagement authority, challenging the wisdom of a particular engagement, and invoking disengagement actions. In addition, there is the suggestion that we always begin engagement at the maximum range possible. If there is no threat agent ahead of us, this would be the separation required to engage the "phantom" vehicle (assuming, of course, that at this range we don't overlook an intermediate threat). When real vehicles enter our view, the process of engaging is initiated—the final steady state condition is established, together with an appropriate transition strategy and the point of initiation. Authority may be granted at this time, however, if the engagement is too far off, this would only be provisional, subject to validation prior to the transition maneuver. It would, however, establish communication and notify the lead vehicle that the follower is aware of its presence and what its intentions are. This may be of little consequence in an urban environment because the likelihood of engaging a phantom probably only exists for the first vehicle on the system. In rural application, this forward view must be reset every time an engaged vehicle leaves the lane in light traffic conditions.

With this concept, vehicle check-in takes on additional duties. In addition to determining the health of a vehicle, additional data must be generated to initialize the separation manager:

- The "as-is, where-is" functional authority of the vehicle.
- Factoring in any ruling authority limits that may be in existence at the time.
- Calibrating the controllability of the vehicle (stopping characteristics) as they exist at that time, factoring in roadway calibration factors if they are used.

- Establishing and calibrating the initial engagement rule to be used to manage the acceleration and merge operations. This process essentially “turns on” the automated capability for that vehicle.

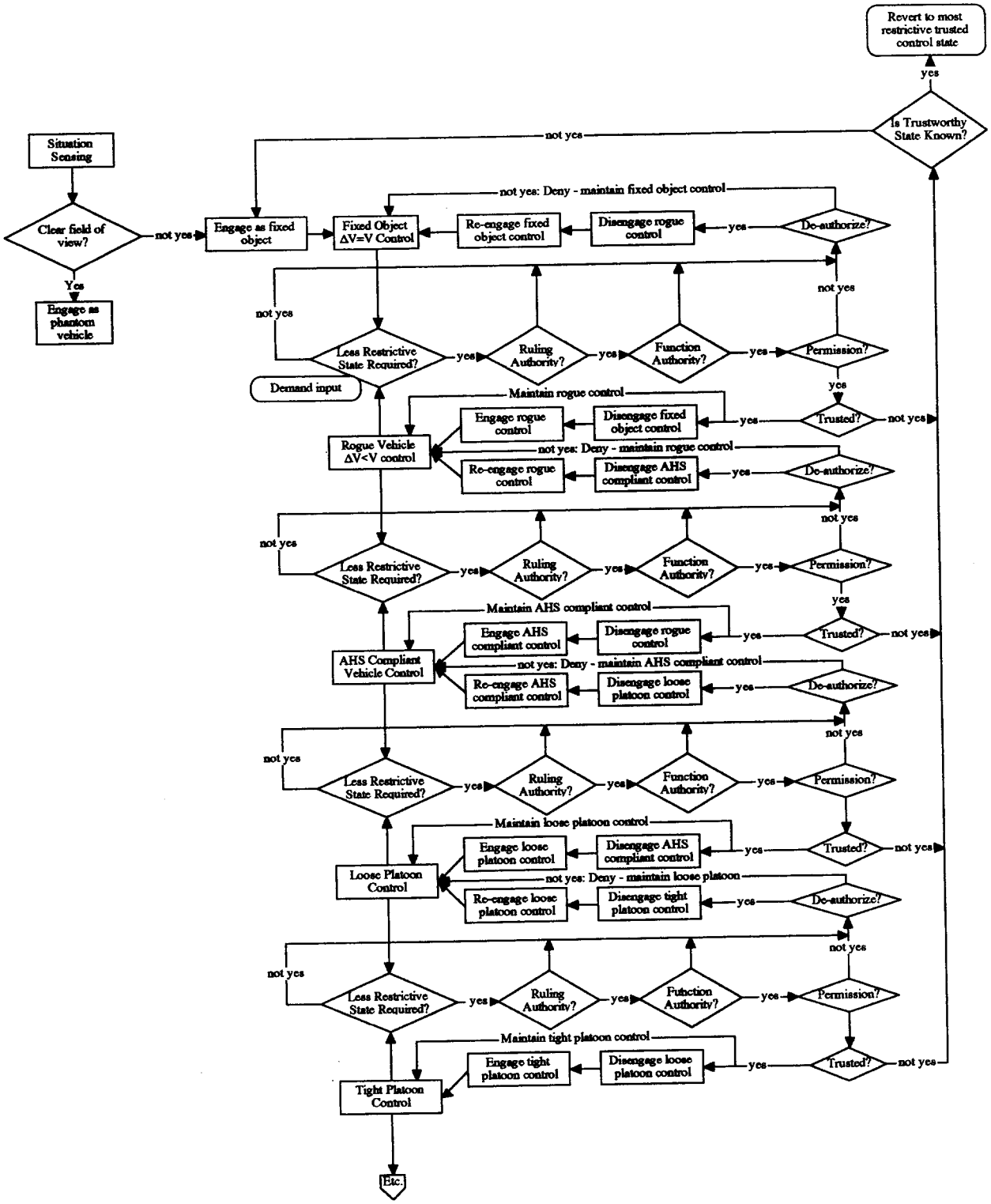


Figure 71. Concept of operation for separation management.

Others exist, but these serve to illustrate the role of check-in as an integral part of separation management. These functions may be performed by the vehicle-based separation manager, but they are still allocated to the check-in process.

Accommodation of Operator Input

In earlier sections, we made a number of references to the potential for operator input. While an AHS must be capable of transporting a vehicle to an absolutely safe state, without any operator intervention, there may be conditions where operator input is desired or necessary. We have not examined the human factors issues associated with operator intervention actions. However, we believe there are at least five situations where it could be effectively utilized within the concepts of authority discussed above.

Operator Attitude Adjustment

There may be some cases where an operator wishes to disengage to a more restrictive state. This may be a result of a perceived malfunction or perhaps simply because small separations between vehicles are no longer comfortable. Some capability to allow the operator to serve as another signal to the separation manager, declaring the existing engagement invalid, in turn causing the separation manager to seek a more restrictive state. This would utilize all normally functioning separation controls. Therefore, this operation would be accommodated under full control.

Conflict Resolution

There may be situations where the sensing system may not be definite in identifying threat agents (e.g., animals). The AHS will assume the absolute worst option. If the driver could be involved in this decision, by some query, these conflicts may be resolved without a worst case assumption.

Threat Situation Intervention

This is a capability to notify the separation manager of an impending dangerous situation. An operator may see forward situations developing (e.g., several vehicles forward) and should have the capability to alert the vehicle control system. This would be handled through the separation manager's urgent intervention capabilities.

Extremis Alert

This is an extension of threat situation intervention. There should be the capability to initiate a vehicle extremis intervention action if, for some reason, normal vehicle sensing fails to sense the extremis situation. An operator initiated extremis alert would activate the normal extremis actions, pre-programmed and calibrated by the separation manager based on the current vehicle state. This is potentially very problematical because of the possibility of false action or unwarranted panic reactions. An extremis action is itself a collision inducing event. This is tolerable if a real extremis situation exists. If not, however, the consequences are clear. We feel strongly that this capability should be present, but are unclear on ways to limit it to real extremis situations.

Extremis Takeover

We do not advocate that the AHS ever be able to force a manual takeover as an extremis intervention action. However, we feel it necessary to allow the operator to take control of his/her vehicle in an extremis situation, allowing a manual evasive maneuver, such as manual steer around, to be executed. This will probably be demanded. The problems are the same as for extremis alert—its use when it is not warranted and its potential collision inducing effects.

FINDINGS AND CONCLUSIONS

This report has highlighted many concerns regarding the ability of an AHS to achieve a collision free environment, in terms of in-line collisions, in the absence of malfunctions. While there are significant technical challenges to be met, we do not consider any to be beyond resolution. The following summarizes some of the more global concerns that have developed during this investigation:

- An AHS vehicle must be capable of engaging all forms of threat agents that appear on an AHS lane. These include other AHS vehicles, rogue vehicles (vehicles not known to under full AHS control), and nonvehicles, including dropped loads, animals, people, etc.

- A separation management function should be developed to handle the decision-making function for steady state separations, transition maneuvers, urgent fault intervention maneuvers, and extremis maneuvers.

- The concepts of managing engagement through authority, fail-safe procedures, and privilege/burden relationships appear to be applicable to AHS operations and should be considered for the separation manager.

- From our simple dynamic models, it appears that as we move toward small separation operations (tight platoons), the susceptibility to malfunctions and transferred collisions increases. Chain collisions will be difficult to prevent, without prevention of the initial collision.

- Small separation operations require the maximum capabilities in separation management. We are not fully convinced that separations on the order of a few feet can be supported over the full range of motions and worst case expectations of an AHS. It appears that brake suppression devices, to limit worst case maneuvers, as well as capabilities of coordinated braking and extremely small response time, will be required. We suspect that there will be some proof of concept work in these areas. We further feel that extensive simulations will be required to test the validity of small separation concepts over the full duty cycles expected.

- AHS operations will require a level of situation awareness that far exceeds the implied requirements of current AHS concepts. We suspect that a considerable amount of proof of concept work will be required in the entire arena of sensing and decision processes to adequately assess the situation to be controlled.

- A corollary to situation awareness is the communication required to adequately establish and maintain a valid engagement. There is a need to establish agreement and continually verify validity one-on-one. How will a vehicle verify that it is talking to the right vehicle? A

number of marine casualties have occurred because authority and agreement had been reached between the wrong vessels. How can we control this? Similarly, if extremis or malfunction broadcast methods are used to trigger intervention actions, how do we know which vehicles should be notified? How do we limit a broadcast to these vehicles so that we don't influence the entire system?

- While the techniques discussed in exit transition concerns can be alleviated, we still believe that it may be very difficult to ensure that the AHS does not eject a vehicle into an unmanageable situation.

APPENDIX A

INADEQUATE ENGAGEMENT RULES

Separation less than minimum safe limits for no collision
1. Separation control inadequate
1.1. Separation rules inadequate
1.1.1. Inadequate assessment of braking capabilities
1.1.1.1. Inadequate recognition of braking rate influencers
1.1.1.1.1. Vehicle-related influencem
1.1.1.1.1.1. "Characteristic" performance influencers
1.1.1.1.1.1.1. Nominal brakingrates
1.1.1.1.1.1.2. Standard tires
1.1.1.1.1.1.3. Suspension design and load transfer characteristics
1.1.1.1.1.2. "As-is" performance influencers
1.1.1.1.1.2.1. Tires
1.1.1.1.1.2.2. Tirewear
1.1.1.1.1.2.3. Tire inflation
1.1.1.1.1.2.4. Suspension changes
1.1.1.1.1.2.5. Load distribution
1.1.1.1.1.2.6. Brake fade
1.1.1.1.2. Roadway-related influencers
1.1.1.1.2.1. "Characteristic" influencers
1.1.1.12.1.1. Geometry
1.1.1.1.2.1.1.1. Curves
1.1.1.1.2.1.1.2. Grades
1.1.1.1.2.1.1.3. Combined coupling (brakes/steering)
1.1.1.1.2.1.2. Surface
1.1.1.1.2.1.2.1. General
1.1.1.1.2.1.2.2. Bumps
1.1.1.1.2.1.2.3. Waviness
1.1.1.1.2.1.2.4. Joints
1.1.1.1.2.1.2.5. Surface treatment
1.1.1.1.2.2. "As-is" influencers
1.1.1.1.2.2.1. Salt/Sand
1.1.1.1.2.2.2. Potholes
1.1.1.1.2.2.3. Repairs
1.1.1.2. Inadequate recognition of environment-related influences
1.1.1.2.1. Inadequate recognition of influencers
1.1.1.2.1.1. Inadequate recognition of "characteristic" (prevailing) influencers
1.1.12.1.1.1. Temperatures
1.1.1.2.1.1.2. Visibility
1.1.1.2.1.2. Inadequate recognition of "As-is" influencers
1.1.1.2.1.2.1. Ice
1.1.1.2.1.2.2. Snow
1.1.1.2.1.2.3. Rain
1.1.1.2.1.2.4. Temperature

1.1.1.2.1.2.5. Visibility
1.1.12.2. Inadequate recognition of influences
1.1.1.2.2.1. Vehicle characteristic influences
1.1.1.2.2.1.1. Ice/slush on vehicle suspension
1.1.1.22.1.2. Temperature on suspension
1.1.1.2.2.1.3. Temperature on tire characteristics
1.1.12.2.1.4. WetBrakeperformance
1.1.1.2.2.2. Roadway characteristic influences
1.1.1.22.2.1. Surface effects
1.1.1.2.2.2.2. Friction effects
1.1.1.3. Inadequate valuation of braking rate influences
1.1.1.3.1. Inadequate determination of functional relationships
1.1.1.3.2. Inadequate consideration of measurement capabihties
1.1.1.4. Inadequate consideration of braking constraints on burdened vehicle
1.1.1.4.1. Comfort limits jerk)
1.1.1.4.2. Dual role - burdened and privileged
1.1.2. Inadequate assessment of effects of vehicle dynamics on stopping distance
1.1.2.1. Inadequate recognition of influencers
1.1.2.1.1. Velocity
1.1.2.1.2. Acceleration
1.1.2.2. Inadequate recognition of environment-related influences
1.1.22.1. Inadequate recognition of influencers
1.1.2.2.1.1. Wind
1.1.2.2.1.2. Gusts
1.1.2.22. Inadequate recognition of influences
1.1.2.2.2.1. Velocity variations
1.12.2.2.2. Deceleration increases/decreases
1.1.2.3. Inadequate valuation of vehicle dynamics influences
1.1.2.3.1. Inadequate determination of functional relationships
1.1.2.3.2. Inadequate consideration of measurement capabilities
1.1.3. Inadequate consideration of control delays on stopping distance
1.1.3.1. Inadequate consideration of delay soueces
1.1.3.1.1. Conflicting object recognition
1.1.3.1.2. State sensing
1.1.3.1.3. Performance criteria
1.1.3.1.3.1. Jerk limits
1.1.3.1.3.2. Deceleration profile limits
1.1.3.1.4. Control actuator response characteristics
1.1.3.1.5. Controlled element response characteristics
1.1.3.2. Inadequate consideration of environmental influences on response
1.1.3.2.1. Ice
1.1.3.22. snow
1.1.3.2.3. slush
1.1.3.2.4. water
1.1.3.2.5. temperature
1.1.3.3. Inadequate valuation of control delay influences
1.1.3.3.1. Inadequate deterinination of functional relationships

1.1.3.3.2. Inadequate consideration of measurement capabilities
1.1A. Inadequate consideration of values for stopping distance influencers
1.1A.1. Inadequatemetrics
1.1A.1.1. Vehicle-based influencers
1.1.4.1.2. Roadway-based influencers
1.1.4.2. Inadequate flinctional relationships
1.1.5. Inadequate selection of influencer values or ranges for control laws
1.1.5.1. Inadequate consideration of situation awareness capabilities
1.1.5.1.1. Separation measures
1.1.5.1.2. Vehicle speed (own vehicle and leading vehicle)
1.1.5.1.3. Vehicle accelerations (own vehicle and leading vehicle)
1.1.5.2. Inadequate consideration of separation management capabilities
1.1.5.2.1. Ability to measure values of influencing variables
1.1.5.2.2. Comprehension of measurement variationsiprecision
1.1.5.2.3. Comprehension of on-vehicle controllerlactuator response characteristics
1.1.6. Inadequate translation of influencer values to control laws
1.1.7. Inadequate consideration of control boundary
1.1.7.1. Inadequate determination of influencer values that exceed design control limits
1.1.7.2. Inadequate situation innagement rules (more restrictive states)
1.1.7.2.1. Degraded system operations
1.1.7.2.2. Vehicle rejection criteria
1.1.7.2.3. Degraded vehicle operations
1.1.7.2.3.1. Speed limits
1.1.7.2.3.2. Minimum separation modification
1.2. Separation enforcement inadequate
1.2.1. Inadequate pre-trip controls (Vehicle based, check-in based, wayside-based)
12.1.1. Inadequate determination of vehicle state
1.2.1.1.1. Inadequate vehicle situation awareness
1.2.1.1.1.1. Vehicle state detection inadequate
1.2.1.1.1.1.1. Inadequate translation of contol laws into vehicle state signals
1.2.1.1.1.1.2. State variables not adequately sensed
1.2.1.1.1.1.2.1. No valid proxy measure exists
1.2.1.1.1.1.2.2. No sensors
1.2.1.1.1.1.2.3. Inadequate sensors
1.2.1.1.1.1.2.3.1. type
1.2.1.1.1.1.2.3.2. range
12.1.1.1.1.2.3.3. location
1.2.1.1.1.1.2.3.4. sensitivity
1.2.1.1.1.12.3.5. precision
1.2.1.1.1.2. Vehicle state interpretation inadequate
12.1.1.1.2.1. signal fusion
1.2.1.1.1.2.2. signal calibration
1.2.1.1.1.2.3. decision logic
12.1.1.1.2.4. software errors
1.2.1.1.2. Inadequate vehicle situation assessment
1.2.1.12.1. Test measures-to~vehicle capability algorithm Inadequate
1.2.1.1.2.2. Decision errors

1.2.1.1.2.3. Software errors
1.2.1.2. Inadequate determination of roadway state
1.2.1.2.1. Inadequate roadway situation awareness
1.2.1.2.1.1. Roadway state detection inadequate
1.2.1.2.1.1.1. Inadequate translation of control laws into roadway state signals
1.2.1.2.1.1.2. State variables not adequately sensed
1.2.1.2.1.1.2.1. No valid proxy measure exists
1.2.1.2.1.1.2.2. No sensors
1.2.1.2.1.1.2.3. Inadequate sensors
1.2.12.1.1.2.3.1. type
1.2.1.2.1.1.2.3.2. range
1.2.1.2.1.1.2.3.3. location
1.2.1.2.1.1.2.3.4. sensitivity
1.2.1.2.1.1.2.3.5. precision
1.2.1.2.1.2. Roadway state interpretation inadequate
1.2.1.2.1.2.1. signal fusion
1.2.1.2.1.22. signal calibration
1.2.1.2.1.2.3. decision logic
1.2.1.2.1.2.4. software errors
1.2.1.2 2. Inadequate roadway situation assessment
1.2.1.2 2.1. Test measures-to~roadway capability algorithm inadequate
1.2.1.2.2.2. Decision errors
1.2.1.2 2.3. Software errors
1.2.1.3. Inadequate combination of roadway/vehicle states
1.2.1.4. Inadequate decision
1.2.1 A.1. State-to-real performance algorithm inadequate
1.2.1.4.2. Rejection criteria inadequate
1.2.1.4.3. Separation criteria inadequate
1.2.1.4.4. Decision error
1.2.1.4A.1. Inadequate decision logic
1.2.1.4A.2. Software error
1.2.1.5. Inadequate control execution
1.2.1.5.1. Capabilities do adjust generic separation criteria inadequate
1.2.1.5.2. Capabilities to adjust vehicle-specific separation criteria inadequate
1.2.1.5.3. Communication errors
1.2.1.5.4. Acceptance errors
1.2.1.5.5. Verification errors
1.2.2. Inadequate enroute controls (Vehicle based, check-in based, wayside-based) (Same as pre-trip but aimed at detecting changes from pre-trip conditions)
1.2.2.1. Inadequate determination of vehicle4o-vehicle state
1.2.2.1.1. Inadequate situation awareness (Separation, velocity, acceleration-continuously monitored)
1.2.2.1.1.1. Vehicle-to-vehicle state detection inadequate
1.2.2.1.1.1.1. No sensors
1.2.2.1.1.1.2. Inadequate sensors
1.2.2.1.1.1.2.1. type
1.2.2.1.1.12.2. range
1.2.2.1.1.1.2.3. location

1.2.2.1.1.1.2.4. sensitivity
1.2.2.1.1.1.2.5. precision
1.2.2.1.1.2. Vehicle-to-vehicle state interpretation inadequate
1.2.2.1.1.2.1. signal fusion
1.2.2.1.1.2.2. signal calibration
1.2.2.1.1.2.3. decision logic
1.2.2.1.1.2.4. software errors
12.2.1.2. Inadequate situation assessment
1.2.2.1.2.1. Decision errors
1.2.2.12.2. Software errors
1.2.2.2. Inadequate determination of vehicle state
1.2.2.2.1. Inadequate vehicle situation awareness
1.2.2.2.1.1. Vehicle state detection inadequate
12.2.2.1.1.1. inadequate translation of control laws into vehicle state signals
1.2.2.2.1.1.2. State variables not adequately sensed
1.2.2.2.1.1.2.1. No valid proxy measure exists
1.2.2.2.1.1.2.2. No sensors
1.22.2.1.12.3. inadequate sensors
1.22.2.1.1.2.3.1. type
12.22.1.1.2.3.2. range
1.2.2.2.1.12.3.3. location
1.2.2.2.1. 1.2.3A. sensitivity
1.2.2.2.1.1.2.3.5. precision
1.2.2.2.1.2. Vehicle state interpretation inadequate
12 2.2.1.2.1. signal fusion
1.2.2 2.12.2. signal calibration
1.2 2.2.1.2.3. decision logic
1.2.2.2.12.4. software errors
1.2.2.2.2. Inadequate vehicle situation assessment
1.2 2.2 2.1. Test measures-to-vehicle capability algorithm inadequate
1.2 2.2.2.2. Decision errors
1.2 2.2.2.3. Software errors
1.2.2.3. Inadequate determination of roadway state
1.2.2.3.1. inadequate roadway situation awareness
1.2.2.3.1.1. Roadway state detection inadequate
1.2.2.3.1.1.1. inadequate translation of control laws into roadway state signals
12.2.3.1.1.2. State variables not adequately sensed
1.2.2.3.1.1.2.1. No valid proxy measure exists
1.2.2.3.1.1.2.2. No sensors
1.2.2.3.1.1.2.3. inadequate sensors
1.2.2.3.1.1.2.3.1. type
1.2.2.3.1.12.32. range
1.2.2.3.1.1.2.3.3. location
1.2.2.3.1.1.2.3.4. sensitivity
1.2.2.3.1.1.2.3.5. precision
1.2.2.3.1.2. Roadway state interpretation inadequate
1.2.2.3.1.2.1. signal flsion

1.2.2.3.1.2.2. signal calibration
1.2.2.3.1.2.3. decision logic
1.2.2.3.1.2.4. software errors
1.2.2.3.2. Inadequate roadway situation assessment
1.2.2.3.2.1. Test measures-to-roadway capability algorithm inadequate
1.2.2.3.2.2. Decision errors
1.2.2.3.2.3. Software errors
1.2.2.4. Inadequate combination of roadway/vehicle states
1.2.2.5. Inadequate decision
1.2.2.5.1. State-to-real performance algorithm inadequate
1.2.2.5.2. Rejection criteria inadequate
1.2.2.5.3. Separation criteria inadequate
1.2.2.5A. Decision error l.2.2.5A.1. inadequate decision logic
1.2.2.5A.2. Software error
1.2.2.6. Inadequate control execution
1.2.2.6.1. Capabilities do adjust enroute generic separation criteria inadequate
1.2.2.6.2. Capabilities to adjust emoute vehicle-specific separation criteria inadequate
Communication errors
1.2.2.6.3. Communication errors
1.2.2.6.4. Acceptance errors
1.2.2.6.5. Verification errors

APPENDIX B

INADEQUATE SEPARATION MANAGEMENT

In-line collision involving MIS vehicle, under MIS control Accident threats exist

1. Collision threat exists

1.1. Conflict Agent Exists

In the context of this analysis, one element of a conflict situation is assumed: the subject vehicle, which is always taken to be the threatened vehicle, insofar as the threat agents all represent impediments to an "assured clear distance" for the subject vehicle. Obviously, our subject vehicle will itself be a threat agent to following vehicles.

1.1.1. Fixed agents

Fixed object agents are those threat agents that represent a conflict that has no ability to move out of the way. All collision avoidance capability must be provided by the subject vehicle. We recognize that their are transient agents included in this category (people and animals). However, because of the unpredictability of their motions, we feel it unwise to consider their mobility in a collision avoidance strategy. This category also includes stopped vehicles --without consideration of why they are stopped. It may be the result of a backup from MIS lane exit facilities or an MIS vehicle malfunction. Regarding the latter, we do not believe it wise to avoid accepting responsibility for avoiding this collision within the envelope of normal operations. We have also made no distinction on the basis of object size. Obviously, a small object may not represent a real "collision" threat However, it does represent a threat to control capability -- throwing a vehicle off course or inducing wheel-hop at a critical point where lateral and longitudinal control requirements are critical.

1.1.1.1. Non-vehicle object

1.1.1.2. Stopped vehicle

1.1.1.3. Person

l.1.1A. Animal

1.1.2. Rogue vehicles

The "rogue" vehicle is a vehicle that, for whatever rean, is not knowr: to be under some level of MIS control. More than likely, this will be a non-MIS vehicle, on the MIS lane either by design or inappropiate intent. However, note the emphasis on "not known...." A vehicle may be under full MIS control; but, for some reason, this is not known to our subject vehicle. We must treat this vehicle as an uncontrolled nogue. This is another "malfunction" that we feel must be accommodated within the shell of normal operations.

1.1.3. MIS vehicles

An MIS vehicle, in this report, is always meant to be an MIS-controlled vehicle- controlled, in full, as intended by the particular control law in force at the time.

1.2. Conflict situation present

1.2.1. Mainline Collisions

1.2.1.1. Vehicle4o-vehicle collisions, stable, in4ine conditions

1.2.1.1.1. Subject vehicle-to-leading vehicle Collisions

1.2.1.1.1.1. lead vehicle stopped

1.2.1.1.1.2. lead vehicle moving

12.1.1.1.2.1. MIS-controlled Vehicle

1.2.1.1.1.2.2. Non-AHS-controlled Vehicle
1.2.1.1.2. Trailing vehicle-to-subject vehicle collisions
1.2.1.1.2.1. MIS controlled vehicle
1.2.1.1.2. Trailing vehicle-to-subject vehicle collisions
1.2.1.1.2.1. MIS controlled vehicle
1.2.1.1.2.2. Non-MIS controlled vehicle
1.2.1.2. Single MIS vehicle collisions
1.2.1.2.1. Collision with guideway structures in lane
1.2.1.2.2. Collision with lane-fouling objects
1.2.1.2.2.1. Collisions with large objects
1.2.1.2.2.1.1. Trees, poles, etc.
1.2.1.2.2.1.2. Dropped load
1.2.1.2.2.1.3. Dropped equipment
1.2.1.2.2.1.4. Debris/equipment incursion from adjacent lanes
1.2.1.2.2.2. Collision with People
1.2.1.2.2.3. Collision with large animals
1.2.1.3. Collision with Shared Right-of-way vehicle intrusion
1.2.1.3.1. Intentional intrusion
1.2.1.3.1.1. MIS Controlled situation
1.2.1.3.1.1.1. Merging MIS vehicle
1.2.1.3.1.1.2. lane changing MIS vehicle
1.2.1.3.1.2. Manual Controlled vehicle
1.2.1.3.2. Unintentional incursion

1. Enabling Conditions Exist
1.1. Inadequate overall operational situation awareness
1.1.1. Inadequate system demand situation awareness
1.1.1.1. Inadequate awareness of demand pressures for restrictive state selection
1.1.1.1.1. Capacity
1.1.1.1.2. Velocity
1.1.1.1.3. Comfort limits
1.1.1.2. Inadequate awareness of demand bias for resolving restrictive state options
1.1.1.2.1. change restrictive state
1.1.1.2.2. Change restrictive level
1.1.1.2.2.1. velocity
1.1.1.2.2.2. separation of coupled vehicles
1.1.1.2.2.3. length of coupled vehicle platoon
1.1.2. Inadequate threat situation awareness
1.1.2.1. Individual vehicle threat situation awareness
1.1.2.1.1. Inadequate threat agent detection
1.1.2.1.1.1. Unaware of need to detect
1.1.2.1.1.1.1. Threat agent not anticipated
1.1.2.1.1.1.1.1. False hypothesis - overall threat assumptions
1.1.2.1.1.1.2. Threat agent not expected
1.1.2.1.1.1.2.1. False hypothesis - boundary exclusion control effectiveness
1.1.2.1.1.2. Inadequate capabilities to detect
1.1.2.1.1.2.1. Inadequate definition of threat agent indicators
1.1.2.1.1.2.2. Inadequate field of view

1.1.2.1.1.22.1. Inadequate sensor capabIlities
1.1.2.1.1.2.2.2. Inadequate detection range
1.1.2.1.1.2.2.2.1. Inadequate requirements specification
1.1.2.1.1.2.2.2.2. Inadequate calibration
1.1.2.1.1.2.2.3. Inadequate consideration of detection constraints
1.1.2.1.1.2.2.3.1. Physical constraints (curves, barriers, obstacles, etc..)
1.1.2.1.1.2.2.3.2. Situational constraints
1.12.1.1.2.2.3.2.1. Inadequate agent "signal"
1.1.2.1.1.2.2.3.2.2. Inadequate signal discrimination
1.1.2.1.1.2.2.4. Electronic equivalent of expectancy (focus)
1.1.2.12. Inadequate threat assessment
1.1.2.1.2.1. Inadequate threat agent identification
1.1.2.1.2.1.1. Unaware of need to identify
1.1.2.1.2.1.2. Inadequate strategy
1.1.2.1.2.12.1. Inadequate compliance with state control strategy
1.1.2.1.2.1.2.1.1. Critical identification parameters not understood
1.1.2.12.12.12. Proximate measures inadequate
1.1.2.1.2.12.1.2.1. Compliance with need
1.1.2.1.2.12.1.2.2. Flawed implementation expectations
1.1.2.12.12.2. Inadequate fail-safe consideration
1.1.2.1.2.1.3. Inadequate implementation
1.12.12.1.3.1. Inadequate specification of sensorsisignal logic
1.1.2.1.2.1.3.2. Inadequate compliance with strategy
1.1.2.1.2.2. Inadequate threat situation determination
1.1.2.1.22.1. Inadequate assessment of privileged vehicle state
1.1.2.12.2.1.1. Unaware of need to determine
1.12.1.2.2.1.2. Inadequate strategy
1.12.1.2.2.12.1. Inadequate compliance with state control strategy
1.12.12.2.1.2.1.1. Critical state parameters not understood
1.12.1.22.1.2.1.2. Proximate measures inadequate
1.12.1.2.2.1.2.1.2.1. Compliance with need
1.1.2.1.22.12.12.2. flawed implementation expectations
1.12.1.2.2.1.2.2. Inadequate fail-safe consideration
1.1.2.1.2.2.1.3. Inadequate implementation
1.1.2.1.22.1.3.1. Inadequate specification of sensors/signal logic
1.1.2.1.2.2.1.3.2. Inadequate compliance with strategy
1.1.2.12.2.2. Inadequate assessment of burdened vehicle state
1.12.1.2.2.2.1. Inadequate strategy
1.1.2.1.2.2.2.1.1. Inadequate compliance with state control strategy
1.1.2.1.2.2.2.1.1.1. Critical state parameters not understood
1.1.2.1.2.2.2.1.1.2. Proximate measures inadequate
1.1.2.1.2.2.2.1.1.2.1. Compliance with need
1.1.2.1.2.2.2.1.1.2.2. Flawed implementation expectations
1.1.2.1.2.2.2.12. Inadequate fail-safe consideration
1.1.2.1.2.2.2.2. Inadequate implementation
1.1.2.1.2.2.2.2.1. Inadequate specification of sensors/signal logic
1.1.2.1.2.2.2.2.2. Inadequate compliance with strategy

1.1.2.2. Inadequate awareness of current systemic threat situations

This subject refers to awareness of conditions that suggest the need for a change in system operations to control certain threats. The form of control is generally restricting exposure to threat situations. Included in this category would be the detection and assessment of objects in the roadway, fires or hazmat spills in adjacent lanes, accidents on the MIS system, etc..

The form of control would, in general not influence a vehicle in the immediate danger zone, but would reduce exposure of other vehicles by imposing operating constraints.

This category of situation awareness may duplicate similar capabilities on individual vehicles or it may address threat situations that cannot be effectively detected by individual vehicles.

1.1.2.2.1. Inadequate strategy
1.1.2.2.1.1. Inadequate compliance with state control strategy
1.1.2.2.1.1.1. Critical state parameters not understood
1.1.2.2.1.1.2. Proximate measures inadequate
1.1.2.2.1.1.2.1..Compliance with need
1.1.2.2.1.1.2.2..Flawed implementation expectations
1.1.2.2.1.2. Inadequate fail-safe consideration
1.1.2.2.2. Inadequate implementation
1.12.2.2.1. Inadequate specification of sensorslsignal logic
1.1.2.2.2.2. Inadequate compliance with strategy
1.1.3. Inadequate control-ability situation awareness
1.1.3.1. Inadequate awareness of vehicle limits to authority
1.1.3.1.1. Control-ability of privileged vehicle
1.1.3.1.1.1. Inadequate strategy
1.1.3.1.1.1.1. Inadequate compliance with state control strategy
1.1.3.1.1.1.1.1. Critical state parameters not understood
1.1.3.1.1.1.1.2. Proximate measures inadequate
1.1.3.1.1.1.1.2.1. Compliancewithneed
1.1.3.1.1.1.1.2.2. Flawed implementation expectations
1.1.3.1.1.1.2. Inadequate fall-safe consideration
1.1.3.1.1.2. Inadequate implementation
1.1.3.1.1.2.1. Inadequate specification of sensors/signal logic
1.1.3.1.1.2.2. Inadequate complaance with strategy
1.1.3.1.2. Control-ability of burdened vehicle
1.1.3.1.2.1. Inadequate strategy
1.1.3.1.2.1.1..Inadequate compliance with state control strategy
1.1.3.12.1.1.1. Critical state parameters not understood
1.1.3.1.2.1.1.2. Proximate measures inadequate
1.1.3.1.2.1.1.2.1. Compliance with need
1.1.3.1.2.1.1.2.2. Flawed implementation expectations
1.1.3.1.2.1.2. Inadequate fall-safe consideration
1.1.3.1.2.2. Inadequate implementation
1.1.3.1.2.2.1. Inadequate specification of sensors/signal logic
1.1.3.1.2.2.2..Inadequate compliance with strategy
1.1.3.2. Inadequate awareness of roadway limits to authority

1.1.3.2.1. Inadequate strategy
1.1.3.2.1.1. Inadequate compliance with state control strategy
1.1.3.2.1.1.1. Critical state parameters not understood
1.1.3.2.1.1.2. Proximate measures inadequate
1.1.3.2.1.1.2.1. Compliance with need
1.1.3.2.1.1.2.2. Flawed implementation expectations
1.1.3.2.1.2. Inadequate fail-safe consideration
1.1.3.2.2. Inadequate implementation
1.1.3.2.2.1. Inadequate specification of sensors/signal logic
1.1.3.2.2.2. Inadequate compliance with strategy
1.1.3.3. Inadequate awareness of environmental limits to authority
1.1.3.3.1. Inadequate strategy
1.1.3.3.1.1. Inadequate compliance with state control strategy
1.1.3.3.1.1.1. Critical state parameters not understood
1.1.3.3.1.1.2. Proximate measures inadequate
1.1.3.3.1.1.2.1. Compliance with need
1.1.3.3.1.1.2.2. Flawed implementation expectations
1.1.3.3.1.2. Inadequate fall-safe consideration
1.1.3.3.2. Inadequate implementation
1.1.3.3.2.1. Inadequate specification of sensors/signal logic
1.1.3.3.2.2. Inadequate compliance with strategy

1.2. Inadequate system-wide threat management strategy

Each specific operating mode will deal with these system aspects as related to the specific issue. However, there is a need for an overall strategy to ensure that an integrated system results. Furthermore, there are many requirements for transition management: merging, entering, exiting, and transition between the primary threat management strategies (control state). Again, each specific engagement strategy will deal not only with maintaining engagement, but also the processes of engaging from a different operating mode and disengaging from that to join another

1.2.1..Inadequate threat control coverage
1.2.1.1. Inadequate recognition of overall threat environment

It is very important that the full range of threats faced by MIS vehicles be addressed. The "shopping list" cannot be arbitrarily truncated on the basis of preliminary assumptions. A full spectrum of threat scenarios must be developed for each operating situation as well as threats induced as the system traverses various operating modes from start-up to shutdown, from high demand to low demand, and from a bad environment to a good environment. These scenarios should stress the limits of possible operating and threat situations. It is important that the full range of possible threats be examined; simply because an omission for a system with this degree of public and private scrutiny could undermine the confidence that it has received a complete treatment We must be prepare to deal with the 747, the bowling ball, and the bullet (The latter is rapidly becoming significant threat)

1.2.1.2. Inadequate awareness of potential threat situations
1.2.1.2.1. Inadequate recognition of potential threat agents
1.2.1.2.2. Inadequate recognition of potential threat situations
1.2.1.3. Inadequate recognition of overall threat control responsibility
1.2.1.3.1. Threats overlooked/ignored

No identified threat can be summarily dismissed. Each must be dealt with in a consistent and defensible manner. No identified threat should be overlooked or ignored in this prccess.

1.2.1.3.2. Unwise dismissal by defining them to be outside "normal" operations

Included here are threats that are removed from consideration on the basis of expected low likelihood or low consequence. The issue points to the wisdom of these decisions. The most likely scenario for this issue is the dismissal of threats posed by non-MIS vehicles simply on the basis that they are not supposed to be present Unless adequate exclusion provisions exist that can guarantee exclusion, an engagement process must be in ------ even though it may be used very little. Furthermore, the required capabilities to engage may be required for other needs within the "normal" system and only require a proper calibration to function in this role.

1.2.1.3.3. Unwise dismissal on basis control difficulty

Includes threats that are extremely difficult to control --- such as a bullet striking the vehicle. It is true that there are threats that are "uncontrollable" within the bounds of reasonableness. However, most assumptions of this nature are fbcusing on the difficulty to control by engagement. These threats must be dealt with!!! This can be done by knowledgeable and recorded dismissal decisions. If they pose an unacoeptable threat, the implication is that efforts must be made to control.by exclusion techniques. No possible threat should go unaddressed--even if we are sure that we cannot adequately control them.

1.2.2..Inadequate overall threat control strategy

1.2.2.1. Inadequate systemic controls

1.2.2.1.1. Flawed assumptions of effectiveness

1.2.2.1.2. Flawed assumptions of implementability

1.2.2.2. Inadequate boundary controls

1.22.2.1. Inadequate physical threat agent exclusion techniques

1.2.2.2.1.1. Flawed assumption of physical exclusion effectiveness

1.2.2.2.1.2. Flawed assumption of implementability

1.2.2.2.2. Inadequate conditional authority exclusion techniques

1.2.2.2.2.1. False hypothesis - physical exclusion effectiveness

1.2.2.2.2.2. Flawed assumption of conditional exclusion effectiveness

1.22.22.3. Inadequate strategy

1.2.2.2.2.3.1. Inadequate compatibility with engagement control strategy

12.22.2.3.2. Inadequate compliance with engagement control expectations

1.2.2.2.3. Inadequate MIS vehicle initializing techniques

1.22.2.3.1. Inadequate understanding of need for initializing MIS vehicle

1.2.2.2.3.2. Inadequate recognition of role/requirements

1.2.2.2.3.2.1. Limiting restrictive state

1.222.3.2.2. Initial engagement rules

1.2.2.2.3.2.3. Engagement law calibration

1.2.2.2.3.3. Inadequate strategy

1.2.2.2.3.3.1. Inadequate compatibility with restrictive state/authority concepts

1.22.2.3.3.2. Inadequate compatibility with engagement control strategies

1.22.2.3.3.3. Inadequate compliance with engagement control expectations

1.22.3. inadequate engagement controls

12.2.3.1. False hypothesis - boundary control effectiveness
1.22.3.2. Flawed assumption of engagement effectiveness
12.2.3.3. Inadequate recognition of role/requirements
1.2.2.3.3.1. Primary threat management
1.22.3.3.2. Secondary threat management
1.2.2.3.3.2.1. Transferred threats
1.2.2.3.3.2.2. Intrinsic threats
1.22.3.3.2.3. Malfunctions
1.2.2.3.3.3. System safety management support
12.2.3.3.3.1. Authority management support
1.2.2.3.3.3.2. Restrictive state management support
1.2.2.3.3.4. Coordination with other control requirements
1.2.2.3.3.4.1. Other threat situations
1.2.2.3.3A.2. Other restrictive state situations
1.2.2.4. Inadequate accommodation of system safety concepts
1 .2.2A. 1. inadequate recognition of "restrictive states"
1.2.2.4.2. Inadequate recognition of "authority" to engage restrictive states
1 .2.2A.3. inadequate recognition of control "fail-safety"
1.2.2.5. Inadequate accommodation of human operator intervention
1.2.2.5.1. Emergency/valid
12.2.5.2. Choice/anxiety
1.2.2.5.3. Choice/choice
1.2.2.6. Inadequate consideration of simultaneous, multiple states
1.2.2.6.1. State as privileged vehicle
12.2.62. State as burdened vehicle
1.2.2.7. Inadequate treatment of reasonable malfunction management
1.2.2.7.1. Inadequate recognition of reasonable malfunctions
1.2.2.7.1.1. Transferred threats
1.2.2.7.1.2. Out-of-spec performance
1.2.2.7.2. Inadequate malfunction management strategy
1.2.2.7.2.1. Active
1.2.2.7.2.2. Reactive
1.2.2.7.2.2.1. lack of precalibrated expectations
1.2.2.7.2.2.2. Inadequate considerations of privileged vehicle state constraints
1.2.3..Inadequate system-wide safety control supervision
1.2.3.1. Inadequate understanding of role/responsibility
12.32. Inadequate authority monitoring
1.2.3.2.1. Critical parameters not understood
1.2.3.2.2. Proximate measures inadequate
1.2.3.22.1. Compliance with need
1.2.3.2.2.2. Flawed implementation expectations
1.2.3.2.3. Inadequate specification of sensors/signal logic
1.2.3.2A. Inadequate situation awareness
1.2.3.3. Inadequate restrictive state management capability
1.2.3.3.1. Inadequate enforcement capability
1.2.3.3.1.1. techniques for directing a state change
1.2.3.3.1.2. techniques for establishing bias in multiple option situations

12.3.3.2. Inadequate recognition of transition requirements
1.2.3.3.2.1. State-to-state
1.2.3.3.2.2. entry/exit
1.2.3.3.2.3. Merging
1.2.3.3.2.4. Start-up/shutdown
12.3.3.2A. 1. Normal
l.2.3.3.2A.2. Malfunction related
1.2.3.3.3. Inadequate Transition controls
1.2.3.3.3.1. Inadequate recognition of transition phases
1.2.3.3.3.1.1. State control program to disengagement program
1.2.3.3.3.1.2. Disengagement program to new state engagement program
1.2.3.3.3.1.3. Engagement program to new state control program
1.2.3.3.3.2. Inadequate transition strategy
1.2.3.3.3.2.1. Failure to recognize constraints on disengagement
1.2.3.3.3.2.1.1. Role as privileged vehicle
1.2.3.3.3.2.1.2. Role as burdened vehicle
1.2.3.3.3.22. Failure to recognize threat exposure during transition maneuver
1.2.3.3.3.2.3. Failure to recognize need to cease and revert
1.2.3.3.3.3. Inadequate procedures for changing signal focus
1.2.3.3.3.4. Inadequate procedures for changing control rules
1.2.3A. Inadequate restrictive level management capability
l.2.3A.1. Inadequate enforcement capability
1.2.3.4.1.1. techniques for directing a rule re-calibration
1.2.3.4.1.2. techniques for establishing bias in multiple option situations
1.2.3.42. Inadequate transition procedures
1.3..Inadequate specific threat management
1.3.1..Specific threat not controlled
1.3.1.1. Inadequate system-wide threat management strategy
1.3.2. Inadequate specific threat control
1.3.2.1. Inadequate systemic exposure control
1.3.2.1.1..Inadequate strategy
1.3.2.1.2..Inadequate implementation
1.3.2.2. Inadequate boundary controls
1.3.2.2.1. Inadequate Physical exclusion control
1.3.2.2.1.1. False hypothesis - overall control strategy
1.3.2.2.1.2. Critical exclusion parameters not understood
1.3.2.2.1.3. Inadequate application of sensors/signal logic
1.3.2.2.1.4. Flawed expectancy regarding effectiveness of physical constraints
1.3.2.2.1.5. Inadequate consideration of fail-safe requirements
1.3.2.2.2. Inadequate conditional exclusion control
1.3.2.2.2.1. False hypothesis - overall control strategy
1.3.2.2.2.2. Critical authority parameters not understood
1.3.2.2.2.3. Inadequate application of sensors/signal logic
1.3.2.2.2.4. Authority condition detection inadequate
1.32.2.2A.1. Inadequate proximate measures
1.3.2.2.2A.1.1. Inadequate representation of true parameter
1.3.2.2.2A.1.2. Unrealistic expectations of measurement capability

1.3.2.2.2A.2. Flawed expectancy
1.3.2.2.3. Inadequate MIS vehicle initializing control
1.3.2.2.3.1. Inadequate strategy
1.3.2.2.3.1.1..Inadequate compatibility with restrictive state/authority concepts
1.3.2.2.12. Inadequate compatibility with engagement control strategies
1.3.2.2.3.1.3. Inadequate compliance with engagement control expectations
1.3.2.2.3.2. Inadequate initializing procedures
1.3.2.2.3.2.1. Limiting restrictive state
1.3.2.2.3.2.2. Initial engagement rules
1.3.2.2.3.2.3. Engagement law calibration
1.3.2.3. Inadequate threat engagement controls
1.3.2.3.1. Normal engagement not anticipated
1.3.2.3.1.1. False hypothesis - control allocation wisdom
1.3.2.3.1.2. False hypothesis - boundary controls
1.3.2.3.1.2.1. Effectiveness
1.3.2.3.12.2. Functional health
1.3.2.3.1.3. False hypothesis - systemic exposure management
1.3.2.3.1.3.1. Effectiveness
1.3.2.3.1.3.2. Functional health
1.3.2.3.2. Incorrect engagement rules invoked
1.3.2.3.2.1. False hypothesis - situation awareness
1.3.2.3.2.2. False hypothesis - boundary controls
1.3.2.3.2.2.1. Authority of privileged vehicle
1.3.2.3.2.2.2. Authority of burdened vehicle
1.3.2.3.2.3. False hypothesis - conditions of application
1.3.2.3.2.3.1. Conditions of application unclear
1.3.2.3.2.3.2. Proximate measures fail to represent true desieed measures
1.3.2.3.2.3.3. Inadequate fail-safe considerations
1.3.2.3.3. Ineffective engagement rules
1.3.2.3.3.1. Inadequate engagement control strategy
1.3.2.3.3.1.1. Inadequate strategy to maintain engagement
1.3.2.3.3.1.1.1. Inadequate recognition of the threat control problem
1.3.2.3.3.1.1.1.1. Inadequate understanding of the conflict mechanics
1.3.2.3.3.1.1.1.2. Inadequate understanding of influencing parameters
1.3.2.3.3.1.1.1.3. Inadequate consideration of the effects of influencing parameters
1.3.2.3.3.1.1.1.4. Inadequate recognition of "worst case" situation
1.3.2.3.3.1.1.2. Inadequate recognition of the threat control requirements
1.3.2.3.3.1.1.2.1. Inadequate definition of worst case situation
1.3.2.3.3.1.1.2.2. Inadequate recognition of control options and constraints
1.3.2.3.3.1.1.2.3. Inadequate understanding of the variables affecting control-ability
1.3.2.3.3.1.2. Inadequate strategy to engage
1.3.2.3.3.1.3. Inadequate strategy to disengage
1.3.2.3.3.2. Inadequate control process "quality"
1.3.2.3.3.2.1. Inadequate management of transferred threats
1.3.2.3.3.2.1.1. Inadequate recognition of transferred threats
1.3.2.3.3.2.1.1.1. Within control state
1.3.2.3.3.2.1.1.2. To other control states

1.3.2.3.3.2.1.1.3. From other control states
1.3.2.3.3.2.1.2. Inadequate understanding of implications
1.3.2.3.3.2.1.2.1. Limits of control law applicability
1.3.2.3.3.2.1.2.2. Control law recalibration requirements
1.3.2.3.3.2.1.3. Inadequate actions taken
1.3.2.3.3.2.1.3.1. Inadequate specification of procedures for compensation
1.3.2.3.3.2.1.3.1.1. Control law calibration
1.3.2.3.3.2.1.3.1.2. Restrictive state change
1.3.2.3.3.2.1.3.2. Inadequate implementation of procedures
1.3.2.3.3.2.2. Inadequate management of intrinsic threats
1.3.2.3.3.2.2.1. Worst case "growth"
1.3.2.3.3.2.2.2. Control-ability deterioration
1.3.2.3.3.2.2.2.1. Vehicle capability deterioration
1.3.2.3.3.2.2.2.2. Roadway capability deterioration
1.3.2.3.3.2.3. Inadequate control of malfunction exposure
1.3.2.3.3.2.3.1. Inadequate understanding of malfunction exposure
1.32.3.3.2.3.2.Inadequate recognition of control responsibility
1.3.2.3.3.2.3.3. Inadequate control strategy
1.3.2.3.3.2.3.3.1. Detection
1.3.2.3.3.2.3.3.2. Restrictive state change
1.3.2.3.3.2.3.3.3. Restrictive level change
1.3.2.3.3.3. Inadequate integration with overall operational situation awareness
1.3.2.3.3.3.1. Inadequate definition of requirements for applying the rules
1.3.2.3.3.3.1.1. Required conditions for granting authority
1.3.2.3.3.3.1.1.1. Threat conditions
1.3.2.3.3.3.1.1.2. Control-ability conditions
1.3.2.3.3.3.1.2. Required conditions for denying authority
1.3.2.3.3.3.1.3. Required conditions for withdrawing authority
1.3.2.3.3.3.2. Inadequate metrics for establishing conditions
1.3.2.3.3.3.2.1. Proximate measures do not reflect intended measure
1.3.2.3.3.3.2.2. Measures do not reflect measurement capabilities
1.3.2.3.3 A. Inadequate compliance with overall system safety concepts
1.3.2.3.3A. 1. Inadequate implementation of fail-safe principles
1.3.2.3.3.4.1 1. Fail-safe principles not addressed
1.3.2.3.3A.1.2. Inadequate specification of fail-safe conditions
1.3.2.3.3.4.1.2.1. Inadequate coverage
1.3.2.3.3.4.1.2.2. Inadequate metrics
1.3.2.3.3.4.1.3. Inadequate monitoring of fail-safe conditions
1.3.2.3.3.4.1.4. Inadequate interaction with state authority management
1.3.2.3.3.4.2. Inadequate compliance with of state "authority" management
1.3.2.3.3.4.2.1. Inadequate specification of conditions for authority
1.3.2.3.3A.2.1.1. Required conditions for granting authority
1.3.2.3.3.4.2.1.1.1. Threat conditions
1.3.2.3.3.4.2.1.1.2. Control-ability conditions
1.3.2.3.3.4.2.1.2. Required conditions for maintaining authority
1.3.2.3.3.4.2.1.2.1. Threat situation
1.3.2.3.3.4.2.1.2.2. Control-ability conditions

1.3.2.3.3.4.2.1.3. Required conditions for withdrawing authority
1.3.2.3.3.4.2.1.3.1. Changing threat situation
1.3.2.3.3.4.2.1.3.2. Changing control-ability conditions
1 .3.2.3.3A.3. Inadequate management of "restrictive states"
1.3.2.3.3.4.3.1. Communication procedures for initiating requests to engage
1.3.2.3.3.4.3.2. Procedures for establishing agreement
1.3.2.3.3.4.3.3. Procedures for resetting authority
1.3.2.3.3.5. Inadequate consideration of implementation constraints
1.3.2.3A. Inadequate enforcement of engagement rules
1.3.2.3.4.1. Inadequate situation awareness - monitoring of critical conditions
1.3.2.3.4.1.1. Indicators of need to change restrictive level
1.3.2.3.4.1.2. Indicators of need to change restrictive state
1.3.2.3.4.2. Inadequate capability to effect change
1.3.2.3.42.1. Changing restrictive level within restrictive state control
1.3.2.3.4.2.2. Changing restrictive state

APPENDIX C

SAFETY CONCERNS NOT SPECIFICALLY ANALYZED

Lateral Stability and Patch Saturation

The majority of this investigation involved longitudinal control associated with separation management. In the analyses performed, braking capability is the major factor, and concerns were expressed regarding the ability to account for variables that influence the maximum capability. This was the central focus of appendix A. Of particular concern were the variables that posed intrinsic threats—variables that could experience changing values during a trip that, in turn, could reduce maximum braking capability. These same concerns exist for lateral control. The concern is particularly the ability to detect when water, snow, or other friction reducing variables can lead to a loss of lateral stability (e.g., hydroplaning).

Further, since lateral and longitudinal resting forces applied by the road must utilize the same tire/road "patch," are there conditions where saturation may exist (e.g., wind gusts, combined braking and cornering)? Obviously, lateral stability must take precedent over braking in its share of the patch capabilities. This is the concept behind ABS. While ABS may have positive braking rate influences, its primary function is to effectively utilize the capabilities, essentially limiting the combined forces of braking and lateral control to the maximum capability of the patch. In this negotiation, the braking vector is always the loser. ABS was designed to ensure that priority of patch capability be given to generating forces to maintain lateral control. This introduces a problem in selecting the maximum braking capability of a vehicle. Must we account for some patch allocation rule to ensure that safe separation is not based on a braking capability that will not exist?

Side-swipe Accidents

Our analysis was directed toward in-line collisions. Threats posed from vehicles in adjacent lanes were limited to lane intrusion and were treated as a merge or sudden intrusion threat. In either case, threat management dealt with a threat agent appearing in the AHS lane, and the control responses were invoked by the separation management function. In reality, this should be a longitudinal separation manager. In situations where a vehicle is exposed to parallel lane operation, particularly a manual parallel lane, can we develop the capability to provide lateral separation management? The sensing involved could be problematical. We could always be in contact with a parallel vehicle. When do we declare a "side-swipe imminent" situation? How close is too close? Can we adjust lane position by introducing some offset centerline to accommodate wandering vehicles in a parallel lane?

This problem may not be as critical for urban applications, or at least, applications considering physical lane barriers. But this is an unlikely option in rural applications.

APPENDIX D

REPRESENTATIVE SYSTEM CONFIGURATIONS

For the purpose of this document, the research team considered four primary representative system configurations (RSCs). Detailed descriptions of these RSCs can be found in the AHS Precursor Systems Analyses Overview Report. Only the characteristics of these RSCs relative to the research in this activity area are contained herein.

In general terms, the RSCs can be summarized as follows:

Representative system configurations.

RSC	Traveling Unit	Headway Policy	Vehicle Intelligence	Guideway Intelligence
1. Average Vehicle Smart Highway	Individual Vehicle	Uniform	Average	Active
2. Smart Vehicle Average Highway	Individual Vehicle	Platoon	Autonomous	Passive
3. Smart Pallet Average Highway	Pallet	Uniform	Autonomous	Passive
4. Smart Vehicle Passive Highway	Individual Vehicle	Independent	Autonomous	Passive
Note: [1]RSC 2 consists of three lane configuration variations, resulting in a total of six specific RSCs.				

Each RSC used in this research requires a specific definition of the associated roadway configuration. Three of the four primary RSCs (i.e., 1, 3, 4) were assigned only one roadway configuration, and one of the RSCs (i.e., 2) was assigned three different roadway configurations. The result is a total of six variations of the four primary RSCs, described by their *mainline, AHS access,* and *separation characteristics*.

Mainline

None of the RSCs investigated in this research effort involved a roadway which is completely AHS for all lanes, with no provisions for non-AHS vehicles. However, three distinctly different mainline roadway configurations were associated with the target RSCs and considered:

1. Two lanes in each direction, with the left lane in each direction serving mixed AHS and non-AHS traffic.

2. Three lanes in each direction with the left lane in each direction serving only AHS traffic.

3. Two lanes in each direction serving non-AHS traffic and a reversible lane between the non-AHS lanes serving only AHS traffic.

AHS Access

Access to the lane in which AHS is provided can involve a variety of entry/exit designs, some of which require maneuvering through non-AHS traffic to get to the AHS lane. Others simply provide direct access to the AHS lane via an exclusive ramp system.

For the sake of this research, entry and exit facilities were addressed only at a high level to determine compatibility with roadway design strategies. The main interest in entry/exit for this effort is simply to acknowledge whether a ramp system is on the left or right side of a lane set, spacing between terminals, and whether the ramp is intended for mixed or exclusive AHS flows. Other research teams have conducted detailed studies of entry/exit facilities (Area J—Entry/Exit Analysis) and their deployment, and have documented those results in other reports.

The following AHS lane access components were considered germane to the RSCs in this research:

1. Mixed Ramps—AHS vehicle enters/exits the freeway facility by using the same ramp facilities as non-AHS vehicles. Special lanes may be provided for AHS vehicles on the ramps to facilitate check-in and check-out, but the AHS vehicle must maneuver through non-AHS lanes when traveling between the AHS lane and the ramp system.

2. Exclusive Ramps—All entry and exit points serving the AHS are provided by ramps intended exclusively for the use of AHS vehicles only and are physically located such that no maneuvers by AHS vehicles through non-AHS traffic are necessary to reach the AHS lane.

3. Transition Lane—Similar to the mixed ramp concept where AHS and non-AHS vehicles utilize the same ramps, but includes a transition lane located adjacent to the AHS lane. The transition lane is used for maneuvers into and out of the AHS lane. Traffic flow in the transition lane may be AHS only or mixed flow, and AHS vehicles must maneuver through non-AHS lanes and traffic to reach the AHS lane.

Lane Separation

The means by which separation of AHS and non-AHS traffic is accomplished is closely associated with how entry/exit may be accomplished. In terms of the RSCs considered for this research, the following two concepts were considered:

1. None—Separation of AHS and non-AHS traffic is accomplished by signing and striping only.

2. Barrier—Physical barrier used to separate AHS and non-AHS traffic streams along the length of the AHS lane.

Using these characteristics, the resulting six variations of the four primary RSCs are summarized as follows:

Global RSC characteristics.

RSC	Mainline Roadway Configuration	AHS Lane Access			Lane Separation	
		Mixed	Exclusive Ramps	Transition Lanes	None	Barriers
1	3 Lanes each direction Exclusive AHS Lt. lane	X		X	X	
2A	3 Lanes each direction Exclusive AHS Lt. lane	X			X	
2B	3 Lanes each direction Exclusive AHS Lt. lane		X			X
2C	2 Non-AHS lanes each direction Reversible excl. AHS center lane		X			X
3	3 Lanes each direction Exclusive AHS Lt. lane		X			X
4	2 Lanes each direction Mixed traffic Lt. lane	X			X	

The graphics on the following sheets illustrate the general roadway configurations of the six variations of RSCs used in this research. The basic assumptions as to how each RSC would operate in summarized in the following table. Detailed descriptions of characteristics beyond the roadway deployment characteristics may be found in the AHS precursor systems analyses overview report.

RSC assumptions.

Parameter	RSC 1	RSC 2	RSC 3	RSC 4
Vehicle Type	Individual Passenger Car	Individual Passenger Car	Single Car Pallet, Automatic Control Only	Individual Passenger Car
Headway Policy	Uniform	Platoon	Uniform	Independent
Vehicle Intelligence	Good	Smart	Smart	Very Smart
Roadway Intelligence	Good	Average	Average	Dumb
Lane Configuration	Mixed traffic on inside AHS lane with manual traffic on outside lane	Dedicated AHS lane(s) with transition lane and manual lane(s)	Dedicated reversible AHS lane with pullover space adjacent to AHS lane	All lanes mixed traffic
Barriers	None	None	Between AHS and Non-AHS Lanes Only	None
Entry/Exit Ramps	Current Type	Current Type	Current Types for Non-AHS Dedicated for AHS	Current Type
Transition to AHS	Where: In AHS lane When: At driver command after sector control OK How: Manual switch	Where: In Transition Lane When: At driver command after sector control OK How: Manual switch	Where: In Pallet Attach & Detach Area When: Upon link to pallet How: Automatic with link	Where: In AHS lane When: At driver command after sector control OK How: Manual switch
Check-Out of AHS Vehicle Systems	Combination of periodic certification and polling of internal sensors	Combination of periodic certification and polling of internal sensors	Pallets under control of central authority—Inspected before allowing on AHS	Combination of periodic certification and polling of internal sensors
Failure to Transition Results In:	Driver must continue under manual control	Driver must continue under manual control in transition lane or re-enter manual lane	Essentially cannot fail to transition unless driver refuses to enter destination	Driver must continue under manual control

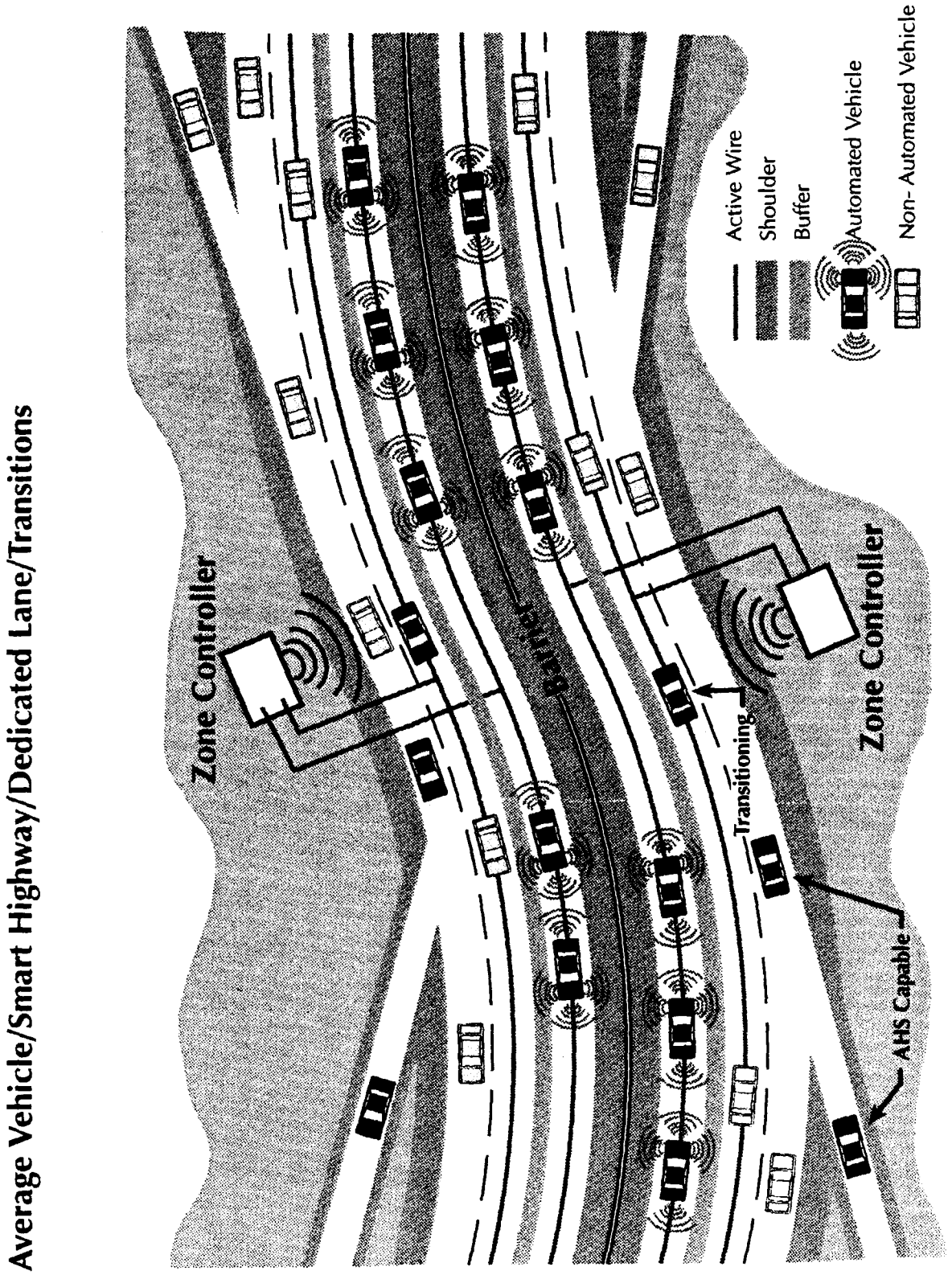


Figure 1. RSC 1.

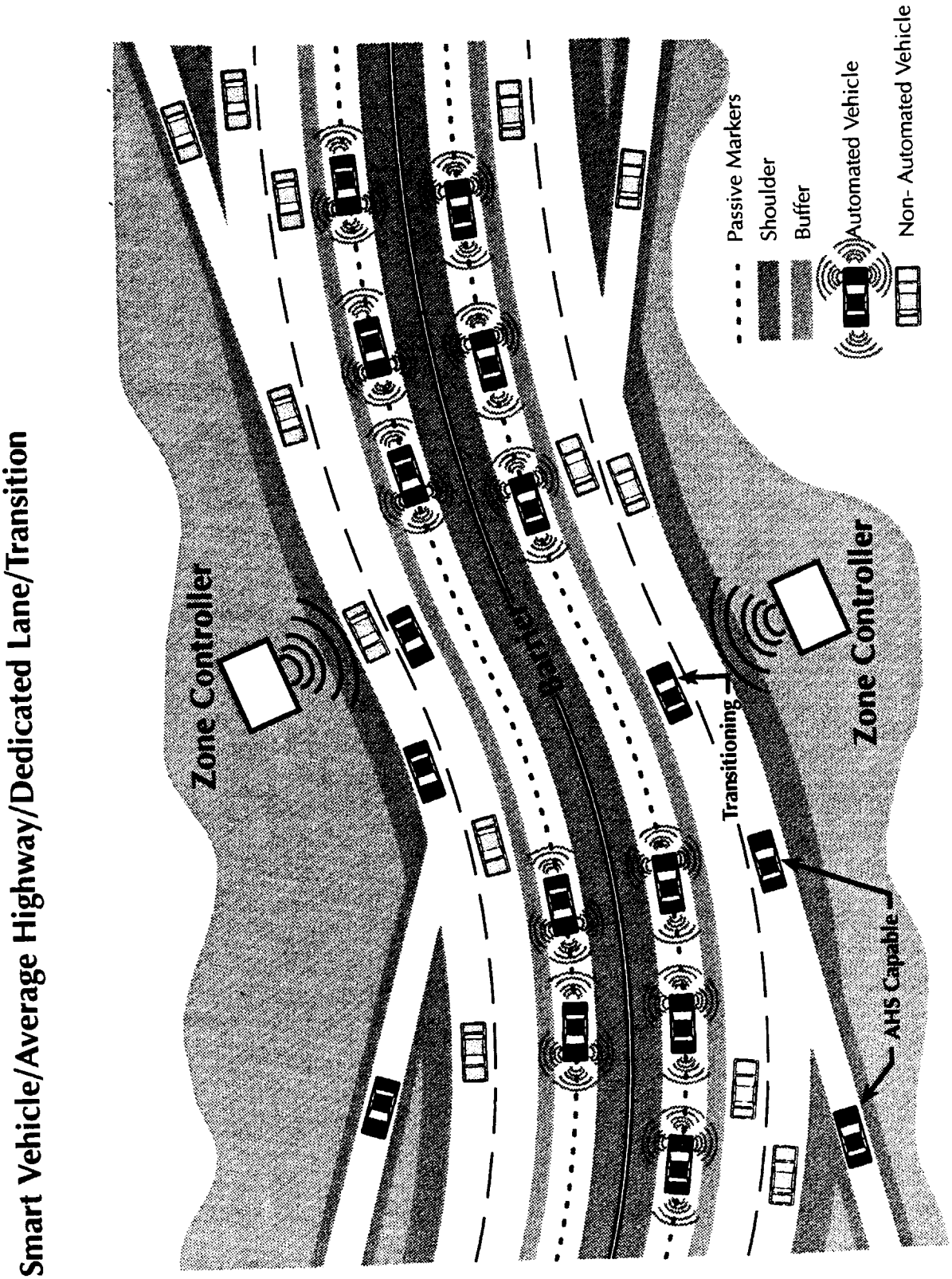


Figure 2. RSC 2A.

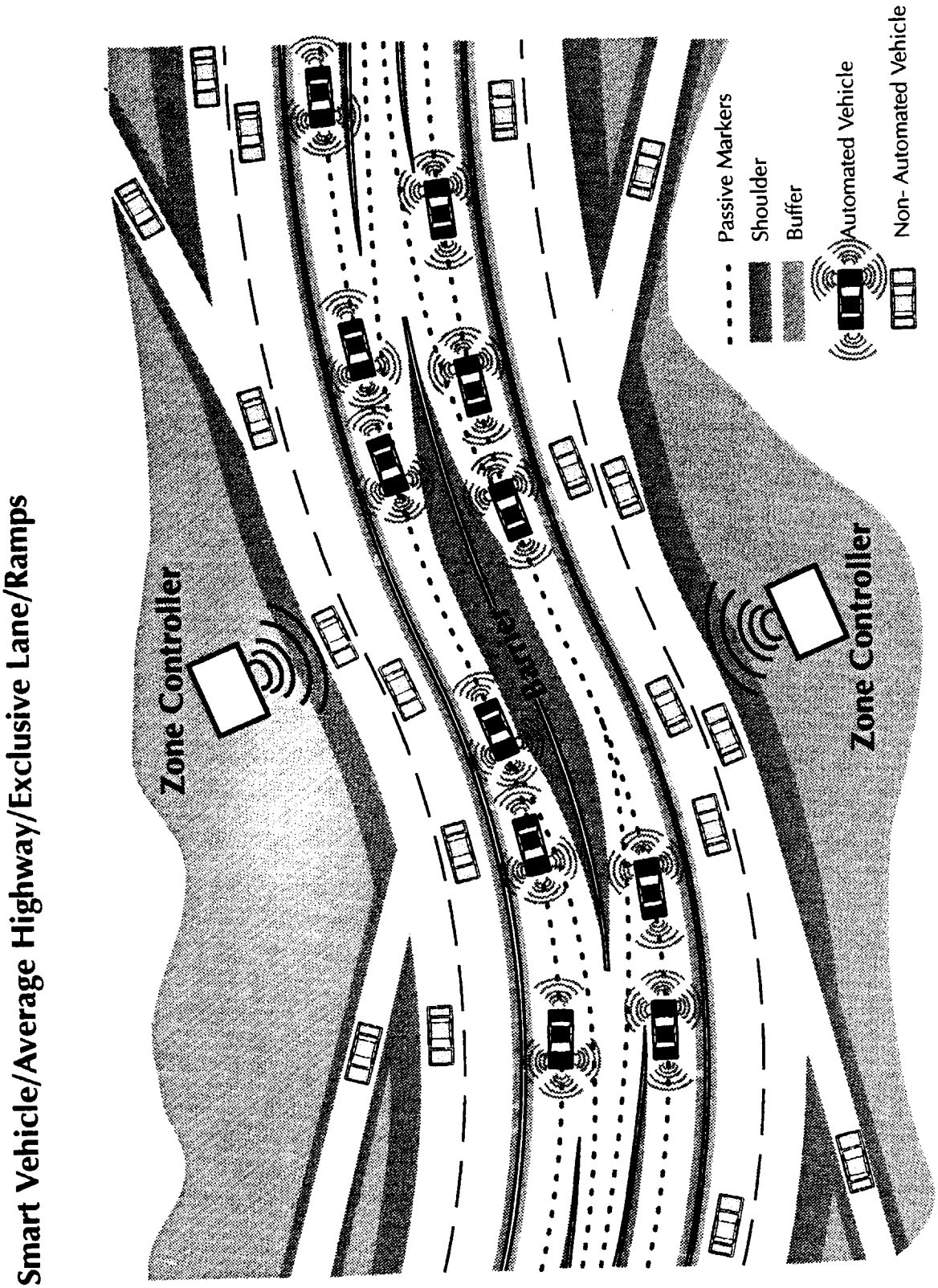


Figure 3. RSC 2B.

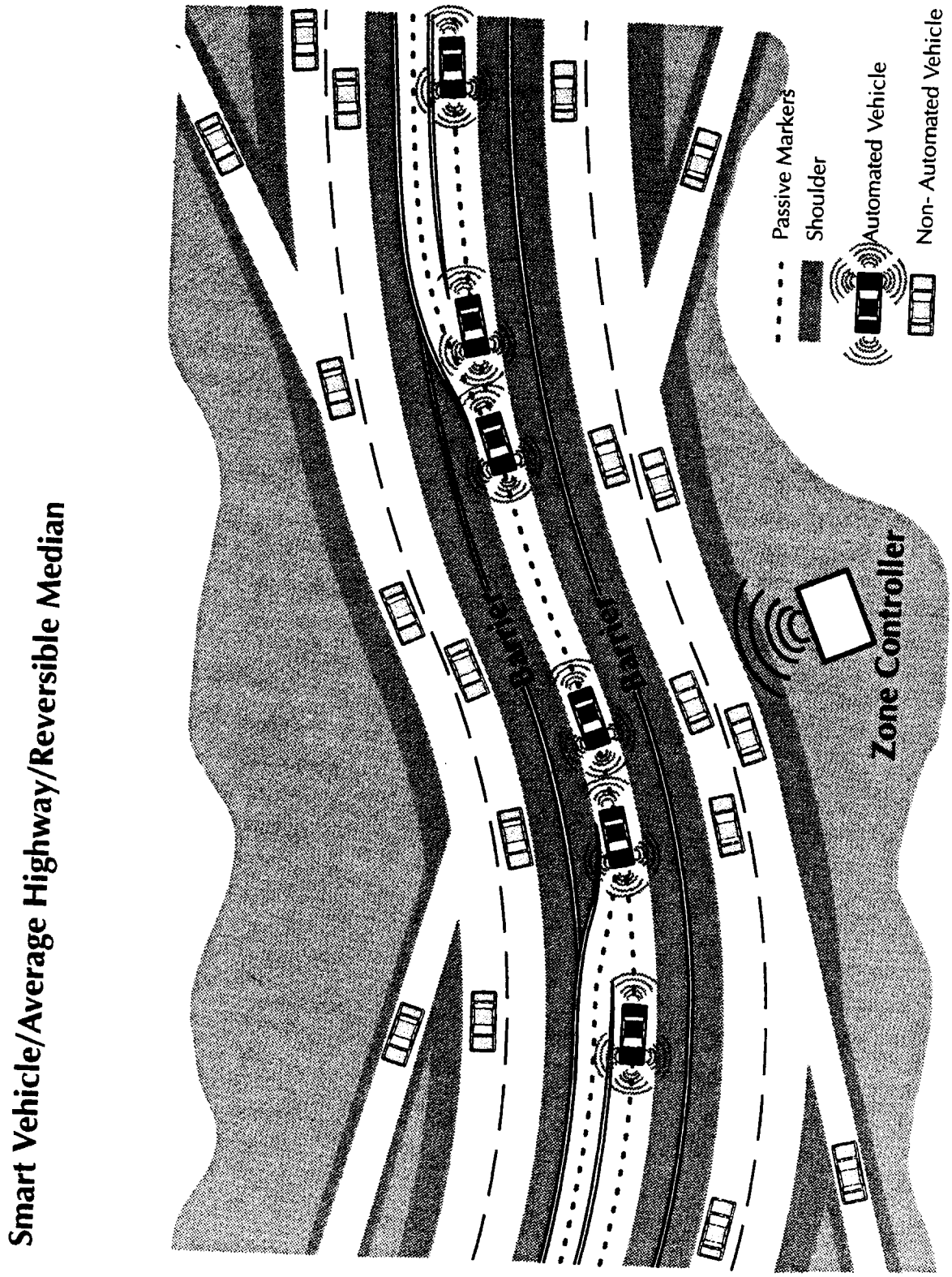


Figure 4. RSC 2C.

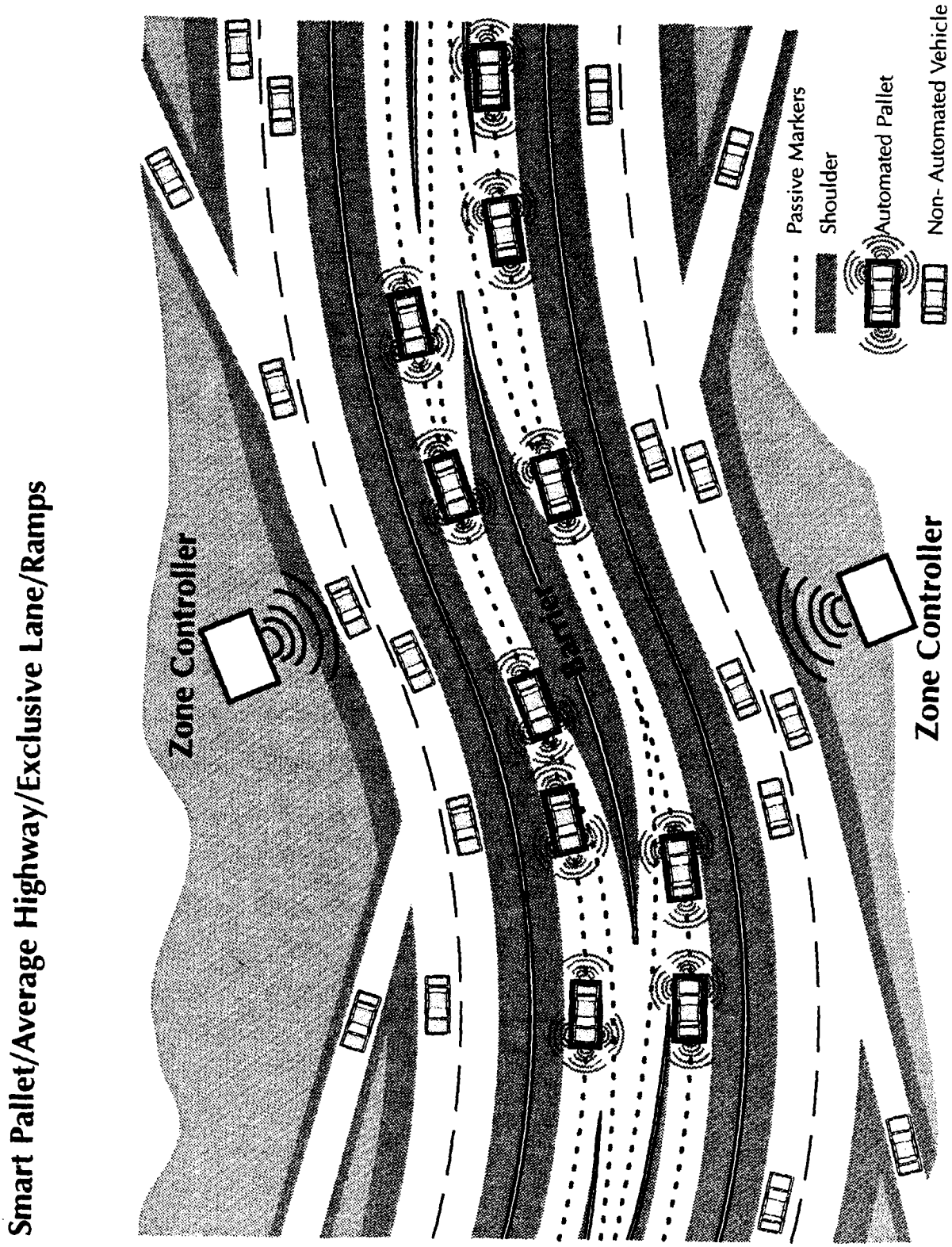


Figure 5. RSC 3.

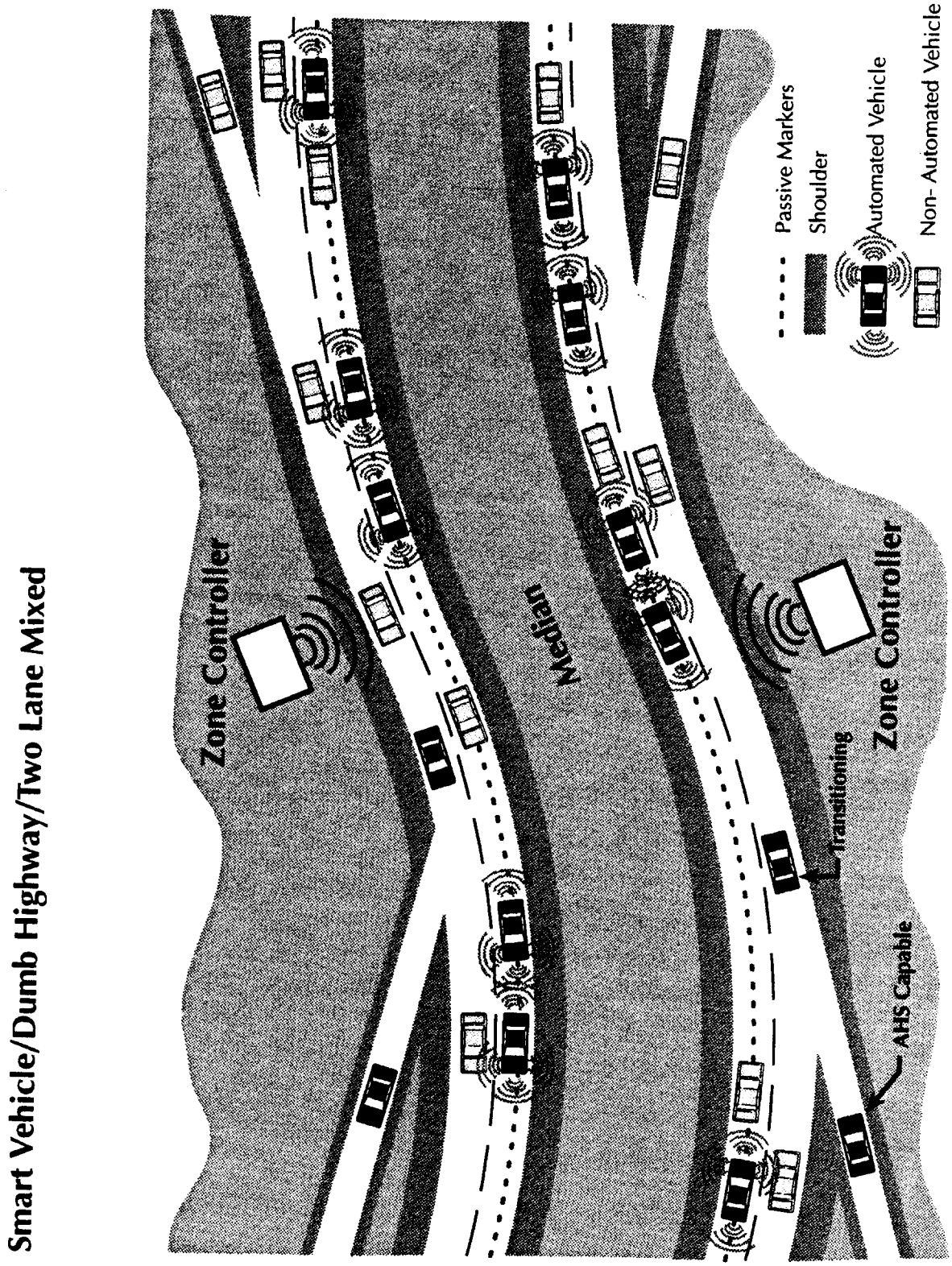


Figure 6. RSC 4.