Title

Major Failure Events of Automated Highway Systems: Three Scenarios from the Driver's Perspective

Authors

Tsao, H.-S. Jacob
Plocher, Thomas A.
Zhang, Wei-Bin
et al.

Publication Date

1997-02-01

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

Major Failure Events of Automated Highway Systems: Three Scenarios from the Driver's Perspective

H.-S. Jacob Tsao, Thomas A. Plocher, Wei-Bin Zhang, Steven E. Shladover

California PATH Working Paper
UCB-ITS-PWP-97-4

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

February 1997

ISSN 1055-1417

MAJOR FAILURE EVENTS OF AUTOMATED HIGHWAY SYSTEMS:

THREE SCENARIOS FROM THE DRIVER'S PERSPECTIVE

H.-S. Jacob Tsao
PATH Program, Institute of Transportation Studies, University of California, Berkeley

Thomas A. Plocher
Honeywell Technology Center, Minneapolis, Minnesota

Wei-Bin Zhang
Steven E. Shladover
PATH Program, Institute of Transportation Studies, University of California, Berkeley

ABSTRACT

Automated Highway Systems (AHS) have the potential for offering large capacity and safety gains without requiring significant amounts **of** additional right-of-way. Since the general public will be the users of the AHS, human factors must play a pivotal role in the research and development of AVCS technologies and AHS operation. In two companion reports, three attributes critical to AHS human factors were identified and seven scenarios featuring variations in these attributes proposed. To ensure the identification of all major ***compounding*** attribute combinations, detailed operational events, from the perspective of the driver, were identified. This paper focuses on failure events, where a failure event is defined to be the occurrence of a functional failure during a normal operational event.

After briefly reviewing the seven "first-generation" scenarios, this report first describes the criteria for selecting the three "second-generation" scenarios and then reports the selection result. While examining each of the normal operational events identified for the three scenarios, we identify possibly multiple major failure events by assuming the failure of ***one*** operational function at a time. Failure events resulting from the failure of multiple operational functions can be inferred. For each failure event, we also define possible failure consequences and possible system responses to resolve the failure event. These second-generation scenarios are selected for studying AHS human factors and are *not* being advocated by the authors as the better deployment choices among the seven first-generation scenarios, even

from the human-factors point-of-view. Similarly, the responses provided for the major failure events are not being advocated as the better ones. Rather, to truly identify human capability in failure/emergency situations and not to rule out possible human abilities prematurely, we tend to stretch the limit **of** human capability in the responses. The true human capability is a crucial subject for future investigation.

KEY WORDS: Automated Highway Systems (AHS), Advanced Vehicle Control Systems (AVCS), Human Factors, Normal Operational Events, Failure Events

MAJOR FAILURE EVENTS OF AUTOMATED HIGHWAY SYSTEMS: THREE SCENARIOS FROM THE DRIVER'S PERSPECTIVE

H.-S. Jacob Tsao

Thomas Plocher

Wei-Bin Zhang

Steven E. Shladover

EXECUTIVE SUMMARY

IMPORTANCE OF AHS HUMAN FACTORS

Automated Highway Systems (AHS) have the potential for offering large capacity and safety gains without requiring significant amounts of additional right-of-way. Recent advances in key Advanced Vehicle Control Systems (AVCS) technologies have shown the potential of highway automation. Given these advances, an opportune and challenging area **of** research is how to operate an AHS. The Federal Highway Administration (FHWA) has initiated a series of "Precursor Systems Analyses of Automated Highway Systems" to encourage research in this area. Since the general public will be the users **of** the AHS, human factors must play a pivotal role in the research and development of AVCS technologies and AHS operation. The FHWA has sponsored a research project "Human Factors Design of Automated Highway Systems" led by Honeywell Inc., for which the California PATH program at UC Berkeley serves as a subcontractor.

THE HUMAN FACTORS PROJECT

The research project consists **of** 16 tasks, Tasks A through **P.** The objective of Task A is to define and characterize, in terms of operational scenarios, a limited number of visions for an AHS. Task A has 9 components, Tasks A.l through A.9. Task A.2 (Develop First Generation Scenarios) calls for the

development of at least six fully automated AHS scenarios. Six such scenarios and a scenario with partial automation have been documented in [4,5]. Detailed lists of normal operational events for the six fully automated AHS scenarios can be found in [4].

THE FOCUS OF THIS REPORT

Task A.7 (Develop Second Generation Scenarios) selects three scenarios from the seven first-generation scenarios and, for each of the selected scenarios, provides enough detail *so* that all operational events having major human factors implications, including normal as well as failure events, can be identified. This report documents in detail the research findings for that Task.

The scenario descriptions [4,5] and the lists of normal operational events [4] for the seven first-generation scenarios already contain sufficient details about their normal operation for the human factors project. However, only a preliminary study on vehicle/system failures was performed in Task **A.2.** Therefore, we concentrate on and report only about the failure event analysis in this paper.

TECHNICAL BACKGROUND

The proper operation **of** an AHS hinges on the proper operation of (1) all vehicles in the AHS, (2) means of communication between the roadside control system and all the vehicles in the AHS, *(3)* roadside control system, (4) roadway support **of** automation (e.g. lane markings, lane lines for vision-based systems or magnetic markers for magnetic-field-sensing systems, for lane tracking), *(5)* roadway support for driving, (e.g. roadways free of debris and satisfactory road surface), and *(6)* driver participation. The proper operation of each of the above requires the proper operation of the supporting functions, each of which contributes to the proper AHS operation. A failure event is defined to be the occurrence of a functional failure during a normal operational event.

Given the plethora of normal operational events specified for the six fully automated AHS operating scenarios, Zhang et al. **[6]** defined two types of functions to abstract the scenarios for a more generalized AHS functional analysis: operational functions and elemental functions. These functions are

derived so that each normal operational event specified in [4] can be represented as a combination of some of the operational functions and each operational function is supported by a specific combination of some of the elemental functions. We adopt the function definitions given in **[6]** and use the failure of individual ***operational*** functions for identifying the failure events.

Zhang et al. ***[6]*** also identified the following four major system components, across which the elemental functions are distributed. (i) Traffic management center: responsible for providing route recommendations for traffic flow control. (ii) Roadside coordination equipment: responsible for defining paths for individual vehicles and coordinating vehicle movements. (iii) Vehicle: responsible for controlling lateral and longitudinal movements of a vehicle, and (iv) Human driver: responsible for maneuvering the vehicle during manual driving and transition and for information monitoring during automated driving.

THE SCOPE OF THIS **PAPER**

We identify major failure events by assuming the failure of ***one*** supporting ***operational*** function during a normal operational event. Since the failure of an ***elemental*** function may cause the simultaneous failure of multiple operational functions during ***one*** normal operational event, the true impact of an elemental function failure on the driver can be accurately studied only if the consequences of and the responses to the operational function failures are combined. For example, the failure of the elemental function "sensing", which is currently not broken down to "sensing for lateral control" and "sensing for longitudinal control", would lead to a simultaneous failure of the operational functions "lane tracking function" and "headway regulation function", which would in turn lead to "loss of both lane tracking control and headway control" during the (single) normal operational event "maintaining safety distance with the vehicle in front while moving along the current lane". Note that there may be a ***vast*** number of such "compound" failure events. **To** limit the scope of this report, we chose ***not*** to use the failure of ***elemental*** functions as the key to identifying possible failure events. However, with the information provided in this report, the compound failure events can be derived or inferred.

For the same reason, we do not systematically address the possibility and result of simultaneous failure

of multiple operational functions. However, we will identify and discuss particularly ***dangerous*** and human-factors-impacting events like "loss of all automatic control" that either are equivalent to or could result from a simultaneous failure of multiple operational functions.

A normal operational event may require more functional support than what the event statement [4,5] explicitly addresses. For example, a simple event like "vehicle moves along its current lane at the target speed" requires the absence of any debris on the roadway. A complete description of all possible failure events is beyond the scope of this project. We only provide the ones that may have major human factors implications.

A possible system ***response*** to a failure event may include both automated reactions by the vehicle/roadside as well as drivers' participation. Both are **AHS** system functions and can be regarded as "emergency functions", as opposed to the normal AHS system functions. Note that they would fail just as the functions supporting normal AHS operation. To further limit the scope of this report, we do ***not*** address the events resulting from the failures of these "emergency functions".

A vehicle function may be a manual vehicle function (e.g. manual braking, propulsion and steering) or an automated vehicle function (e.g. automated headway/speed control and automated steering), of which some manual vehicle functions are an integral part. To focus on the consequences of automation failures and on the potential role of the drivers in resolving the failure events, we do not consider the failure of any manual vehicle functions. In other words, when the driver is expected to take over vehicle control after certain automation failures, the manual vehicle functions (excluding the drivers' participation) are always assumed operational.

APPROACH:

After briefly reviewing the seven first-generation scenarios, this report first describes the criteria for selecting the three second-generation scenarios and then reports the selection result. While examining each of the normal operational events identified for the three scenarios [4], we identify possibly multiple major failure events by assuming the failure of ***one*** supporting operational function, as defined in

[6], at a time.

To derive all the major failure events resulting from the ***single*** failure of ***one*** specific ***elemental*** function, the reader needs to (i) identify the operational functions which will fail as a result of the (single) elemental function failure, and (ii) while examining each normal operational event [4,5], identify possibly multiple failure events by assuming one arbitrary combination of the operational function failures at a time.

SUMMARY OF **RESULTS**

The selected scenarios are: **(1)** Mixed-Traffic Lanes (with manual vehicles and automated vehicles sharing the same lane) with Autonomous Vehicles Capable of Automated Lane-Flow, **(2)** Segregated Highway (without mixing automated traffic with manual traffic) with Free-Agent Vehicle Following, and **(3)** Shared Highway (with dedicated automated lanes) with Lane Barriers and Platooning.

For each of the three scenarios, we list the representative major failure events. (See THE SCOPE OF **THIS** PAPER.) For each failure event, we also define possible failure consequences and possible system responses to resolve the failure event. In addition, we provide the set of elemental functions that may contribute to the failure of the operational functions that cause the failure event. We also point out, for each failure event, the corresponding normal operational event.

These generation scenarios are selected for studying AHS human factors and are *not* being advocated by the authors as the better deployment choices among the seven first-generation scenarios, even from the human factors point **of** view. Similarly, the responses provided for the major failure events are not being advocated as the better ones. Rather, to truly identify human capability in failure/emergency situations and not to rule out possible human abilities prematurely, we tend to stretch the limit of human capability in the responses. The true human capability will be the subject of investigation at a later stage of this project.

ORGANIZATION OF THE PAPER

After briefly summarizing the seven first-generation AHS operating scenarios, Section 2 first discusses the criteria for selecting the second-generation scenarios and then describes the three selected scenarios. Section 3 summarizes our approach to the failure event analysis and explains the rationale. Section 4 describes, for each of the three second-generation scenarios, the major failure events. For each such event, we identify the (single) operational function that causes the failure event, possible (multiple) elemental functions causing the operational function failure, possible consequences of the failure event and finally some possible system responses. Section 5 concludes the report.

MAJOR FAILURE EVENTS OF AUTOMATED HIGHWAY SYSTEMS: THREE SCENARIOS FROM THE DRIVER'S PERSPECTIVE

(1) INTRODUCTION

IMPORTANCE OF AHS HUMAN FACTORS

Automated Highway Systems (AHS) have the potential for offering large capacity and safety gains without requiring significant amounts of additional right-of-way. Recent advances in key Advanced Vehicle Control Systems (AVCS) technologies have shown the potential of highway automation. Given these advances, an opportune and challenging area of research is how to operate an AHS. The Federal Highway Administration (FHWA) has initiated a series of "Precursor Systems Analyses of Automated Highway Systems" to encourage research in this area. Since the general public will be the users of the AHS, human factors must play a pivotal role in the research and development of AVCS technologies and AHS operation. The FHWA has sponsored a research project "Human Factors Design of Automated Highway Systems" led by Honeywell Inc., for which the California PATH program at UC Berkeley serves as a subcontractor.

THE HUMAN FACTORS PROJECT

The research project consists of 16 tasks, Tasks A through P. The objective of Task A is to define and characterize, in terms of operational scenarios, a limited number of visions for an AHS. Task A has 9 components, Tasks A.1 through A.9. Task A.2 (Develop First Generation Scenarios) calls for the development of at least six fully automated AHS scenarios. Six such scenarios and a scenario with partial automation have been documented in [5]. Detailed lists of normal operational events for the six fully automated AHS scenarios can be found in [4].

THE FOCUS OF THIS PAPER

Task A.7 (Develop Second Generation Scenarios) selects three scenarios from the seven first-generation

scenarios and, for each of the selected scenarios, provides enough detail *so* that all operational events having major human factors implications, including normal as well as failure events, can be identified. This report documents in detail the research findings for that Task.

The scenario descriptions [4,5] and the lists of normal operational events *[5]* for the seven first-generation scenarios already contain sufficient details about their normal operation for the human factors project. However, only a preliminary study on vehicldsystem failures was performed in Task A.2. Therefore, we concentrate on and report only about the failure event analysis in this paper.

TECHNICAL BACKGROUND

Given the plethora of normal operational events specified for the six fully automated *AHS* operating scenarios, Zhang et al. **[6]** defined two types of functions to abstract the scenarios for a more generalized AHS functional analysis: operational functions and elemental functions. These functions are derived *so* that each normal operational event specified in [4] can be represented as a combination of some of the operational functions and each operational function is supported by a specific combination of some of the elemental functions. We adopt the function definitions given in *[6]* and define a failure event to be the occurrence of a functional failure during a normal operational event.

THE SCOPE OF THIS PAPER

We identify major failure events - the failure events that may have major human factors implications - by assuming the failure of *one* supporting *operational* function during a normal operational event. Although we do not systematically address the possibility and result of simultaneous failure of multiple operational functions, we will identify and discuss particularly *dangerous* and human-factors-impacting events like "loss of all automatic control" that either are equivalent to or could result from a simultaneous failure of multiple operational functions. To resolve the failure events safely, automated "emergency" vehicle/system functions may be required. To further limit the scope of this report, we do *not* address the events resulting from the failures of these "emergency functions". To focus on the consequences of automation failures and on the potential role of the drivers in resolving the failure events,

we do not consider the failure of any manual vehicle functions.

SUMMARY OF RESULTS

The selected scenarios are: **(1)** Mixed-Traffic Lanes (with manual vehicles and automated vehicles sharing the same lane) with Autonomous Vehicles Capable of Automated Cruising, **(2)** Segregated Highway (without mixing automated traffic with manual traffic) with Free-Agent Vehicle Following, and **(3)** Shared Highway (with dedicated automated lanes) with Lane Barriers and Platooning.

For each of the three scenarios, we list the representative major failure events. For each failure event, we also describe possible failure consequences and example system responses to resolve the failure event. In addition, we provide the set of elemental functions that may contribute to the failure of the operational functions that cause the failure event. We also point out, for each failure event, the corresponding normal operational event. We also point out how to derive the failure events resulting from the failure of one ***elemental*** function failure.

These scenarios are selected for studying ***AHS*** human factors and are ***not*** being advocated by the authors **as** the better deployment choices among the seven first-generation scenarios, even from the human factors point of view. Similarly, the responses provided for the major failure events are not being advocated **as** the better ones. Rather, to truly identify human capability in failure/emergency situations and not to rule out possible human abilities prematurely, we tend to stretch the limit of human capability in the responses. The true human capability will be the subject of investigation at a later stage of this project.

ORGANIZATION OF THE PAPER

After briefly summarizing the seven first-generation ***AHS*** operating scenarios, Section 2 first discusses the criteria for selecting the second-generation scenarios and then describes the three selected scenarios. Section **3** summarizes our approach to the failure event analysis and explains the rationale. Section **4** describes, for each of the three second-generation scenarios, the major failure events. Section ***5*** con-

cludes the report.

(2) THE THREE SECOND-GENERATION SCENARIOS

After briefly summarizing three critical design issues for human factors in fully automated AHS and the seven first-generation AHS operating scenarios, this section first discusses the criteria for selecting the second-generation scenarios and then describes the selected three.

(2.1) Three Critical Design Issues for Human Factors in Fully Automated AHS

The seven first-generation operating scenarios [5] consist of one partially automated AHS and six fully automated AHS. The partially automated AHS was selected to highlight not only a possible eventual AHS deployment but also a possible evolutionary step towards full automation. Tsao et al. [4] evaluated many AHS design options and identified the following three as the most important attributes for AHS human factors: (1) separation of automated traffic from the manual traffic, (2) separation among automated traffic, and (3) the vehicle-following (longitudinal-separation) rule for the automated traffic. Each of these three major attributes has two major options. We now briefly discuss these options.

Physical Isolation of Automated Traffic

Separation between the automated traffic and the manual traffic, if at all, may be achieved by physical barriers or traffic regulations. In a segregated automated system, automated traffic is ***physically isolated*** from the manual traffic and only automated vehicles can enter such a system. A lower degree of separation would be achieved if certain consecutive lanes are dedicated to the automated traffic and no manual vehicles are allowed on them. In such a system, a lane between the automated lanes and the manual lanes, called the transition lane, is needed for vehicles to transition between manual and automatic control. (Note that, to enable continuous automated driving from one highway to another, eight additional connector ramps dedicated to only the automated traffic would have to be built.) A system without separation would have no dedicated lanes for automated traffic, and automated vehicles and manual vehicles would share all the lanes together. This issue has great impact on safety, capacity,

driver acceptance, etc.

Lane Barriers

Two major options for separation among the automated traffic are physical lane barriers and logical non-barrier markings. Since AHSs are expected to operate with short spacing among automated vehicles, a failure of an automated vehicle has the potential of creating multiple serious collisions. Since the automated vehicles involved in even a minor collision (or their debris) may skid, spin or sway into a neighboring lane, a major collision may result. Motivated by these concerns, Hitchcock [1] proposed the erection of barriers between lanes. Three different degrees of physical separation are: no barriers at all, barriers between the transition lane and the neighboring automated lane only, and barriers between any two adjacent automated lanes as well. Concomitant with the existence of lane barriers is the necessity of openings for vehicles to change lanes when necessary. The barriers may decrease the *lateral capacity* of an AHS significantly. If a vehicle hits one end of a barrier, a serious accident may result. Although changing lanes will be automated, passing through these openings, as well as the mere existence of these barriers, may have psychological impacts on the drivers and passengers.

Platooning vs. Free-Agent Longitudinal Separation (Vehicle-Following)

Two basic vehicle-following (longitudinal-separation) rules are the ***platooning rule*** and the ***free-agent rule.*** The platooning rule was first proposed and studied by Shladover in the late 70's [2] and has received renewed attention in the last few years. Under this rule, two adjacent vehicles in the same lane are kept either very close to, or very far from, each other. As a result, vehicles are organized in a clustered formation. Each cluster of vehicles is called a ***platoon.*** This rule fully utilizes the fact that, after a failure, the relative speed of the two vehicles at the time of collision, if any, is small if they are either very close to each other or very far apart. Shladover [2] showed that the capacity increases significantly with platoon size. Under the free-agent rule, vehicles move without any clustered formation and the minimum longitudinal spacing is significantly longer than typical intra-platoon spacings, but significantly shorter than typical inter-platoon spacings. Tsao and Hall [3] developed a probabilistic

model and a software tool for analyzing AHS longitudinal collision/safety between two automated vehicles and used them to compare the two rules.

(2.2) The Seven First-Generation Scenarios

The six fully automated operating scenarios [4,5] feature different combinations of these three attributes. A critical assumption made in all six scenarios is that only one vehicle type is accommodated in the AHS. A common physical characteristic among these scenarios is the necessity of eight additional connector ramps dedicated to the automated traffic at each highway-to-highway intersection for both continuous automated driving and throughput efficiency. The seven scenarios [5] are:

(1) Mixed-Traffic Lanes (with manual vehicles and automated vehicles sharing the same lane) with Autonomous Vehicles Capable of Only Automated Cruising (but not lane-changing)

(2) Shared Highway without Barriers under Free-Agent Vehicle Following

(3) Shared Highway without Barriers under Platooning

(4) Shared Highway (with dedicated automated lanes) with Barriers and Free-Agent Vehicle Following

(5) Shared Highway with Barriers and Platooning

(6) Segregated Highway (without mixing automated traffic with manual traffic) with Free-Agent Vehicle Following

(7) Segregated Highway with Platooning

Note that the names of these seven scenarios are slightly different from those used in [5], but there should be no danger of confusion.

(2.3) The Criteria for the Selection of Second-Generation Scenarios

The criteria used in the selection process is as follows:

(1) There should be one partially automated operating scenario for the following reasons:

Compared to the fully automated AHS, the driver is much more involved in driving. In other words, he/she must assume many of the driving functions that are automated in fully automated AHS. In particular, hdshe has the task of switching driving modes (manual vs. automatic) rather frequently, especially in heavy traffic. (He/she has to switch to the manual driving mode to change lanes or overtake, and then switch back to automatic for automated driving.)

(Based on this criterion, Scenario 1 is selected and only two out of the six fully automated scenarios need to be selected.)

(2) The three major *AHS* attributes and the two major options for each attribute give rise to six major design characteristics: shared highway, segregated highway, barriers, no barriers, platooning and free-agent rule. **To** ensure that the impact of each of these six is examined in detail, each one should be included in at least one of the two selected fully automated scenarios.

(3) Since only two are to be selected, they should be the two extremes in terms **of** human factors implications, i.e. the most complex one and the simplest one from the view point **of** driver task and comfort. In this way, we can gauge the complexity of the middle ones by "interpolation". Also, if there are no major issues associated with the most complex one, there should be no major AHS human factors issues at all. However, if the simplest one reveals major issues, they need to be seriously examined and resolved **as** soon as possible.

(2.4) The Second-Generation Scenarios

Based on these criteria, we selected the following three scenarios: Scenario 1, Scenario **6,** and Scenario 5. Note that each of the six major AHS characteristics is included in exactly one fully automated scenario and the two fully automated scenarios are indeed the two extremes, with Scenario **6 as** the simplest one and Scenario 5 as the most complex one among the six.

For ease **of** future referencing, we label the three scenarios as follows, where the prefix **SS** stands for

Second-generation Scenario:

(SS1) Mixed-Traffic Lanes (with manual vehicles and automated vehicles sharing the same lane) with Autonomous Vehicles Capable of Only Automated Cruising (but not lane-changing)

(SS2) Segregated Highway (without mixing automated traffic with manual traffic) with Free-Agent Vehicle Following, and

(SS3) Shared Highway (with dedicated automated lanes) with Lane Barriers and Platooning.

Before listing failure events for the three selected scenario, we make the following remarks:

(1) The two fully automated operating scenarios are selected to study AHS human factors, and are *not* being advocated as the most desirable AHS operating scenario, even from the view-point of human factors.

(2) The partial automation scenario, i.e. Scenario SS1, may not increase the capacity of the freeway.

(3) BACKGROUND, SCOPE AND APPROACH OF THE FAILURE EVENT ANALYSIS

(3.1) Background

Failure Event: Functional Failure During a Normal Event

The proper operation of an AHS hinges on the proper operation of (1) all vehicles in the **AHS,** (2) means of communication between the roadside control system and all the vehicles in the AHS, **(3)** road-side control system, **(4)** roadway support of automation (e.g. lane markings, lane lines for vision-based systems or magnetic markers for magnetic-field-sensing systems, for lane tracking), ***(5)*** roadway support for driving, (e.g. roadways free of debris and satisfactory road surface), and ***(6)*** driver participation. The proper operation of each of the above requires the proper operation of the supporting functions, each of which contributes to the proper AHS operation. **A** failure event is defined to be the occurrence **of** a functional failure during a normal operational event.

Functions: Operational and Elemental

Given the plethora of normal operational events specified for the six fully automated AHS operating scenarios, Zhang et al. **[6]** defined two types of functions to abstract the scenarios for a more generalized **AHS** functional analysis: operational functions and elemental functions. These functions are derived *so* that each normal operational event specified in **[4]** can be represented as a combination of some of the operational functions and each operational function is supported by a specific combination of some of the elemental functions. We adopt the function definitions given in **[6]** and use the failure of individual ***operational*** functions **for** identifying the failure events.

Distribution of Elemental Functions

Zhang et al. **[6]** also identified the following four major system components, across which the elemental functions are distributed. (i) Traffic management center: responsible for providing route recommendations for traffic **flow** control. (ii) Roadside coordination equipment: responsible for defining paths for individual vehicles and coordinating vehicle movements. (iii) Vehicle: responsible for controlling lateral and longitudinal movements of a vehicle, and (iv) Human driver: responsible for maneuvering the vehicle during manual driving and transition and for information monitoring during automated driving.

(3.2) The Scope of the Failure Event Analysis

Failure of One Operational Function

We identify major failure events by assuming the failure of ***one*** supporting ***operational*** function during a normal operational event. Since the failure of an ***elemental*** function may cause the simultaneous failure of multiple operational functions during ***one*** normal operational event, the true impact of an elemental function failure on the driver can be accurately studied only if the consequences of and the responses to the multiple operational function failures are combined. For example, the failure of the elemental function "sensing", which is currently not broken down to "sensing for lateral control" and "sensing for longitudinal control", would lead to a simultaneous failure of the operational functions "lane tracking function" and "headway regulation function", which would in turn lead to "**loss** of both lane tracking control and headway control" during the (single) normal operational event "maintaining safety distance with the vehicle in front while moving along a lane". Note that there may be a *vast*

number of such "compound" failure events. To limit the scope of this report, we chose *not* to use the failure of *elemental* functions as the key to identifying possible failure events. However, with the information provided in this report, the compound failure events can be derived or inferred.

For the same reason, we do not systematically address the possibility and result of simultaneous failure of multiple operational functions. However, we will identify and discuss particularly *dangerous* and human-factors-impacting events like "loss of all automatic control" that either are equivalent to or could result from a simultaneous failure of multiple operational functions.

Human-Factors-Impacting Failure Events Only

A normal operational event may require more functional support than what the event statement *[5]* explicitly addresses. For example, a simple event like "vehicle moves along a lane at the target speed" requires the absence of any debris on the roadway. Therefore, many failure events could occur during one normal operational event. A complete description of all possible failure events is beyond the scope of this project. We only provide the ones that may have major human factors implications.

No Failure of Emergency Functions

A possible system *response* to a failure event may include both automated reactions by the vehicle/roadside as well as drivers' participation. Both are AHS system functions and can be regarded as "emergency functions", as opposed to the normal AHS system functions. Note that they would fail just as the functions supporting normal AHS operation. To further limit the scope of this report, we do *not* address the events resulting from the failures of these "emergency functions".

Failure of Automated Functions Only

A vehicle function may be a manual vehicle function (e.g. manual braking, propulsion and steering) or an automated vehicle function (e.g. automated headway/speed control and automated steering), of which some manual vehicle functions are an integral part. To focus on the consequences of automation failures and on the potential role of the drivers in resolving the failure events, we do not consider the failure of any manual vehicle functions. In other words, when the driver is expected to take over vehicle control, total or partial, after certain automation failures, the manual vehicle functions (excluding the

drivers' participation) are always assumed operational.

Minimum Driver Responsibility

Driver intervention in AHS may be a hazard by itself. Therefore, it is considered only when drivers are in danger of fatality or injury and it has the potential of mitigating the danger. If drivers of automated vehicles are expected to participate in resolving any failure events, their training is required. Because of the lack of opportunity to practice in real traffic, drivers will likely forget their training before they actually need to use it. Therefore, we assume that their role should be simple and the required driver reactions should be ***small in number, simple in nature*** *and* ***natural in human reflex***. The true effectiveness and the potential hazard of driver intervention will be the focus of a later phase of this project.

A Basis for a Full-scale Failure Event Analysis

Scenario-specific assumptions will be made in the next section. All these assumptions are made to help focus this analysis on the major failure events and also to simplify the analysis. Note that they, together with the scope reductions made earlier in this section, can be used to identify the failure events not discussed in this report and the potential complexity of a full-scale failure event analysis.

(3.3) Approach

While examining each of the normal operational events identified for the three scenarios [4], we identify possibly multiple major failure events by assuming the failure of ***one*** supporting operational function, as defined in [6], at a time.

To derive all the major failure events resulting from the ***single*** failure of ***one*** specific ***elemental*** function, the reader needs to (i) identify the operational functions which will fail as a result of the (single) elemental function failure, and (ii) while examining each normal operational event [5], identify possibly multiple failure events by assuming one arbitrary combination of the operational function failures at a time.

(4) THE MAJOR FAILURE EVENTS OF THE THREE SECOND-GENERATION SCENARIOS

In the three following Subsections, **(4.1)** through **(4.3),** we will analyze the failure events for the three second-generation scenarios. For each of the three second-generation scenarios, we identify representative major failure events according to the scope defined in Section **3.** For each failure event, we state the operational function(s) causing the failure event, possible elemental functions causing the operational function failure(s), possible consequences of the failure event and finally some example system responses.

Steps in Evaluating a **Normal** Operating Scenario

From the human factors and safety points of view, the process of evaluating/improving a specific scenario designed for normal operation should include the following steps:

(1) Identify all possible major failure events.

(2) For each of the major failure events, identify all possible consequences.

(3) For each of the possible consequences, identify the possible human role in its resolution, i.e. study the human ability in resolving the failure events.

(4) For each of the possible consequences, considering the human ability *of* resolving the failure event, identify possible automated emergency vehicldsystem functions that can help resolve the failure event.

(5) Identify the events that should never occur or should occur with only minute probability because their safe resolution via a combination of human intervention and automated emergency vehicle/system functions is either impossible or impractical. These events can be referred to **as** catastrophic events. These events will lead to constraints on vehicldsystem design.

(6) Conduct a quantitative study to find the occurrence probability (frequency) of all failure events.

(7) Determine a design that balances the consequences of failure events and probability of their occurrence against the design complexity.

Focusing on Events and Consequences; Responses Exampled

This report concentrates primarily on (1) and (2) above. In addition, it provides possible system responses, where the system consists of (i) the drivers, (ii) the vehicles and (iii) the roadside control

system. These responses include drivers' participation and some presumed automated emergency vehicle/roadside functions. The ability of human drivers to react to failure events will be the focus of investigation at a later stage of this human factors project. The subject of designing emergency automated vehicldsystem functions is by itself a challenging subject of future research. (In fact, these two subjects are closely related because of the need to distribute the resolution responsibility between the driver and the vehicle/roadside.) Therefore, the system responses provided in this report are merely examples and should not be interpreted as rigid specifications for the associated scenarios.

Organization of Subsections

Each of the following three Subsections, (4.1) - (4.3), is organized as follows:

- Modifications to the first-generation scenario, if any
- Organization of the failure events
- Assumptions and principles used in defining failure event responses
- The common responses to any failure event
- The format of event description
- The event list: event-specific reactions only (given in the Appendix).

(4.1) The Major Failure Events for Scenario SS1

Organization of the Failure Events

Failure events are grouped according to the following three phases: transition from manual to automated driving mode, automated cruising (along a lane without lane changes), and transition from automated to manual driving mode.

Assumptions and Principles Used in Defining Failure Event Responses

(SS1.A1) Driver has the option of using only the automated lateral (i.e. steering or tracking) control or only the automated longitudinal control. But, we assume that when a failure occurs during automated driving, both lateral and longitudinal control are automated.

(SS1.A2) We assume that, after the automatic lateral control function fails, the longitudinal control

function remains functioning. Therefore, the driver can take over only the lateral control and continue using the automatic longitudinal control. The reverse also holds, for longitudinal control failures.

(SS1.A3) **To** focus on the failure of automated functions, we assume that the vehicle manual controls always work. For example, after the automated longitudinal control has failed, the manual longitudinal control (i.e. manual propulsion and manual braking) still functions.

Common Responses

Response to a failure event contains three stages: detection, notification, reaction. A set of common responses and the condition of their applicability have been identified.

(SS1.CR1) If the failure is caused by the failure of sensors, we assume that the vehicle cannot detect the failure by itself. But, the driver may detect it. However, if the failure is caused by non-sensing failures, the vehicle can detect the failure by itself. If the warning mechanism still works, the vehicle informs the driver of the failure. Since the vehicle moves in midst of mixed traffic, we do not discuss the possibility of neighboring vehicles detecting the failure. (Even if the neighboring vehicles detect the failure through the failed vehicle's erratic behavior, they cannot inform the failed vehicle of the failure due to lack of communication capability.)

(SS1.CR2) Upon detection by the vehicle of its own failure, it informs the driver of the failure and instructs the driver how to react.

(SS1.CR3) If the failure is detected by the driver, he/she takes over according to the emergency plan to be specified in the event list below.

(SS1.CR4) The failed vehicle memorizes the failure or the take-over attempt and denies any future request by the failed vehicle's driver to invoke automated driving until the vehicle has been repaired and re-certified to be fit for automated driving by a off-highway inspection station. This may deter the abuse of emergency take-over procedure during normal transition back to manual control.

These common responses will not be repeated in the events to be listed in the next subsection. Unless otherwise indicated, these apply to all failure events.

We will address ONLY the event-specific reactions in the event list. More explicitly, we will address:

(1) the participation by the driver of the failed vehicle, e.g. taking over the longitudinal control.

(2) the automated reaction by the failed vehicle, e.g. deceleration, if not yet detected and reacted by the driver.

The major failure events are given in Appendix A.

(4.2) The Major Failure Events for Scenario SS2

Organization of the Failure Events

As in the listing of the normal operational events, the failure events are grouped according to the following five phases of operation:

(P1) Enter System:

- inspection failures
- transition failures

(P2) Enter Automated Lanes:

- vehicle failures occurring while a vehicle is moving from an automated on-ramp into the neighboring automated lane.

(P3) Travel in Automated Lanes

- lane-flow failures, i.e. failures occurring while a vehicle is moving along a lane without lane changes
- lane-change failures
- location-constrained lane-change failures, i.e. failures occurring during traffic merging or diverging at the location of a lane merge or lane division

(P4) Exit Automated Lanes

- vehicle failures occurring while a vehicle is moving into an automated off-ramp from the neighboring automated lane.

(P5) Exit System

- transition failures

Assumptions and Principles Used in Defining Failure Event Responses

These assumptions are made to help focus this analysis on the major failure events and to simplify the analysis. Note that they, together with the scope reductions made in Section 3, can be used to point out, for scenario SS2, the failure events not discussed in this report and the potential complexity of a full-scale failure event analysis.

(Assumptions on the Scope of Failure Event Description)

(SS2.A1) Communication between vehicles and between a vehicle and the roadside control system is not safety critical, although communication failure may lead to performance degradation. Therefore, we do not list any events due to only communication failures.

(SS2.A2) Four major types of vehicle operational function failures to be identified are: failure of speed control, headway control, longitudinal position control and steering control. The only type of *multiple* vehicle operational function failures to be identified in this paper is the loss of all automatic control.

(Assumptions on Failure Detection and Notification)

(SS2.A3) After a vehicle detects its own failure, it informs the roadside system and the surrounding vehicles directly. In other words, the roadside system does not relay the failure acknowledgement to the surrounding vehicles. This is to ensure fastest response to the failure.

(SS2.A4) After a driver takes over any vehicle control functions, we assume that the vehicle has the capability to inform the the roadside control system and the surrounding vehicles immediately and simultaneously.

(SS2.A5) After the surrounding vehicles have detected the unexpected behavior by the failed vehicle, they inform the roadside control system. We assume that the roadside control is capable of

identifying correctly and quickly the failed vehicle based on a fusion of information from multiple sources.

(Assumptions on the Event Response Description)

(SS2.A6) No detailed specification for how the surrounding vehicles will react:

After a vehicle failure that is not detected by the failed vehicle itself, the surrounding automated or automation-equipped vehicles may be able to sense the abnormal behavior. They may even be able to react to it for safety. Since such sensing and reaction abilities of the surrounding vehicles cannot be predicted with accuracy at this point, we refrain from explicitly stating specific abilities and reactions. Instead, we use the general concept of "isolation of the failed vehicle and slow-down of traffic" to vaguely characterize the reactions if the surrounding vehicles and the roadside system detect the failure. We also assume that the surrounding vehicles and the roadside control system would react similarly when they are informed of the failure by the failed vehicle.

(SS2.A7) No drivers of the surrounding vehicles will intervene: We assume that no driver take-over will take place in reaction to other vehicles' failure. Therefore, the only human participation in a failure event is by the driver of the failed vehicle.

Note that by (6) and (7), the primary variables in our **DESCRIPTION** of the response to a failure event are the intervention by the driver of the failed vehicle and the failed vehicle's automated emergency functions.

(Assumption on Driver's Role in Failure Reaction)

(SS2.A8) After any of the longitudinal control functions (speed control, headway control and longitudinal position control) of a vehicle has failed, possible immediate system responses include automatic deceleration and driver take-over of longitudinal control followed by manual deceleration.

- We first deal with the case where the vehicle is moving along a lane without engaging in any lane-change maneuvers:

If the vehicle becomes aware of the failure before any intervention by the driver (i.e. it detects the failure by itself or it is informed of the failure by the roadside before the driver intervenes) and the automatic braking still functions, the vehicle brakes to avoid any collision. If the vehicle is about to collide with the vehicle in front, it decelerates as fast as it could to avoid the collision. Otherwise, it decelerates gradually (to avoid any possibility of collision with the vehicle behind). In the meantime, the vehicle notifies the roadside control system and the surrounding vehicles for isolating the failed vehicle and slowing down the traffic for safety.

However, if the vehicle detects the failure but the automatic braking no longer functions, the vehicle warns the driver to take over only the longitudinal control while shutting down vehicle propulsion. The driver then brakes to avoid any collision. (The manual deceleration rate should depend on the circumstances the same way as the automated deceleration rate.) In the meantime, the vehicle notifies the roadside control system and the surrounding vehicles immediately and simultaneously for isolation and traffic slow down. Note that an automated vehicle may be equipped with a "panic button" which triggers a fastest deceleration to avoid a collision with a vehicle ahead in the same lane. If the failed vehicle is so equipped, the driver can press the panic button instead of taking over the longitudinal control to avoid a collision. (However, since the automatic braking may not be functioning, pressing the panic button may not trigger actual deceleration. To avoid such a problem, the braking mechanism of the panic button should be ultra-reliable.) Since the panic button is a major automated emergency vehicle function and its safety and human factors implications are unclear at this stage, we merely mention the possibility of having such a feature and conduct our analysis without assuming its presence on the failed automated vehicle.

If the driver detects the failure before the vehicle becomes aware of the failure, we propose, as an example, that the driver take over only the longitudinal control. The deceleration rate again depends on the circumstances the same way as the automated deceleration rate.

Upon take-over, the vehicle notifies the roadside control system and the surrounding vehicles of the take-over for isolation and traffic slow-down. (The driver can use the panic button if the vehicle is *so* equipped and the circumstances warrants. As indicated earlier, no panic button is assumed available on the failed automated vehicle.)

- We now deal with the case where the vehicle is changing lane (under coordination with vehicles in the destination lane).

If the vehicle becomes aware of the failure before the driver intervenes, it determines whether it should abort or complete the lane change. We assume that the decision to complete the lane change implies that the vehicle would not collide into the side of a vehicle in the destination lane before the completion of the lane change. In either case, if the automatic braking still works, the vehicle decelerates. If the vehicle is in danger of a collision with the vehicle in front after the completion of the lane change, the vehicle decelerates as fast as possible to avoid the collision. Otherwise, it decelerates gradually to avoid a collision with the vehicle behind it. However, if the automatic braking does not work, the vehicle warns the driver to take over the longitudinal control while stopping the propulsion. The manual deceleration rate should depend on the circumstances the same way as the automated deceleration rate.

If the driver detects the failure before the vehicle becomes aware of it, the driver should decide whether to abort or complete the lane change. To complete the maneuver, the driver has to take over only the longitudinal control. (He/she may also take over the lateral control.) Otherwise, he/she has to take over both the longitudinal and the lateral control. The manual deceleration rate should depend on the circumstances the same way as the automated deceleration rate. (If the failed automated vehicle is equipped with a panic button, he/she can press that button in lieu of a manual fast deceleration.)

However, after a longitudinal failure during a lane change maneuver at a lane merge loca-

tion (location-constrained lane change), the responses could be different because there is much less space (if any) for emergency maneuvering compared to the available space in the case of a regular lane change (from one automated lane to another). Therefore, abort may not be a viable solution. If the vehicle becomes aware of the failure before the driver intervenes, it **does** not **ask** the driver to take over. Instead, it uses its own intelligence to avoid collisions. It may steer itself off the course and use the limited space at the merge location to avoid collisions. The surrounding vehicles would use their own intelligence to avoid collisions too. If the driver detects it first, we propose that hdshe be not permitted to take over any control.

(SS2.A9) After **loss** of lateral (tracking) control, however, the responses could be different. If the vehicle becomes aware of the failure before the driver intervenes, it instructs the driver to take over only the lateral control. Otherwise, we propose driver take-over of only the lateral control. These apply whether the vehicle is moving along a lane, changing lane, merging at a lane merge or diverging at a lane division.

(SS2.A10) After a vehicle loses all automatic control, we assume that the surrounding vehicles would detect the failure and, together with the roadside control system, isolate the failed vehicle and slow down. We also assume that the vehicle cannot become aware of and react to the failure. In other words, the only possible reaction by the failed vehicle is the intervention by the driver of the failed vehicle. (The panic button, if so equipped, presumably does not work.) If the vehicle is in the lane-flow mode, the driver takes over at least the lateral control immediately with the option of taking over both the lateral and longitudinal control simultaneously. (The rationale is that it is easier for the surrounding vehicles to avoid a longitudinal collision with the failed vehicle than for them to avoid a lateral collision. Having the driver take over the lateral control **as** soon **as** possible could help avoid a lateral collision.) If the failure occurs when the vehicle is making a regular lane change, the driver should take over both the lateral and the longitudinal control. However, only the lateral control should be taken over by the driver if the vehicle is making a location-constrained

lane change. (The rationale is identical to its counterpart for not proposing to have the driver take over the longitudinal control after a failure of the longitudinal control during a location-constrained lane change at the location of a lane merge. See last paragraph of SS2.A8.)

The Common Responses to Failure Events and Their Applicability

Response to a failure event contains three stages: detection, notification, reaction. Despite a large number of possible failure events, a set of six common responses and the condition for their applicability have been identified. (SS2.CR1) - (SS2.CR4) are common to the detection and notification stages of all events. (SS2.CR5) - (SS2.CR6) contain common reactions to any failure event. Some minor assumptions are also made to simplify the discussion.

(SS2.CR1) If the failure is caused by the failure of sensors, we assume that the vehicle cannot detect the failure by itself. But, the driver may detect it. However, if the failure is caused by non-sensing failures, the vehicle can detect the failure by itself. If the warning mechanism still works, the vehicle informs the driver of the failure. Even if the failure is not detected by the vehicle itself and its driver, the surrounding vehicles may be able to detect it based on the unexpected behavior of the failed vehicle.

(SS2.CR2) Upon detection by the vehicle of its own failure, it informs the driver of the failure and instructs him/her how to react. In the meantime, it informs the roadside control system immediately. The roadside system in conjunction with the surrounding (functioning) vehicles calls off all pending or planned maneuvers in the vicinity, isolates the failed vehicle and slows down the traffic for safety. (An operational communication link is assumed.)

(SS2.CR3) If the failure is detected by the driver, he/she takes over according to the emergency plan to be specified later in the failure event list. Upon driver take-over, the vehicle informs the roadside control system and the surrounding vehicles of the human intervention. The roadside control system in conjunction with the surrounding (functioning) vehicles calls off all pending or planned maneuvers in the vicinity, isolates the failed vehicles and slows down

the traffic for safety. (An operational communication link is assumed.)

(SS2.CR4) If the failure is detected by some surrounding vehicles, they inform the roadside control system, which in turn informs the failed vehicle itself and all the surrounding vehicles. The failed vehicle informs its driver of the failure and instructs the driver how to react. The roadside control system in conjunction with the surrounding automated vehicles calls **off** all pending or planned maneuvers in the vicinity, isolates the failed vehicle and slows down the traffic. (An operational communication link is assumed,)

(SS2.CR5) The failed vehicle, either after the driver has resumed complete manual control or after it **has** been slowed down or **stopped** automatically, has to be removed, under its own force or towed, from the **AHS** through an automated off-ramp.

(SS2.CR6) The failed vehicle's requests for reentry to the **AHS** will be denied until the failure has been corrected.

These common responses will **NOT** be repeated in the events to be listed in the next subsection. Unless otherwise indicated, these apply to all failure events.

We will address ONLY the event-specific reactions in the event list. More explicitly, we will address:

(1) the participation by the driver of the failed vehicle, e.g. taking over only the lateral control: We discuss only the initial reactions by the driver for averting the danger resulting from the failure but not his/her subsequent participation after the danger has been avoided, e.g. resuming full control and driving the vehicle off the AHS.

(2) the automated reaction by the failed vehicle itself, if the failure has not yet been detected and reacted to by the driver, e.g. automated deceleration.

(3) rarely, the reaction by the surrounding vehicles and the roadside control system.

The major failure events are given in Appendix B.

(4.3) The Major Failure Events for Scenario *SS3*

Modifications to Scenario **S3**

(SS3.M1) We first introduce a few new concepts and terms.

A subplatoon is defined to be a number of consecutive vehicles within a platoon. A lane change by a subplatoon from one lane to another requires several preparation steps. For ease of discussion, assume that the lane-change subplatoon is in the middle of the platoon. Recall this scenario allows a lane-changing subplatoon to join another platoon while it is entering the destination lane. Also assume that the subplatoon joins the receiving platoon in the middle of the platoon. The preparation steps then include: (i) creating a gap between the subplatoon and the vehicles in front of it, (ii) creating a gap between the subplatoon and the vehicles in rear, (iii) creating a gap, called the receiving gap, in the middle of the receiving platoon large enough to allow a safe entry of the subplatoon. After the actual lane change maneuver, the three subplatoons merge to form one single platoon. We define the concept of a departure interim gap as the gap created in either (i) or (ii). Upon the (complete) arrival of the whole subplatoon at the destination lane and before the three subplatoons merge, there exist two gaps, one before and the other behind the joining subplatoon. Either of these two gaps will be called an arrival interim gap. An interim gap refers to either a departure interim gap or an arrival interim gap.

With the new terminology, we describe the modification:

The required length of an interim gap may be shorter than the inter-platoon spacing and longer than the intra-platoon spacing. This can be safe if the duration is short.

(SS3.M2) The driver of a manually driven but automation-equipped vehicle, after receiving the permission from the roadside control system to enter the transition lane, receives guidance from the vehicle/roadside control system regarding the right time and place to enter the transition lane.

(SS3.M3) There are markings on the pavement between the transition lane and its neighboring manual lane indicating a no lane-change zone. A good place for such markings is at the vicinity of a gate. (However, the driver may nevertheless change lane near a gate into the transition

lane from the neighboring manual lane due to lack of physical barriers.)

(SS3.M4) When a platoon is moving from the transition lane into the neighboring automated lane or vice versa, it is not allowed, for safety reasons, to simultaneously join another platoon (as part of the lane-change maneuver). Also, for the same reasons, only a whole platoon, not just any subplatoon, can make such a change lane. In other words, the "group" of vehicles must be separated from the other vehicles in the transition lane by at least an inter-platoon spacing.

Note that disallowing this "compound" maneuver is motivated by the the following consideration. If the lane-changing platoon suffers any longitudinal or coordination failure, the platoon may suddenly slow down. Since there may be manually-driven vehicles on the transition lane, this sudden deceleration can result in a collision into the platoon. Also, if the traffic on the destination automated lane suffers any anomaly, e.g. longitudinal failure of any vehicle of the receiving platoon, it will likely lead to a sudden deceleration of the lane-changing platoon. Manually driven vehicles following the platoon may not be able to react soon enough to avoid a collision.

Disallowing a platoon from joining another platoon while exiting the automated lanes into the transition lane is also motivated by our opinion that allowing *so* would not benefit traffic flow and control.

(SS3.M5) When a platoon is merging from an automated on-ramp into the existing traffic on the neighboring automated lane or when a platoon on the ending lane at a lane merge location is merging into the existing traffic on the continuing lane, it is not allowed, for safety reasons, to simultaneously join another platoon (as part of the location-constrained lane change maneuver).

(SS3.M6) The automated patrol vehicles use the automated lanes the same way any automated vehicles do. However, the roadside control system makes way for the patrol vehicles.

Organization of the Failure Events

As in the listing of the normal operational events, the failure events are grouped according to the following five phases of operation:

(P1) Enter System: Events are further partitioned into two subgroups: Enter System from the Transition Lane and Enter System from an Automated On-ramp. The events within the first subgroup pertain to:

- non-automation-equipped vehicles entering the transition lane
- hazardous interactions between the automated traffic and the manual traffic on the manual lanes and the transition lane
- inspection failures
- transition failures
- preplatooning failures

The events within the second subgroup pertain to only the last three types of failures.

(P2) Enter Automated Lanes: Events are partitioned into two subgroups: Enter Automated Lanes from the Transition Lane and Enter Automated Lanes from an Automated On-Ramp. The events within the first subgroup pertain to:

- non-automation-equipped vehicles entering the automated lanes
- impaired vehicles entering the automated lanes
- vehicle failures during a platoon (or vehicle) lane change from the transition lane into its neighboring automated lane (without joining another platoon in the automated lane in the process)

The events within the second subgroup pertain to:

- impaired vehicles entering the automated lanes
- vehicle failures occurring while a platoon (or a vehicle) moves from an automated on-ramp into the neighboring automated lane (without simultaneously joining another platoon in the automated lane).

(P3) Travel in automated Lanes Events pertain to:

- lane-flow failures, i.e. failures occurring while a platoon is moving along in a lane without any vehicle or platoon lane changes,
- lane-change failures
- location-constrained lane-change failures, i.e. failures occumng during traffic merging or diverging at the location **of** a lane merge or lane division

(P4) Exit Automated Lanes: Events **are** partitioned into two subgroups: Exit Automated Lanes **from** the Transition Lane and Exit Automated Lanes from an Automated Off-Ramp. The events within the first subgroup pertain to:

- vehicle failures during a platoon lane change into the transition lane from the neighboring automated lane (without simultaneously joining another platoon in the transition lane)

The events within the second subgroup pertain to:

- vehicle failures occurring while a platoon is moving into an automated off-ramp from the neighboring automated lane.

(P5) Exit System: Events are further partitioned into two subgroups: Exit System from the Transition Lane and Exit System from an Automated Off-ramp. The events within the first subgroup pertain to:

- hazardous interactions between the automated traffic and the manual traffic on the manual lanes and the transition lane
- deplatooning failures
- transition failures

The events within the second subgroup pertain to only the last two types of failures.

Assumptions and Principles Used in Defining Failure Event Responses

These assumptions are made to help focus this analysis on the major failure events and to simplify the analysis. Note that they, together with the scope reductions made in Section **3,** can be used to point out, for scenario **SS3,** the failure events not discussed in this report and the potential complexity of a

full-scale failure event analysis.

(Assumptions on the Scope of Failure Event Description)

(SS3.A1) Communication between vehicles and between a vehicle and the roadside control system is not safety critical, although communication failure may lead to performance degradation. Therefore, we do not list any events due to only communication failures.

(SS3.A2) Four major types of vehicle operational function failures to be identified are: failure of **speed** control, headway control, longitudinal position control and steering control. The only type of multiple vehicle operational function failures is the loss of all automatic control.

(SS3.A3) **We** assume that the arrival interim gap can be significantly shorter than the inter-platoon spacing. However, the length of a departure interim gap is close to or exactly the length of the inter-platoon spacing.

This assumption is motivated in general by safety and in part by the following two specific reasons. First, the duration of the arrival gaps could be short. But, the duration of the departure gaps may be much longer, which makes a small departure interim gap potentially unsafe. (The platoon containing the lane-change subplatoon needs to initiate the preparation earlier and would expect longer elapsed time waiting for the preparation by other vehicles.) Second, before the arrival of the lane-changing subplatoon, the receiving gap could be large enough for safety.

As a result of this assumption, we do not explicitly address those failure events occurring while a subplatoon is changing lane from one automated lane to another through a gate, after the departure interim gaps have been created. Instead, these events are considered equivalent to those occurring while a full platoon changes lane from one automated lane to another through a gate. We will treat only the latter types of failure events. However, we will explicitly treat the failure events occurring while a whole platoon changes lane and simultaneously joins another platoon in the destination lane (from its front, from its rear or

in the middle).

(Assumptions on Failure Detection and Notification)

(SS3.A4) After a vehicle detects its own failure, it informs the roadside system directly. In the mean-time, it **informs** the lead vehicle of the platoon (if it is not the lead vehicle itself) and the surrounding vehicles. In other words, the lead vehicle does not relay the failure acknowledgement to the roadside control system **from** the failed vehicle. This is to ensure fastest response to the failure.

(SS3.A5) After a driver takes over any vehicle control functions, we assume that the vehicle has the capability to inform the lead vehicle of the platoon, the roadside control system, and the surrounding vehicles immediately and simultaneously.

(SS3.A6) After the surrounding vehicles have detected the unexpected behavior by the failed vehicle, they inform the roadside control system. We assume that the roadside control is capable of identifying correctly and quickly the failed vehicle based on a fusion of information from multiple sources.

(SS3.A7) The roadside control system detects the presence of an intruder, i.e. a non-automation-equipped vehicle or an automation-equipped vehicle denied entry by the roadside control system, in the automated lanes as follows.

If **an** automated vehicle, after having sensed the presence of another vehicle in the automated lanes and having initiated a request for communication with the vehicle, fails to obtain any response, it informs the roadside control system of such an incident. The roadside control system, based on such "sightings" from other automated vehicles and through an information fusion process, then infers the presence of the intruder.

(Assumptions on the Event Response Description)

(SS3.A8) No detailed specification for how the surrounding vehicles will react:

After a vehicle failure that is not detected by the failed vehicle itself, the surrounding

automated or automation-equipped vehicles may be able to sense the abnormal behavior. They may even be able to react to it for safety. Since such sensing and reaction abilities of the surrounding vehicles cannot be predicted with accuracy at this point, we refrain from explicitly stating specific abilities and reactions. Instead, we use the general concept of "isolation of the failed vehicle and slow-down of traffic" to vaguely characterize the reactions if the surrounding vehicles and the roadside system detect the failure. (Note that isolation includes, among other things, breaking the failed vehicle off from the platoon.) We also assume that the surrounding vehicles and the roadside control system would react similarly when they are informed of the failure by the failed vehicle.

(SS3.A9) No drivers of the surrounding vehicles will intervene:

We assume that no driver take-over will take place in a reaction to other vehicles' failure. Therefore, the only human participation in a failure event is by the driver of the failed vehicle.

Note that by (8) and (9), the primary variables in our DESCRIPTION of the response to a failure event are the intervention by the driver of the failed vehicle and the failed vehicle's automated emergency functions.

(Assumptions on Driver's Role in Failure Reaction)

(SS3.A10) After any of the longitudinal control functions (speed control, headway control and longitudinal position control) of a vehicle has failed, possible immediate system responses include automatic deceleration and driver take-over of longitudinal control followed by manual deceleration.

- We first deal with the case where the platoon is moving along a lane without engaging in any lane-change maneuvers:

If the vehicle detects the failure by itself and the automatic braking still functions, the vehicle brakes to avoid any collision. If the vehicle is a lead vehicle and it is about to collide

with the vehicle in front, it decelerates as fast as it can to avoid the collision. Otherwise, it decelerates gradually. If the vehicle is a trailing member of a platoon, it brakes fast but not so fast that the vehicle behind could rear-end into it.

However, if the vehicle detects the failure but the automatic braking no longer functions, the vehicle warns the driver to take over only the longitudinal control while stopping automated propulsion. The driver then brakes to avoid any collision. (The manual deceleration rate should depend on the circumstances the same way as the automated deceleration rate.) In the meantime, the vehicle notifies the lead vehicle, the roadside control system and the surrounding vehicles for isolating the failure vehicle and traffic slow down. Note that an automated vehicle may be equipped with a "panic button" which triggers a fastest deceleration to avoid a collision with a vehicle ahead in the same lane. If the failed vehicle is so equipped, the driver can press the panic button instead of taking over the longitudinal control to avoid a collision. (However, since the automatic braking may not be functioning, pressing the panic button may not trigger actual deceleration. To avoid such a problem, the braking mechanism of the panic button should be ultra-reliable or separate from automatic braking.) Since the panic button is a major automated emergency vehicle function and its safety and human factors implications are unclear at this stage, we merely mention the possibility of having such a feature and conduct our analysis without assuming its presence on the failed automated vehicle.

If the driver detects the failure, we propose, as an example, that the driver take over only the longitudinal control. The deceleration rate again depends on the same circumstances as the automated deceleration rate. Upon take-over, the vehicle notifies the lead vehicle, the roadside control system and the surrounding vehicles of the take-over for isolation and traffic slow-down. (The driver can use the panic button if the vehicle is so equipped and the circumstances warrant. As indicated earlier, no panic button is assumed available on the failed automated vehicle.)

- We now deal with the case where the platoon is changing lane through a gate (under coordination with platoons in the destination lane).

In this situation, driver take-over could be very dangerous. Therefore, we propose no driver take-over but to rely on automated emergency vehicldsystem functions. This is the case whether the failure is detected by the vehicle itself or by the driver and whether the vehicle is the lead vehicle or a trailing member of a platoon. (Even if the failed automated vehicle is equipped with a panic button, we do not propose its use.)

(SS3.A11) After loss of lateral (tracking) control, however, the responses could be different. If the vehicle detects it by itself, it instructs the driver to take over the lateral control. If the driver detects it first, we propose driver take-over of only the lateral control. These apply whether the vehicle is moving along in the same lane, changing lane through a gate, merging at a lane merge or diverging at a lane division.

(SS3.A12) After a vehicle loses all automatic control, we assume that the surrounding vehicles would detect the failure and, together with the roadside control system, isolate the failed vehicle and slow down. We also assume that the vehicle cannot detect the failure by itself. (The panic button, if *so* equipped, presumably does not work.) If the platoon is in the lane-flow mode, the driver takes over all control, the lateral control immediately and then the longitudinal control. However, only the steering control should be taken over by the driver if the platoon is making a lane change, regular or location-constrained, through a gate.

(SS3.A13) Although the driver must pass a readiness test before he/she can take over control, no such test is required for emergency take-overs. (A design issue is how to prevent abuse of the emergency take-over procedure during a normal transition back to the manual driving mode.)

(Assumptions on Automated (Non-Driver) Reactions)

(SS3.A14) Vehicle operational function failures that occur during a lane change are distinguished with respect to the position **of** a vehicle in a platoon. Basically, when one event is identified for

a failure of the lead vehicle of a lane-changing platoon, a similar one involving a trailing member of a platoon is also stated. The difference between the two events is mainly in the automated reactions rather than the driver's role.

After a failure during a lane change, the lane change maneuver may have to be aborted. There are two major options in aborting the lane change. One option is to leave the decision to the individual vehicles, referred to later as self-determination. while the other is to determine a break point in the platoon so that only the vehicles behind the break point should abort the lane change.

If the failed vehicle is a lead vehicle and it detects the failure by itself, then both options seem viable (if the communication capability is not compromised). In particular, the lead vehicle can determine the break point and inform the vehicles of this decision. However, if the failed vehicle is a trailing vehicle of a platoon, informing the lead vehicle and waiting for its decision may take too long (in particular if the message is relayed from vehicle to vehicle). An advantage of leaving the decision to the individual vehicles is the quick reaction. Note that a intra-platoon communication scheme relying on relay of messages from one vehicle to its adjacent vehicles may not be sufficiently fast for collision avoidance during some of the failure events.

Note that, under self-determination, there is no active coordination. However, since the vehicles use the same "algorithm" in making the abort decision, there would likely be an actual break-point.

The Common Responses to Failure Events and Their Applicability

Response to a failure event contains three stages: detection, notification, reaction. Despite a large number of possible failure events, a set of six common responses and the condition of their applicability have been identified. (1) - (4) are common to the detection and notification stages of all events. (5) - (6) contain common reactions to any failure event. Some minor assumptions are also made to simplify the discussion.

(SS3.CR1) If the failure is caused by the failure of sensors, we assume that the vehicle cannot detect the failure by itself. But, the driver may detect it. However, if the failure is caused by non-sensing failures, the vehicle can detect the failure by itself. If the warning mechanism still works, the vehicle informs the driver of the failure. Even if the failure is not detected by the vehicle itself and its driver, the surrounding vehicles may be able to detect it based on the unexpected behavior of the failed vehicle.

(SS3.CR2) Upon detection by the vehicle of its own failure, it informs the driver of the failure and instructs him/her how to react. In the meantime, it informs the lead vehicle of its platoon (if it is not a lead vehicle), the roadside control system and the surrounding vehicles simultaneously. The roadside system in conjunction with the surrounding (functioning) vehicles calls off the pending or planned maneuvers in the vicinity, instructs platoons to abort maneuvers currently being executed, isolates the failed vehicle and slows down the traffic for safety. (An operational communication link is assumed.) If the failure occurs on the transition lane or the failed vehicle may enter the transition lane, the roadside control system, in addition to instructing the automated vehicles to isolate the failed vehicle, allows no additional manually-driven vehicles to enter the transition lane near the scene (i.e. by not granting permission to enter). Furthermore, the roadside control system will warn the manually-driven but automation-equipped vehicles of the danger and advise them to move away from the failed vehicle (as part of the attempt to isolate the failed vehicle).

(SS3.CR3) If the failure is detected by the driver, he/she takes over according to the emergency plan to be specified later in the failure event list. Upon driver take-over, the vehicle informs the lead vehicle, the roadside control system and the surrounding vehicles of the human intervention. The roadside control system in conjunction with the surrounding (functioning) vehicles calls off all pending or planned maneuvers in the vicinity, instructs platoons to abort maneuvers currently being executed in the vicinity, isolates the failed vehicles and slow down the traffic for safety. (An operational communication link is assumed.) If the failure occurs on the transition lane or the failed vehicle may enter the transition lane, the

roadside control system provides the same additional response as described in (2) above for isolating the failed vehicle.

(SS3.CR4) If the failure is detected by some surrounding vehicles, they inform the roadside control system, which in turn informs the failed vehicle itself and all the surrounding vehicles. The failed vehicle informs its driver of the failure and instructs the driver how to react. The roadside control system in conjunction with the surrounding automated vehicles calls **off** all pending or planned maneuvers in the vicinity, instructs platoons to abort maneuvers currently being executed, isolates the failed vehicle and slows down the traffic. (An operational communication link is assumed.) If the failure occurs on the transition lane or the failed vehicle may enter the transition lane, the roadside control system provides the same additional response as described in (2) above for isolating the failed vehicle.

(SS3.CR5) The failed vehicle, either after the driver has resumed complete manual control or after it has been slowed down or stopped automatically, have to be removed, under its own force or towed, from the **AHS**

between lane barriers

through lane-change gates

through an automated off-ramp or the transition lane.

(SS3.CR6) The failed vehicle's further requests for reentry to the automated lanes and the transition lane will be denied until the failure has been corrected.

These common responses will **NOT** be repeated in the events to be listed in the next subsection. Unless otherwise indicated, these apply to all failure events. We will address ONLY the event-specific reactions in the event list. More explicitly, we will address:

(1) the participation by the driver of the failed vehicle, e.g. taking over only the lateral control: We discuss only the initial reactions by the driver for averting the danger resulting from the failure but not his/her subsequent participation after the danger has been avoided, e.g. resuming full control and driving the vehicle off the AHS.

(2) the automated reaction by the failed vehicle itself, if the failure has not yet been detected and reacted to by the driver, e.g. automated deceleration.

(3) occasionally, the reaction by the other functioning vehicles in the platoon

(4) rarely, the reaction by the surrounding platoons and the roadside control system.

The major failure events are given in Appendix ***C.***

(5) CONCLUSION

Three scenarios are selected from the seven first-generation scenarios for identifying human capability in resolving emergency situations resulting from *AHS* vehicle/highway failures and are ***not*** being advocated **as** the better deployment choices among the seven first-generation scenarios.. Many failure events have been identified for each of the three scenarios. Yet even more exist, but are beyond the scope of **this** paper. **(See** the scope of this analysis in Section **3.2.) Our** analysis confirms the obvious fact that the complexity of a comprehensive failure event analysis increases with the complexity **of** the automated system.

The responses to the failure events provided in the paper actually stretch the limits of human capability. This is intentional and is intended to avoid any premature exclusion of viable human participation. At a later stage of the human factors project, a proper subset of the human capabilities assumed in the responses will be identified and will serve as the guideline for designing AHS operating strategy. Anticipating a limited human role in failure/emergency resolution, we adopted the principles that human intervention is considered only when drivers or passengers are in danger of fatality or injury and that the human responsibilities should be small in number, simple in nature and natural in human reflex.

Once the human capabilities are identified, the occurrence probabilities of the failure events are determined, and the consequences of the events are quantified, the requirement for automated vehicle/system emergency functions for these scenarios, if any, should become clearer. A task at a later stage of this project will identify these functions. Given the required emergency functions, the feasibility of these scenarios should also become clearer. If the emergency functions cannot be made ultra-reliable, failure analysis for the emergency functions is required and will further complicate the overall failure analysis.

REFERENCES

[1] Hitchcock, A., "Intelligent Vehicle/Highway System Safety: Problems of Requirement Specification and Hazard Analysis", Transportation Research Record No. 1318, 98-103, 1991.

[2] Shladover, S, "Operation of Automated Guideway Transit Vehicles in Dynamically Reconfigured Trains and Platoons," (Extended Summary, Vol. I & 11), UMTA-MA-06-0085-79-1, UMTA-MA-06-0085-79-2 and UMTA-MA-06-0085-79-3, U.S. Department of Transportation, Urban Mass Transportation Administration, Washington, D.C., July, 1979.

[3] Tsao, H.-S.J. and Hall, R.W., "A Probabilistic Model for AVCS Longitudinal Collision/Safety Analysis", IVHS Journal, Vol.1, No. 3, pp. 261-274, 1994.

[4] Tsao, H.-S.J., Hall, R.W. and Shladover, S.E., "Automated Highway Systems Operating Strategies and Events: A Driver's Perspective", PATH Working Paper, in preparation, University of California, Institute of Transportation Studies, Berkeley, California, USA.

[5] Tsao, H.-S.J., Hall, R.W., Shladover, S.E., Plocher, T.A. and Levitan, L.J., "Human Factors Design of Automated Highway Systems: First Generation Scenarios", FHWA Report No. FHWA-RD-93-123, Washington, D.C.

[6] Zhang, W.-B., Shladover, S.E., Hall, R.W. and Plocher, T.A., "Human Factors Design of Automated Highway Systems (AHS): Preliminary Definition of AHS Functions", FHWA Working Paper, in preparation.

APPENDIX A: MAJOR FAILURE EVENTS FOR SS1

In the following list, we use these abbreviations:

OPERATIONAL FUNCTIONS — ELEMENTAL FUNCTIONS:	FUNCTIONS
POSSIBLE CONSEQUENCES OF THE FAILURE:	CONSEQUENCES
EXAMPLE RESPONSES:	RESPONSES
DRIVER OF THE FAILED VEHICLE:	DRIVER
FAILED VEHICLE:	VEHICLE
OTHER VEHICLES AND ROADSIDE CONTROL SYSTEM:	OTHERS

Note that the absence of a specific item implies the absence of event-specific reactions. Parenthesized headings indicate the phase of normal operation.

To reduce repetition, we omit the common responses and provide only a concise description. But to clarify how to interpret the responses, consider the following example (Event SS1.6). We give the full description with common responses and then the concise description without them. Please note the difference.

Full Description:

(SS1.6) Lane tracking function fails.

OPERATIONAL FUNCTIONS — ELEMENTAL FUNCTIONS: **OF8 - V1, V3, V6**

POSSIBLE CONSEQUENCES OF THE FAILURE:
Vehicle strays out of lane causing collisions with vehicles in the neighboring lanes.

EXAMPLE RESPONSES:

DRIVER OF THE FAILED VEHICLE:

If the failure is caused by the failure of sensors, we assume that the vehicle cannot detect the failure by itself. But, the driver may detect it. If the driver detects it before the vehicle does, he/she takes over only the lateral (steering) control.

FAILED VEHICLE:

If the failure is caused by non-sensing failures, the vehicle can detect the failure by itself. Upon seif-detection, it brakes to a fast stop. If the warning mechanism still works, the vehicle, upon detection of the failure, also informs the driver of the failure and instructs the driver to take over only the lateral (steering) control.

Since the vehicle moves in midst of *mixed* traffic, we do not discuss the possibility of neighboring vehicles detecting the failure. (Even if the neighboring vehicles detect the failure through the failed vehicle's erratic behavior, they cannot inform the failed vehicle of the failure due to lack of communication capability.)

The failed vehicle memorizes the failure or the emergency take over attempt so that any future attempt of the failed vehicle's driver to transition into the automated driving mode will be denied until the vehicle has been inspected by an off-highway station and certified to be fit for automated driving. Note that the denial following an emergency take-over attempt, *after* the attempt but before the inspection, may deter abuse of the emergency take-over procedure during normal transition. (The normal control resumption procedure requires a test of driver readiness while the emergency take-over procedure does not.)

Abbreviated Description:

(SS1.6) Lane tracking function fails.

FUNCTIONS: **OF8** - V1, V3, V6
CONSEQUENCES: Vehicle strays out of lane causing collisions.
RESPONSES:
DRIVER: Takes over the lateral (steering) control.
VEHICLE: **Warns** the driver of the failure and to take over only the lateral (steering) control; brakes to a fast stop.

We are now ready to list the major failure events as follows.

THE **EVENT LIST:**

(Transition from **Manual** to Automated Driving **Mode:)**

(SS1.1) Failure of vehicle inspection and monitoring.

FUNCTIONS: OF1 or OF17
CONSEQUENCES: General unsafe automated driving
RESPONSES: Depending on the nature of the undetected failures **(See** below.)

(SS1.2) Vehicle fails to transition from manual mode to automatic, but informs the driver of a success.

FUNCTIONS: **OF3** - V1, **V3, V4, V6, V7,** V11
CONSEQUENCES: Vehicle on highway under **no** control
RESPONSES:
DRIVER: Takes over total control.

(Fully Automated Lane Cruising:)

(SS1.3) Driver assigns too high a target **speed.**

FUNCTIONS: **OF5** - H4g
CONSEQUENCES: Excessive **speed** on curves.
RESPONSES:
VEHICLE: Vehicle overrides driver-set target **speed** for safety whenever necessary (e.g. on curves).

(SS1.4) Vehicle moves at a higher **speed** than the driver-set **speed.**

FUNCTIONS: **OF5** - V1, V4, V6
CONSEQUENCES: Driver discomfort and **potential** danger
RESPONSES:
DRIVER: Takes over the longitudinal control if he/she detects it.
VEHICLE: **Warns** the driver to take over the longitudinal control. (The availability of the function of comparing the actual **speed** to the set **speed** is assumed.)

(SS1.5) Vehicle invades into the safety spacing between itself and the vehicle in front.

FUNCTIONS: OF6 - V1, V4, V6
CONSEQUENCES: Dangerous driving
RESPONSES: Same **as SS1.4.**

(SS1.6) Lane tracking function fails.

FUNCTIONS: OF8 - V1, **V3,** V6
CONSEQUENCES: Vehicle strays out of lane causing collisions.
RESPONSES:
DRIVER: Takes over the lateral (steering) control if he/she detects it.
VEHICLE: **Warns** the driver of the failure and take-over; brakes to **a** fast stop.

(SS1.7) Vehicle loses all automatic control (while driving along a lane).

FUNCTIONS: OF8; OF5, OF6, OF7
CONSEQUENCES: Collisions with vehicles in the same lane and/or with vehicles and the neighboring lanes.
RESPONSES:
DRIVER: Takes over total control.

(SS1.8) Vehicle fails to recognize traffic signs, e.g. Lane Merge, Highway Ends and Lane Ends.

FUNCTIONS: V14
CONSEQUENCES: Risk of collision
RESPONSES:
DRIVER: Takes over total control.

(Transition from automated to Manual Mode:)

(SS1.9) Vehicle warns the driver to take over, but the driver does not respond to the required test (e.g. driver is **not** conscious).
EXAMPLE: Automated vehicle approaches a lane merge. Vehicle recognizes the sign **and** instructs the driver to take over control for merging, but the driver does **not** take over control.

FUNCTIONS: OF21
CONSEQUENCES: Collisions
RESPONSES:
VEHICLE: If automatic braking works, vehicle decelerates to a **stop. (NOTE:** Should minimize the number of lane merges for safety.)

(SS1.10) Driver fails the readiness test.

FUNCTIONS: V8
CONSEQUENCES: Unwanted automated driving
RESPONSES:
DRIVER: Retries until a preset maximum number of repeated failed trials is exceeded.
VEHICLE: After the preset number is exceeded, vehicle slows down and stops.

(SS1.11) Vehicle cannot be switched back to the manual driving mode.

FUNCTIONS: V8
CONSEQUENCES: Unwanted automated driving
RESPONSES:
DRIVER: **Try** the emergency take-over procedure. **If** it **works,** the failure event is resolved. (Recall that manual controls are assumed to be always working.) If it does not work, there is no recourse. (The availability of a panic button **is** not assumed.)
VEHICLE: Assume that the vehicle is able to realize the failure. Vehicle slows down and stops using automatic braking if it still works; otherwise, **do** the same by turning off ignition. If the vehicle is not able to detect this failure, vehicle **does** nothing.

APPENDIX B: MAJOR FAILURE EVENTS FOR SS2

In the following list, we use the following abbreviations:

NORMAL OPERATIONAL EVENT:	**NORMAL EVENT**
OPERATIONAL FUNCTIONS - ELEMENTAL FUNCTIONS:	**FUNCTIONS**
POSSIBLE CONSEQUENCES OF THE FAILURE:	**CONSEQUENCES**
EXAMPLE **RESPONSES:**	**RESPONSES**
DRIVER **OF THE FAILED VEHICLE:**	DRIVER
FAILED VEHICLE:	**VEHICLE**
OTHER VEHICLES AND ROADSIDE CONTROL SYSTEM:	**OTHERS**

Note that the absence of a specific item implies the absence of event-specific reactions. Parenthesized headings indicate the phase of normal operation.

Due to the similarity between the common responses to failure events of this fully automated AHS scenario and their counterparts in *SS3* (also fully automated), we provide only one example illustrating proper interpretation of the abbreviated event description. **Since** *SS3* is more complicated, we give an example for that scenario. The reader is referred to **APPENDIX 3** for the example.

THE EVENT LIST:

(Enter System:)

(SS2.1) The roadside system fails to detect and reject an impaired vehicle at the entrance.

NORMAL EVENT: **s2.1**
FUNCTIONS: **OF1** - V2, RC1
CONSEQUENCES: Impaired vehicles allowed on **AHS.** (Impairment may be in the form of either a functional failure or functional degradation. **A** degraded function may lead to a functional failure.) **See** the rest of the failure events for possible consequences (and responses). **Note** that this may be a serious failure event because the safety of the **AHS** may heavily depend on the ability of the inspection function to minimize the failure probability.
RESPONSES:
VEHICLE: If vehicle itself detects impairment after entry and before failure, then it informs system. The roadside system and the surrounding vehicles isolate the failed vehicle and slow down the traffic, if necessary, before removing the vehicle from **AHS.** Otherwise, **see** the rest of the failure events for possible responses to the possible consequences.

(SS2.2) Vehicle fails to switch from manual mode to automated mode on an automated on-ramp, after passing the inspection.

NORMAL EVENT: **S2.2**
FUNCTIONS: OF3 - V1, V3, V4, **V6, V7**
CONSEQUENCES: Automated driving not possible
RESPONSES:
OTHERS: Vehicle/system instructs the driver to leave the **AHS.**

(SS2.3) Vehicle fails to switch from manual to automated mode on an automated on-ramp, but the vehicle informs the driver that the transition has been completed.

NORMAL EVENT: **S2.2**
FUNCTIONS: OF3
CONSEQUENCES: Vehicle not under any control
RESPONSES:
DRIVER: Resumes manual control.

(Enter Automated Lanes:)

(SS2.4) Vehicle on an automated on-ramp is incapable of merging into the existing automated traffic on the **AHS** at the merging location due to loss of speed control.

NORMAL **EVENT:** **S2.5**
FUNCTIONS: **OF5** - V1, V4, **V6**
CONSEQUENCES: Possible collisions (side swipe) with the automated vehicles on the right lane
RESPONSES:
DRIVER: No take-over **of** any kind.
VEHICLE: Gives warning when the un-controlled vehicle poses danger to the itself or the surrounding vehicles.

(SS2.5) Vehicle on an automated on-ramp is incapable of merging into the automated traffic on the AHS at the merging location due to loss of longitudinal position control.

NORMAL EVENT: **S2.5**
FUNCTIONS: OF7 - V1, **V4, V6**
CONSEQUENCES: Same as **(SS2.4)**
RESPONSES:
DRIVER: No take-over of any kind.

(SS2.6) Vehicle on an automated on-ramp is incapable of merging into the existing automated traffic on the **AHS** at the merging location due to loss of steering control for merging.

NORMAL **EVENT:** **S2.5**
FUNCTIONS: **OF10** - V1, V3, V6
CONSEQUENCES: Same **as** (SS2.4)
RESPONSES:
DRIVER: **Takes** over only the steering control.
VEHICLE: If time permits, stop the vehicle. Otherwise, instruct the driver to take over only the steering control while it slows down.

(SS2.7) Vehicle **on an** automated on-ramp is incapable of merging into the existing traffic on **the** *AHS* at the merging location due to **loss** of coordination control.

NORMAL EVENT: ***S2.5***
FUNCTIONS: **OF12** - RC3,RC4, RC5, RC8a, RC13, **V13**
CONSEQUENCES: Same **as** (SS2.4)
RESPONSES:
VEHICLE: Slows down; stops after entering the automated lane.

(Travel in Automated Lanes:)

(SS2.8) Vehicle fails to slow down to keep a safety distance behind the vehicle in front due to **a** failure of headway control.

NORMAL EVENT;: **S2.7**
FUNCTIONS: OF6 - V1, V4, V6, (V13, RC5A, RC13)
CONSEQUENCES: Collisions
RESPONSES:
DRIVER: Takes over only the longitudinal control.
VEHICLE: **Warns** the driver to take over only the longitudinal control.

(SS2.9) Vehicle fails to **speed up** to be at a safety distance behind the vehicle in front due to propulsion failure.

NORMAL **EVENT:** **S2.8** and **S2.9**
FUNCTIONS: OF5 - V1, V4, V6
CONSEQUENCES: Slow down of traffic in its current lane.
RESPONSES:
VEHICLE: Stops.

(SS2.10) Vehicle loses all automatic control while moving along a lane.

NORMAL **EVENT:** ***S2.6*** - **S2.9.**
FUNCTIONS: OF8; **OF5**, OF6, OF7
CONSEQUENCES: Collisions with neighboring vehicles, including vehicles in the same lane and those in neighboring lanes.

RESPONSES:

DRIVER: **Takes** over at least the lateral control immediately with the option **of** taking over total control simultaneously and immediately.

(SS2.11) Vehicle loses **speed** control while changing lane.

NORMAL EVENT: S2.10 & S2.12
FUNCTIONS: **OF5** - V1, **V4,** V6
CONSEQUENCES: **Abort of** the lane-change maneuver; collisions.
RESPONSES:

DRIVER: **Takes** over only the longitudinal control if the lane change *can* be safely completed. Otherwise, take over both the longitudinal and lateral control and abort the lane change.

VEHICLE: Decides whether to complete the lane change **or** abort **and instructs** the driver to take over the longitudinal control.

(SS2.12) Vehicle loses headway control while changing lane.

NORMAL EVENT: S2.10 & S2.12
FUNCTIONS: **OF6** - V1, V4, V6, (V13, RCSA, RC13)
CONSEQUENCES: Abort **of** the lane-change maneuver; collisions
RESPONSES: Same **as** SS2.11.

(SS2.13) Vehicle loses longitudinal position control while changing lane.

NORMAL EVENT: S2.10 & S2.12
FUNCTIONS: **OF7** - V1, V4, V6
CONSEQUENCES: Abort of the lane-change maneuver; collisions.
RESPONSES: Same **as** SS2.11.

(SS2.14) Vehicle loses control of steering for lane change while changing lane.

NORMAL EVENT: S2.10 & **S2.12**
FUNCTIONS: OF9 - V1, V3, V6
CONSEQUENCES: Abort of the lane-change maneuver; collisions.
RESPONSES:

DRIVER: Takes over only the steering control; decides whether to abort the lane change.

VEHICLE: **Warns** the driver to take over only the steering control. Provides guidance as to whether the lane change should be aborted.

(SS2.15) Vehicles lose coordination during a lane change maneuver.

NORMAL EVENT: S2.10 & S2.12
FUNCTIONS: OF12 - (RC3, RC4, RC5, RC6, RC8a, RC13, V13)
CONSEQUENCES: Abort of the lane-change maneuver; collisions.
RESPONSES:
VEHICLE: Decides, using on-board sensors only, whether to steer back or to complete the lane change.

(SS2.16) Vehicles lose all automatic control during a lane change maneuver.

NORMAL EVENT: S2.10 & S2.12
FUNCTIONS: OF9; OF5, OF6, **OF7**
CONSEQUENCES: **Abort** of the lane-change maneuver; collisions.
RESPONSES:
DRIVER: **Takes** over total control and aborts the lane change if safe.

(SS2.17) Vehicle fails to slow down to create a safe spacing between itself and the vehicle in front for another vehicle to change lane from a neighboring lane to the front of the vehicle.

NORMAL EVENT: S2.11
FUNCTIONS: OF6 - V1, V4, V6
CONSEQUENCES: Abort the lane change maneuver.
RESPONSES:
DRIVER: **Takes** over the longitudinal control and slows down but only after the vehicle detects the failure and instructs the driver to do so. (The driver does not know that the vehicle should slow down to receive a lane-changing vehicle.) Note that the slow down is not to allow the lane change but to remove the vehicle from the **AHS** safely.
VEHICLE: If the vehicle *can* detect the failure, it instructs the driver to take over. (The ability of the vehicle to detect such a failure is a design feature, even when the sensors function properly.)

(SS2.18) Vehicle fails to abort a lane change when it is necessary to do so.

NORMAL EVENT: S2.13
FUNCTIONS: OF12 - (RC3, RC4, RC5, RC6, RC8a, RC13, V13)
CONSEQUENCES: Collisions are likely to occur before the driver could respond.
RESPONSES:
DRIVER: **Takes** over only the steering control.
VEHICLE: The on-board sensors of the lane-change vehicle should be able to detect the danger and **warn** the driver to **take** over only the steering control.

(SS2.19) Vehicle aborts a lane change for safety but loses the control of steering.

NORMAL **EVENT:** S2.13
FUNCTIONS: **OF9 - V1, V3, V6**
CONSEQUENCES: Possibly collisions
RESPONSES:
DRIVER: **Takes** over only the steering control and steers back to the original lane.
VEHICLE: **Warns** the driver to take over steering control.

(SS2.20) Vehicles on the ending lane fail to merge into the traffic on the continuing lane **at** the location of a lane merge.

NORMAL **EVENT:** S2.14 & S2.15
FUNCTIONS: **(See** SS2.4 - SS2.7)
CONSEQUENCES: **(See** SS2.4 - SS2.7)
RESPONSES: **(See SS2.4 - *SS2.7)***

(SS2.21) Vehicle loses tracking controi while moving along on the Same lane.

NORMAL EVENT: Any lane-flow events (e.g. S2.7)
FUNCTION: **OF8 - V1, V3, V6**
CONSEQUENCES: Collisions
RESPONSES:
DRIVER: Takes over only the steering control.
VEHICLE: **Warns** the driver to take over only the lateral control while decelerating.

(SS2.22) Vehicle fails to diverge into the added lane at the location **of** a lane division due to **loss** of steering control (for diverging).

NORMAL EVENT: S2.16 **& S2.17**
FUNCTIONS: OF11 - V1, **V3,** V6, (RC3, RC8a, RC13)
CONSEQUENCES: Collisions
RESPONSES: Same **as SS2.21.**

(SS2.23) While moving on the **AHS,** vehicle detects component failure via the on-board monitoring function.

CONSEQUENCES: Operational function failures if further component failures occur.
RESPONSES:
VEHICLE: Determines the necessary response to the component failure. Informs the roadside control system and the surrounding vehicles of the next course of actions. Actions may include automated driving off the

AHS, slowdown followed by stop and take-over etc. The exact response depends on the nature of the component failure.

(Exit Automated Lanes:)

(SS2.24) The vehicle fails to enter the exit **ramp** due to loss of steering control.

NORMAL EVENT: S2.18
FUNCTIONS: OF11 - V1, V3, V6, (RC3, RC8a, RC13)
CONSEQUENCES: Collisions
RESPONSES: Same **as** SS2.21

(Exit the System:)

(SS2.25) Driver is not ready to take over control, but the control is switched back to manual **anyway.**

NORMAL EVENT: S2.19 & 2.20
FUNCTIONS: OF20 - H1c,d, V8, V11
CONSEQUENCES: Vehicle under no control.
RESPONSES:
DRIVER: If the driver becomes ready in time, he/she takes over control.
VEHICLE: **(If** vehicles *can* be switched into automated driving mode on the automated off-ramp, the driver *can* request a transition into the automated driving mode and have the vehicle automatically driven to the repository automatically.) **If** vehicle detects lack of driver control of the vehicle, perhaps through the erratic manual driving, it returns to automatic control.

(SS2.26) Driver is ready to take over control but the control cannot be switched to manual.

NORMAL **EVEN":** S2.19 & **S2.20**
FUNCTIONS: OF20 -
CONSEQUENCES: The vehicle will be driven to the repository automatically.
RESPONSES: No responses necessary.

(SS2.27) Driver is not ready to take over control and the vehicle fails **to** enter the automated vehicle repository at exit point.

NORMAL EVENT: S2.21
FUNCTIONS: OF5 - V1, V4, V6
OF6 - V1, V4, V6
OF8 - V1, V3, V6
OF11 - V1, V3, V6, (RC3, RC8a, RC13)

CONSEQUENCES: **Collisions**

RESPONSES:

DRIVER: If **the driver becomes ready, hdshe takes over control.**

APPENDIX C: MAJOR FAILURE EVENTS FOR SS3

In the following list, we use these abbreviations:

NORMAL OPERATIONAL EVENT:	NORMAL EVENT
OPERATIONAL FUNCTIONS - ELEMENTAL FUNCTIONS:	FUNCTIONS
POSSIBLE CONSEQUENCES OF THE FAILURE:	CONSEQUENCES
EXAMPLE RESPONSES:	RESPONSES
DRIVER OF THE FAILED VEHICLE:	DRIVER
FAILED VEHICLE:	VEHICLE
OTHER (FUNCTIONING) VEHICLES IN THE PLATOON	PLATOON
OTHER PLATOONS AND ROADSIDE CONTROL SYSTEM:	OTHERS

Note that the absence of a specific item implies the absence of event-specific reactions. Parenthesized headings indicate the phase of normal operation.

As in Appendix 1, we give an example illustrating how to interpret the abbreviated event list. Consider the event (SS3.16) as follows.

Full Description:

(SS3.16) Lead vehicle loses control of steering for lane change while the platoon is changing lane from the transition lane to the neighboring automated lane through a gate.

NORMAL OPERATIONAL EVENT: S3.16

OPERATIONAL FUNCTIONS — ELEMENTAL FUNCTIONS: OF9 - V1, V3, V6

POSSIBLE CONSEQUENCES OF THE FAILURE:

Abort of the lane-change maneuver; collisions. The failed lead vehicle may collide with the barriers, or collide into one end of a barrier, which may cause serious subsequent collisions. It may also collide into the barriers after having entered the destination lane safely.

EXAMPLE RESPONSES:

DRIVER OF THE FAILED VEHICLE:

If the failure is caused by the failure of sensors, we assume that the vehicle cannot detect the failure by itself. But, the driver may detect it. Upon detection, driver takes over only the steering control and determines whether to continue the lane change or abort it.

FAILED VEHICLE:

Upon driver take-over, the vehicle informs the roadside control system and the surrounding vehicles of the human intervention.

If the failure is caused by non-sensing failures, the vehicle can detect the failure by itself. Note that the surrounding vehicles can detect the failure through the erratic vehicle behavior. In such a case, they inform the roadside control system, which in turn informs the failed vehicle and all the surrounding vehicles. If the warning mechanism still works, the vehicle, upon self-detection or notification, informs the driver of the failure and instructs the driver to take over only the steering control. Also, the failed lead vehicle provides guidance to the driver as to whether to abort the lane change.

Upon detection, the failed vehicle also informs the roadside control system and the surrounding vehicles simultaneously. The failed lead vehicle determines a break point for abort of the platoon lane change. (A potential problem with aborting the platoon lane change is that there may be manually driven vehicles changing lane into the transition lane from the neighboring manual lane under the assumption that the full platoon would enter the automated lane. An alternative is to leave the abort decision to the individual vehicles in the platoon.)

The failed vehicle, either after the driver has resumed complete manual control or after it has been slowed down or stopped automatically, has to be removed, under its own force or towed, from the AHS between lane barriers, through lane-change gates and through an automated off-ramp or the transition lane.

The vehicle as well as the roadside control system memorize the failure or the take-over attempt. The failed vehicle's further requests for reentry to the automated lanes or the transition lane will be denied until the vehicle has been inspected at an off-highway station and certified to be fit for automated driving again. Note that the denial following a take-over attempt may deter the abuse of emergency take-over procedure during normal transition back to manual control.

OTHER (FUNCTIONING) VEHICLES IN THE PLATOON:
Even if the failure is not detected by the vehicle itself and its driver, the surrounding vehicles may be able to detect it based on the erratic behavior of the failed vehicle. If so, they inform the roadside control system, which in turn informs the failed vehicle itself and all the surrounding vehicles.

OTHER PLATOONS AND ROADSIDE CONTROL SYSTEM:
Upon notification of failure or take-over. the roadside control system in conjunction with the surrounding (functioning) vehicles calls off all pending or planned maneuvers, instructs platoons to abort maneuvers currently being executed, isolates the failed vehicles and slows down the traffic for safety. (An operational communication link is assumed.) In addition, the roadside control system allows no additional manually-driven vehicles to enter the transition lane near the scene (i.e. by not granting permission to enter). Furthermore, it warns the manually-driven but automation-equipped vehicles of the danger and advises them to move away from the failed vehicle (as part of the attempt to isolate the failed vehicle).

Abbreviated Description:

(SS3.16) Lead vehicle loses control of steering for lane change while the platoon is changing lane from the transition lane to the neighboring automated lane through a gate.

NORMAL EVENT: S3.16
FUNCTIONS: **OF9** - V1, V3, V6
CONSEQUENCES: Abort of the lane-change maneuver; collisions. The failed lead vehicle may collide with the barriers, or collide into one end **of** a barrier, which may cause serious subsequent collisions. It may **also** collide into the barriers after having entered the destination lane safely.

RESPONSES:
DRIVER: Takes over only the steering control; determines whether to continue the lane change or abort it.
VEHICLE: Same **as** SS3.13. **Also,** provide guidance **as** to whether to abort the lane change.

The abbreviated event list follows:

THE EVENT LIST:

(Enter System - From the Transition Lane:)

(SS3.1) Non-automation-equipped vehicle enters the transition lane.

CONSEQUENCES: Interfering with the normal operation of the AHS and interrupting the traffic on the transition lane and the traffic in and out **of** the automated lanes.
RESPONSES: No recourse.

(SS3.2) Roadside control system fails to detect and reject an impaired vehicle on the transition lane.

NORMAL EVENT: S3.4
FUNCTIONS:
CONSEQUENCES: Impaired vehicles allowed on the automated lanes; see the rest of the failure events for possible consequences. Note that this may be a serious failure event because the safety of the AHS may heavily depend on the ability of the inspection function (and perhaps **also** the real-time on-board monitoring function) to minimize the failure probability. Also note that the inspection is performed while the vehicle is moving.

RESPONSES:

DRIVER: No reaction.

VEHICLE: If vehicle itself detects impairment after entry and before failure, then follow the common notification procedure and the common reaction (i.e. isolation and traffic slowdown).

(SS3.3) Vehicle fails to switch from manual to automated mode on the transition lane but mistakenly informs the driver that the transition has been **successfully** completed.

NORMALEVENT: **s3.5**
FUNCTIONS: OF3
CONSEQUENCES: Vehicle not under any control; collisions
RESPONSES:

DRIVER: Resumes manual control and drives the vehicle out **of** the transition lane and back to the manual lanes.

(SS3.4) Vehicle fails to switch from manual mode to automated mode on the transition lane (but the vehicle does not misinform the driver of a transition **success), although** the vehicle passed the inspection.

NORMAL EVENT: **S3.5**
FUNCTIONS: 0F3
CONSEQUENCES: Automated driving impossible
RESPONSES:

DRIVER: Take over total control; leave the transition lane for the manual lanes.

(SS3.5) An accident on the manual lanes is "spilled" into the transition lane.

CONSEQUENCES: Multiple serious collisions, perhaps involving platoons of vehicles and manual vehicles

RESPONSES: No recourse other than common reactions. (Note that disallowing vehicles to enter the transition lane near the scene until the accident has been cleared **is** part **of** the common response to failure events resulting from vehicle failures on the transition lane.)

(SS3.6) While vehicle speeding up to form one single platoon with the platoon in front on the transition lane, a manually driven vehicle cuts in front of the platoon causing the platoon to decelerate fast.

EVENT: **S3.7 & S3.8**
CONSEQUENCES: Causing the speeding-up vehicle to collide with the platoon from its rear with a high relative speed; subsequent collisions possible.
RESPONSES: No event-specific recourse.

(SS3.7) Vehicle cannot form a platoon with the other vehicles on the transition lane.

NORMAL EVENT: S3.7
FUNCTIONS: OF12; OF5, OF6
CONSEQUENCES: Vehicle cannot use the AHS. (This failure may indicate other problems too.)
RESPONSES:
DRIVER: Take over total control; drive the vehicle off the transition lane back to the manual lanes.

(Enter System - From an Automated On-Ramp:)

(SS3.8) The roadside system fails to detect and reject an impaired vehicle at the automated entrance. (Same as SS2.1.)

(SS3.9) Vehicle fails to switch from manual mode to automated mode on an automated on-ramp, after the vehicle passes the inspection. (Same as SS2.2.)

(SS3.10) Vehicle fails to switch from manual to automated mode on an automated on-ramp, but the vehicle mistakenly informs the driver that the transition has been successfully completed. (Same as SS2.3.)

(SS3.11) Vehicle fails to form a platoon with other vehicles on an automated entrance.

EVENT: S3.14
FUNCTIONS: OF5, OF6, OF12
CONSEQUENCES: Vehicle cannot use the automated lanes. (This failure may indicate other potential problems. This possible failure necessitates a manual ramp off the automated on-ramp after the preplatooning area.)
RESPONSES:
VEHICLE: Move off the automated on-ramp to the manual off-ramp.
DRIVER: After the vehicle has been moved off the automated on-ramp, driver takes over full control of the vehicle and leaves AHS.

(Enter Automated Lane — from the Transition Lane:)

(SS3.12) Non-automation-equipped vehicle enters the automated lanes from the transition lane.

CONSEQUENCES: This could lead to serious danger.
RESPONSES:
OTHERS: Roadside control system in conjunction with the surrounding vehicles isolates the intruder, slows down and stops the traffic. Dispatch AHS patrol units to the scene, either in automated vehicles using the automated and manual lanes or in manual vehicles using only the manual lanes.

(SS3.13) Lead vehicle of a platoon loses **speed** control while the platoon is changing lane from the transition lane to the neighboring automated lane through a gate. (It is assumed that while a platoon changes lane from the transition lane to the neighboring automated lane, it is not **allowed,** for safety reasons, to simultaneously join another platoon.)

NORMAL EVENT: S3.16
FUNCTIONS: **OF5 - V1, V4, V6**
CONSEQUENCES: Abort of the lane-change maneuver; collisions. Since no vehicles are in the sensing range **ahead** on the destination lane **and** the headway control function is assumed to be functioning, collisions with the vehicle or platoon **ahead** are not likely.
RESPONSES:
DRIVER: **No** take-over **of** any kind.
VEHICLE: Determines a break point for abort; a potential problem with aborting the platoon lane change is that there may be manually driven vehicles changing lane into the transition lane from the neighboring manual lane under the assumption that the full platoon would enter the automated lane. (An alternative is to leave the abort decision to the individual vehicles in the platoon.)
PLATOON: Abort the lane change **as** instructed by the lead vehicle. (Alternatively, abort if judged safe by the individual vehicles.)

(SS3.14) Lead vehicle of a platoon loses headway control while the platoon is changing lane from the transition lane to the neighboring automated lane through a gate.

NORMAL EVENT: S3.16
FUNCTIONS: **OF6 - V1, V4, V6, (V13, RCSA, RC13)**
CONSEQUENCES: Abort of the lane-change maneuver; collisions with the platoon **ahead** in the destination lane **and** other platoons.
RESPONSES: Same **as SS3.13.**

(SS3.15) Lead vehicle loses longitudinal position control while the platoon is changing lane from the transition lane to the neighboring automated lane through a gate.

NORMAL **EVENT:** **S3.16**
FUNCTIONS: OF7 - **V1, V4, V6**
CONSEQUENCES: Same **as SS3.14.**
RESPONSES: Same **as SS3.13.**

(SS3.16) **Lead** vehicle loses control of steering for lane change while the platoon is changing lane from the transition lane to the neighboring automated lane through a gate.

NORMAL **EVENT:** **S3.16**
FUNCTIONS: **OF9** - V1, **V3, V6**
CONSEQUENCES: Abort of the lane-change maneuver; collisions. The failed lead vehicle may collide with the barriers, or collide into one end **of a** barrier, which may cause serious subsequent collisions. It may **also** collide into the barriers after having entered the destination lane safely.
RESPONSES:
DRIVER: Takes over only the steering control; determines whether to continue **the** lane change or abort it.
VEHICLE: Same **as SS3.13.** Also, provide guidance **as** to whether to abort the lane change.

(SS3.17) Vehicles lose coordination during a lane change maneuver **from** the transition lane to ***the*** neighboring automated lane through a gate.

NORMAL **EVENT:** **S3.16**
FUNCTIONS: **OF12** - (RC3, **RC4,** RC5, **RC6,** RC8a, RC13, **V13)**
CONSEQUENCES: Abort of the lane-change maneuver; collisions. This could be a very dangerous event, perhaps leading to multiple serious collisions involving multiple platoons and manual vehicles.
RESPONSES:
DRIVER: Same **as SS3.13.**
VEHICLE: Abort (i.e. return to the transition lane) if safe.
PLATOON: Abort (**i.e.** return to the **transition** lane) if safe.

(SS3.18) Lead vehicle loses **all** automatic control while the platoon is changing lane from the transition lane to the neighboring automated lane through a gate. (Note that this event is caused by multiple functional failures on the lead vehicle.)

NORMAL **EVENT:** **S3.16**
FUNCTIONS: **OF8,** OF9; OF5, **OF6, OF7**
CONSEQUENCES: Abort of the lane-change maneuver; collisions. This is a very dangerous event. The possible consequences include those **stated** in **(SS3.13)** - **(SS3.17).** The failed vehicle could plunge into the manual traffic too.
RESPONSES: Same **as SS3.16.** (Driver takes over only steering control.)

(SS3.19) Trailing vehicle of a platoon loses headway control while the platoon is changing lane from the transition lane to the neighboring automated lane through a gate.

NORMAL EVENT: **S3.16**
FUNCTIONS: **OF6** - V1, **V4, V6,** (V13, **RCSA,** RC13)
CONSEQUENCES: Same **as SS3.14.**
RESPONSES: Same **as SS3.17.**

(SS3.20) **Trailing** vehicle loses longitudinal position control while the platoon is changing lane from the transition lane to the neighboring automated lane through a gate.

NORMAL EVENT: **S3.16**
FUNCTIONS: **OF7 - V1, V4, V6**
CONSEQUENCES: Same **as SS3.15.**
RESPONSES: Same **as SS3.17.**

(SS3.21) Trailing vehicle of **a** platoon loses control of **steering** for lane change while changing lane **from** the transition lane to the neighboring automated lane through a gate.

NORMAL EVENT: **S3.16**
FUNCTIONS: **OF9 - V1, V3, V6**
CONSEQUENCES: Same **as SS3.16.**
RESPONSES: Same **as SS3.16.**

(SS3.22) Trailing vehicle of a platoon loses **all** automatic control while changing lane from **the** transition lane to the neighboring automated lane through a gate.

NORMAL EVENT: **S3.16**
FUNCTIONS: **OF, OF6, OF7;** OF8, **OF9**
CONSEQUENCES: Same **as SS3.18.**
RESPONSES: Same **as SS3.21.**

(Enter Automated **Lanes — From** an Automated On-Ramp:)

(SS3.23) Lead vehicle of a platoon loses its **speed** control while the platoon **is** merging from **an** automated on-ramp into the existing automated traffic on the *AHS* at the merging location. (Recall that it is assumed that while a platoon is merging into the existing traffic, it is not allowed, for safety reasons, to simultaneously join any other platoon and form one single platoon.)

NORMAL EVENT: **S3.17**
FUNCTIONS: OF5 - V1, **V4, V6**
CONSEQUENCES: Serious collisions with the vehicles already on the automated lanes.
RESPONSES:
DRIVER: *Takes* over only the longitudinal control only after the platoon has safely entered the neighboring automated lane.
VEHICLE: If the **loss** of control is caused by propulsion failure, stop the vehicle by automatic braking. If the automatic braking failed, have the driver take over the longitudinal control **and** stop the vehicle.
NOTE: **We** assume that there is not sufficient extra space at the merge location for a **safe** abort. However, if such a space is available, an abort may be viable.

(SS3.24) Lead vehicle loses its longitudinal position control while the platoon is merging from an automated on-ramp into the automated traffic on the AHS at the merging location.

NORMAL **EVENT:** **S3.17**
FUNCTIONS: **OF7** - V1, **V4, V6**
CONSEQUENCES: Same as **(SS3.23).**
RESPONSES: Same as **(SS3.23).**

(SS3.25) A member vehicle of a platoon (a lead vehicle or a trailing vehicle) loses its headway control while the platoon is merging from an automated on-ramp into the automated traffic on the **AHS** at the merging location.

NORMAL EVENT: **S3.17**
FUNCTIONS: **OF7** - V1, **V4, V6**
CONSEQUENCES: Same as **(SS3.23).**
RESPONSES: Same as **(SS3.23).**

(SS3.26) A member vehicle of a platoon (a lead vehicle or a trailing vehicle) loses its steering control (for merging) while the platoon is merging from an automated on-ramp into the existing automated traffic on the **AHS** at the merge location.

NORMAL EVENT: **S3.17**
FUNCTIONS: **OF10** - V1, **V3, V6**
CONSEQUENCES: Same as **(SS3.23)**
RESPONSES:
DRIVER: Takes over only the steering control.

(SS3.27) Lead vehicle loses all automatic control while the platoon is merging from an automated on-ramp into the automated traffic on **AHS** at the merging location.

NORMAL EVENT: **S3.17**
FUNCTIONS: **OF7** - V1, V4, V6
CONSEQUENCES: Same as **(SS3.23).**
RESPONSES:
DRIVER: Takes over only the steering control initially; takes over total control only after the platoon has entered the neighboring automated lane.

(SS3.28) Platoon on an automated on-ramp is incapable of merging into the existing traffic on the **AHS** at the merging location due to loss of coordination control.

NORMAL EVENT: **S3.17**
FUNCTIONS: **OF12** - RC3,RC4, RC5, RC8a, RC13, **V13**
CONSEQUENCES: Same as **(SS3.23)**

RESPONSES:

OTHERS: **Abort** the merge, i.e. stop the entering platoon on the on-ramp, if safe. Otherwise, there is no recourse except that platoons should try to avoid collisions using their on-board collision avoidance devices.

(Travel in Automated **Lanes:)**

(SS3.29) Platoon fails to slow down to **keep** a safety distance behind the platoon in front due to **a** failure of the lead vehicle's headway control.

NORMAL EVENT: **S3.19**
FUNCTIONS: **OF6**
CONSEQUENCES: Collisions, perhaps involving platoons.
RESPONSES:

DRIVER: **Takes** over only the longitudinal control initially.

(SS3.30) The lead vehicle of a platoon, while the platoon is speeding up to join the platoon in front, **loses** its headway control.

NORMAL EVENT: **S3.20 & S3.21**
FUNCTIONS: **OF6**
CONSEQUENCES: Collision with the platoon in front.
RESPONSES: Same **as SS3.29.**

(SS3.31) Platoon, while speeding up to join the platoon in front, loses coordination control.

NORMAL EVENT: **S3.20 & S3.21**
FUNCTIONS: **OF12**
CONSEQUENCES: Collision with the platoon in front.
RESPONSES: Same **as SS3.29.**

(SS3.32) Lead vehicle of a platoon loses **speed** control while the platoon is changing lane from one automated lane to a neighboring automated lane through a gate and in the meantime joining another platoon from its front.

NORMAL EVENT: **S3.24** & **S3.25**
FUNCTIONS: OF5
CONSEQUENCES: **Abort** of the lane-change maneuver; collisions. Since no vehicles are in the sensing range ahead on the destination lane, imminent collisions with vehicles in front are not likely. However, since the platoon is joining another platoon upon entering the destination automated lane from its front. losing **speed** control may cause collisions with the receiving platoon if its actual **speed** is lower than the planned speed.

RESPONSES:

DRIVER: No driver take-over of any kind.

VEHICLE: Determines a break point for abort; an additional factor in determining the breakpoint is the presence and the movement of the receiving platoon in the destination lane. (An alternative is selfdetermination.)

OTHERS: The receiving platoon should slow down to avoid a collision with the lane-changing platoon particularly if the actual speed is lower than planned.

(SS3.33) Lead vehicle of a platoon loses headway control while the platoon is changing lane from one automated lane to a neighboring automated lane to join another platoon from its front through a gate.

NORMAL **EVENT:** **S3.24 & S3.25**

FUNCTIONS: **OF6**

CONSEQUENCES: Abort of the lane-change maneuver; collisions. **Since** there is a platoon ahead in the destination lane, a collision with that platoon is possible. Also, since the lane-changing platoon is joining the receiving platoon upon entry into the destination lane from its front, a collision **with** that platoon is also possible.

RESPONSES: Same **as SS3.32.**

(SS3.34) Lead vehicle loses longitudinal position control while the platoon **is** changing lane from one automated lane to a neighboring automated lane to join another platoon from its front through a gate.

NORMAL **EVENT:** **S3.24 & S3.25**

FUNCTIONS: OF7

CONSEQUENCES: **Abort** of the lane-change maneuver; collisions. **Since** there may be platoon ahead in the destination lane, a collision with that platoon is possible. Since the lane-changing platoon is joining the receiving platoon upon entry into the neighboring lane, a collision with that platoon is also possible.

RESPONSES: Same **as SS3.32.**

(SS3.35) Lead vehicle loses control of steering for lane change while the platoon is changing lane from one automated lane to a neighboring automated lane to join another platoon from its front through a gate.

NORMAL EVENT: **S3.24 & S3.25**

FUNCTIONS: OF9

CONSEQUENCES: The failed lead vehicle **may** collide with the barriers, or collide into one end of a barrier. which may cause serious subsequent collisions. It may collide into the barriers after having entered the destination lane

safely.

RESPONSES:

DRIVER: *Takes* over only the steering control.

OTHERS: The receiving platoon should slow down to avoid a collision with the lane-changing platoon. A factor in determining the breakpoint is the presence and the movement of the receiving platoon. (An alternative is self-determination,)

(SS3.36) Lead vehicle loses **all** automatic control while the platoon is changing lane from one automated lane to a neighboring automated lane to join another platoon from its front **through** a gate.

NORMAL EVENT: **S3.24 & S3.25**

FUNCTIONS: OF8, OF9; OF5, OF6, **OF7**

CONSEQUENCES: The failed lead vehicle may collide with the barriers, or collide into one end **of** a barrier, which may cause serious subsequent collisions. It may collide into the barriers after having entered the destination lane safely. The platoon may collide with the receiving platoon and even other vehicles in the destination lane. This is a very dangerous event.

RESPONSES: Same **as SS3.35.**

(SS3.37) Platoons lose coordination control while a platoon is changing lane from one automated lane to a neighboring automated lane to join another platoon from its front through a gate.

NORMAL EVENT: **S3.24** and **S3.25**

FUNCTIONS: **OF12**

CONSEQUENCES: Same **as SS3.34.**

RESPONSES: Same **as SS3.32.**

(SS3.38) Trailing vehicle of a platoon loses headway control while the platoon is changing lane from one automated lane to a neighboring automated lane to join another platoon from its front through a gate.

NORMAL EVENT: **S3.24 & S3.25**

FUNCTIONS: **OF6**

CONSEQUENCES: Same **as SS3.33.**

RESPONSES:

DRIVER: **No** take-over of any kind.

VEHICLE: Abort if safe.

PLATOON: Abort if safe.

(SS3.39) Trailing vehicle of a platoon loses control of steering for lane change while the platoon is changing lane from one automated lane to a neighboring automated lane from its front through a gate.

NORMAL EVENT: **S3.24 & S3.25**
FUNCTIONS: **OF9**
CONSEQUENCES: Abort of the lane-change maneuver; collisions. The failed vehicle may **collide** into the barriers or with one end of a barrier, which may **cause** serious subsequent multiple collisions involving multiple platoons.
RESPONSES:
DRIVER: **Takes** over only the steering control.
VEHICLE: **Provides** guidance about the steering direction, i.e. whether to complete the lane change or to steer back to the original lane.

(SS3.40) Trailing vehicle of a platoon loses all automatic control while the platoon is changing lane from one automated lane to a neighboring automated lane from its front through a gate.

NORMAL **EVENT: S3.24** & S3.25
FUNCTIONS: OF8, OF9; OF5, OF6, **OF7**
CONSEQUENCES: Same **as SS3.36.**
RESPONSES: Same **as SS3.39.**

Failure events occurring while a platoon is changing lane from one automated lane to a neighboring automated lane through a gate to join another platoon from its rear are similar to their counterparts where the platoon is changing lane to join another platoon from its front. Actually, they may be safer and simpler, in terms of human factors, because the space between the receiving platoon and its following platoon in the destination lane is much larger compared to the amount of space (literally none) available for emergency maneuver in the other **case.** (Implicitly assumed here **is** that any emergency maneuver would involve deceleration. Consequently, more space behind the "failed platoon" is safer.) Therefore, we omit the discussion of these events.

(SS3.41) Lead vehicle of a platoon loses headway control while the platoon is changing lane from one automated lane to a neighboring automated lane in the middle (i.e. by moving into a short gap temporarily created for the lane change) through a gate. (Note that this gap could be much shorter than the minimum inter-platoon spacing.)

NORMAL EVENT: **S3.30**
FUNCTIONS: OF6
CONSEQUENCES: Abort of the lane-change maneuver; collisions. Since there **is** a platoon a short distance ahead and a short distance behind too in the destination lane, this could be very dangerous and multiple collisions involving the adjacent platoons may result.

RESPONSES:

DRIVER: **No** take-over of any kind.

VEHICLE: **A** factor in determining the breakpoint **is** the presence and the movement **of** the two parts of the receiving platoon in the destination lane.

OTHERS: The rear part **of the** receiving platoon should slow down to avoid a collision with the lane-changing platoon while the front part may need to accelerate.

(SS3.42) Lead vehicle loses longitudinal position control while **the** platoon is changing lane from one automated lane to a neighboring automated lane in the middle (i.e. by moving **into** a short gap temporarily created for the lane change) through **a** gate.

NORMAL **EVENT: S3.30**
FUNCTIONS: OF7
CONSEQUENCES: Same **as SS3.41.**
RESPONSES: Same **as SS3.41.**

(SS3.43) Lead vehicle loses control **of** steering for lane change while the platoon is changing lane from one automated lane to a neighboring automated lane by moving into a (short) gap temporarily created for the lane change through a gate.

NORMAL EVENT: S3.30
FUNCTIONS: OF9
CONSEQUENCES: The lead vehicle may collide into the barriers or one end of a barrier, which may cause serious multiple collisions involving multiple platoons. It may also collide into the barriers after it has entered the destination lane safely.
RESPONSES: Same **as SS3.41.**

(SS3.44) Lead vehicle loses all automatic control while the platoon **is** changing lane from one automated lane to a neighboring automated lane by moving into a (short) gap temporarily created for the lane change through a gate.

NORMAL EVENT: S3.30
FUNCTIONS: OF8, OF9; OF5, OF6, OF7
CONSEQUENCES: This **is a** very dangerous event. The possible consequences include those stated in **(SS3.41)- (SS3.43)** and beyond.

RESPONSES:

DRIVER: Takes over only the steering control.

PLATOON: The trailing vehicles decide whether to continue the lane change or to return to the original lane.

(SS3.45) Two platoons lose coordination while one of them is changing lane from one automated lane to a neighboring automated lane into the middle of the other platoon through a gate.

NORMAL EVENT: S3.30
FUNCTIONS: OF12
CONSEQUENCES: Same as SS3.41.
RESPONSES: Same as SS3.41.

(SS3.46) Trailing vehicle of a platoon loses headway control while the platoon is changing lane from one automated lane to a neighboring automated lane to join another platoon in the middle through a gate.

NORMAL EVENT: S3.30
FUNCTIONS: OF6
CONSEQUENCES: Same as SS3.41.
RESPONSES: Same as SS3.41 except that an additional factor in determining the break-point is the position of the failed trailing vehicle.

(SS3.47) Trailing vehicle of a platoon loses control of steering for lane change while the platoon is changing lane from one automated lane to a neighboring automated lane in the middle through a gate.

NORMAL EVENT: S3.30
FUNCTIONS: OF9
CONSEQUENCES: Same as SS3.40.
RESPONSES: Same as SS3.40.

(SS3.48) Trailing vehicle loses all automatic control while the platoon is changing lane from one automated lane to a neighboring automated lane by moving into a (short) gap temporarily created for the lane change through a gate.

NORMAL EVENT: S3.30
FUNCTIONS: OF8, OF9; OF5, OF6, OF7
CONSEQUENCES: Same as SS3.44.
RESPONSES: Same as SS3.44.

(SS3.49) Platoon fails to abort a lane change through a gate.

NORMAL EVENT: S3.32
Note that a lane-change abort may result from failures of vehicles in other platoons.
FUNCTIONS: OF9, OF15

CONSEQUENCES: The exact consequences of this failure depends on the exact circumstances of the failure. However, it could cause serious multiple collisions. Note that this event occurs during the normal operational event **S3.32** "Abort a platoon lane change (due to unexpected change in traffic movement) and not after a failure of any operational functions.

RESPONSES: If the abort is needed because the vehicles ahead in the destination lane have unexpectedly decelerated, the lanechanging platoon (as well as the vehicles behind in the destination lane) should at least decelerate accordingly. If the abort is needed because the vehicles behind in the destination lane have unexpectedly accelerated, the continuation of the lane change maneuver through the gate may pose danger too. If the continued lane change is detected by the accelerating platoon, it should then decelerate fast to avoid collisions.

Merging Failures: Failure events occurring while a platoon is merging from the ending lane into the automated traffic on the continuing lane at the location of a lane merge (normal operational events **S3.33** and **S3.34)** are similar, in terms of human factors implications, to those failure events (e.g. **S3.17)** occurring while a platoon is merging from an automated on-ramp into the automated traffic on the neighboring automated lane. Therefore, they are omitted; refer to events **(SS3.22) - (SS3.25)** for a detailed description.

Diverging Failures: Failure events during traffic diverging at the location of a lane division **(S3.35** and **S3.36)** are special cases, in terms of human factors implications, of those failure events occurring during a regular lane change through a gate because, unlike at the regular lane-change gate, there is no traffic from upstream into the added lane (except from the gate). (Exit Automated Lanes — to the Transition Lane:)

Failure events occurring while a platoon is exiting the automated lanes into the transition lane **(S3.37)** are similar to those occurring while a platoon is making a regular lane change through a gate except that there may be manually driven vehicles on the transition lane. The unpredictability of human drivers' behavior gives rise to a new dimension in the possible consequences and responses.

Major Qfferences from the responses stated in those events are (i) the difficulty in isolating the failed platoon because the manually driven vehicles cannot be controlled by the system and (ii) the extra factor for consideration in calculating the break-point.

We choose to state these more complicated failure events as follows and omit the failure events for regular lane changes.

(SS3.50) Lead vehicle **of** a platoon **loses speed** control while the platoon is changing lane into the transition lane from the neighboring automated lane through a gate. (It is assumed that while a platoon changes lane into the transition lane from the neighboring automated lane, it is not allowed, for lack of benefit and for safety reasons, to simultaneously join any other platoon.

NORMALEVENT: **s3.37**
FUNCTIONS: **OF5** - V1, **V4, V6**
CONSEQUENCES: Abort of the lane-change maneuver; collisions. **If** the failure causes the platoon to decelerate abruptly, the lane-changing platoon may collide with the platoon or manually-driven vehicles behind it in the transition lane. Such collisions may be serious.
RESPONSES:
DRIVER: **No** take-over of any kind.
VEHICLE: Determines a break point in the platoon for abort, taking into the consideration of the presence of the manually driven vehicles.

(SS3.51) Lead vehicle **of** a platoon loses headway control while the platoon is changing lane into the transition lane from the neighboring automated lane through a gate.

NORMAL EVENT: **S3.37**
FUNCTIONS: **OF6** - V1, **V4, V6,** (V13, RC5A, RC13)
CONSEQUENCES: Same **as SS3.50.**
RESPONSES: Same **as SS3.50.**

(SS3.52) Lead vehicle loses longitudinal position control while the platoon is changing lane into the transition lane from the neighboring automated lane through a gate.

NORMAL EVENT: **S3.37**
FUNCTIONS: **OF7** - V1, **V4, V6**
CONSEQUENCES: Same **as SS3.50.**
RESPONSES: Same **as SS3.50**

(SS3.53) Lead vehicle loses control of steering for lane change while the platoon is changing lane into the transition lane from the neighboring automated lane through a gate.

NORMAL EVENT: **S3.37**
FUNCTIONS: OF9 - V1, **V3, V6**
CONSEQUENCES: The lead vehicle may collide with the barriers near the gate, collide with one end of a barrier, or invade into the manual lanes. All these possibilities may lead to serious multiple collisions.

RESPONSES:

DRIVER: Takes over only steering control.

VEHICLE: Determines a break point in the platoon for abort. The failed vehicle may provide the driver with guidance regarding the steering direction (i.e. return to the original lane or steer towards the destination lane).

(SS3.54) Platoons lose coordination during a lane change maneuver into the transition lane from the neighboring automated lane through a gate.

NORMAL EVENT: S3.37

FUNCTIONS: **OF12** - (RC3, RC4, RC5, RC6, RC8a, RC13, V13)

CONSEQUENCES: Serious platoon collisions are possible. Compared to the same failure event occurring at a gate between two automated lanes, this event could be more dangerous because of the manually driven vehicles that may be present nearby on the transition lane.

RESPONSES:

VEHICLE: The lead vehicle determine a break point, taking into consideration the presence of the manually driven vehicles. (Alternatively, the lane-changing vehicles may determine the abort individually.)

(SS3.55) Lead vehicle loses all automatic control functions while the platoon is changing lane into the transition lane from the neighboring automated lane through a gate. (Note that this event is caused by multiple functional failures on the lead vehicle.)

NORMAL EVENT: **S3.37**

FUNCTIONS: **OF8, OF9; OF5, OF6, OF7**

CONSEQUENCES: Multiple collisions involving platoons are possible.

RESPONSES:

DRIVER: Takes over only the steering control.

(SS3.56) Trailing vehicle of a platoon loses headway control while the platoon is changing lane into the transition lane from the neighboring automated lane through a gate.

NORMAL EVENT: **S3.37**

FUNCTIONS: **OF6** - V1, **V4,** V6, (**V13,** RC5A, RC13)

CONSEQUENCES: Intra-platoon collisions are possible; also possible are subsequent collisions between the platoon and other vehicles including manually driven vehicles.

RESPONSES:

DRIVER: No take-over of any kind.

VEHICLE: Abort if safe.

(SS3.57) Trailing vehicle **of** a platoon loses control of steering for lane change while the platoon is changing lane into the transition lane from the neighboring automated lane through a gate.

NORMAL **EVENT: S3.37**
FUNCTIONS: OF9 - V1, V3, V6
CONSEQUENCES: Same **as SS3.53.**
RESPONSES:
DRIVER: Takes over only steering control.
VEHICLE: Abort if safe.

(SS3.58) Trailing vehicle **of** a platoon loses **all** automatic control while the platoon **is** changing lane **into** the transition lane from the neighboring automated lane through a gate.

NORMAL **EVENT: S3.37**
FUNCTIONS: OF8, OF9; OF5, OF6, **OF7**
CONSEQUENCES: The possible consequences include those stated in **(SS3.56& SS3.57).**
RESPONSES: Same **as SS3.57.**

(SS3.59) Manually driven vehicle suddenly moves into the transition lane behind the gate where a platoon is changing lane through the gate into the transition lane. Although manually driven but automation-equipped vehicles receive guidance from the roadside system regarding the right time and place to enter the transition lane and there are markings on the pavement indicating a no lane-change zone, the driver may nevertheless change lane near a gate due to lack **of** physical barriers.)

CONSEQUENCES: The manually driven vehicle may collide with the platoon upon the completion of the platoon lane change. Abort of the platoon lane-change; collisions, perhaps involving platoons.
RESPONSES:
VEHICLE: Abort the lane change if safe.
PLATOON: Abort the lane change if safe.

(SS3.60) Platoon fails to abort a lane change to the transition lane from the neighboring automated lane given unsafe behavior by the manually driven vehicles in the transition lane.

NORMAL EVENT: **S3.40**
CONSEQUENCES: The exact consequences depend on the situation. But, serious multiple collisions involving platoons of vehicles are possible.
RESPONSES: Exact responses should depend on the situation. But, sudden and fast emergency braking by the platoons and the manually-driven vehicles behind in the transition lane is expected.

(Exit Automated Lanes — to an Automated Off-Ramp:)

Failure events due to a failure while a platoon is exiting the automated lanes into an automated exit (S3.39) are equivalent, in terms of human factors, to those failure events occurring during traffic diverging at the location of a lane division. Therefore, they are omitted.

(Exit System — from the Transition Lane:)

(SS3.61) Lead vehicle of a platoon loses speed control while the platoon is moving on the transition lane.

NORMAL EVENT: S3.40
FUNCTIONS: OF5
CONSEQUENCES: If platoon moves at a speed higher than the assigned safe speed, then when the platoon catches up with the platoon or vehicle in front, the speed may be too high for the headway control to avoid a collision.
RESPONSES:
VEHICLE & PLATOON: Isolate the lead vehicle from the rest of the platoon.
VEHICLE: If the automated braking still works, the vehicle slows down automatically and gradually. Otherwise, isolation is achieved by movement, relative to the failed vehicle, of other vehicles. After isolation, instruct the driver to resume total control of the vehicle.
DRIVER: Takes over the control upon instruction.

(SS3.62 Lead vehicle of a platoon loses headway control while the platoon is moving on the transition lane.

NORMAL EVENT: S3.40
FUNCTIONS: OF6
CONSEQUENCES: The platoon could collide with the vehicle in front.
RESPONSES: Same as SS3.61.

(SS3.63) Lead vehicle of a platoon loses lane tracking control while the platoon is moving along the transition lane.

NORMAL EVENT: S3.40
FUNCTIONS: OF8
CONSEQUENCES: The platoon could collide with the vehicles on the manual lanes, a barrier, or one end of a barrier. It could even stray into the automated lanes through the gate. Subsequent collisions are possible, some of which may be serious.

RESPONSES:

DRIVER: Takes over the steering control.

(SS3.64) Lead vehicle of a platoon loses all automatic control while the platoon is moving along the transition lane.

NORMAL EVENT: S3.40
FUNCTIONS: OF8, OF9; OF5, OF6, OF7
CONSEQUENCES: The platoon could collide with the vehicles on the manual lanes, a barriers, or one end of a barrier. It could even stray into the automated lanes through the gate. It could collide with the platoons and vehicles in the transition lane. Subsequent collisions are possible, some of which may be serious.

RESPONSES:
DRIVER: Takes over the steering control.

(SS3.65) Trailing vehicle of a platoon loses headway control while the platoon is moving along the transition lane.

NORMAL EVENT: S3.40
FUNCTIONS: OF6
CONSEQUENCES: The vehicle could collide with the vehicle in front with a small speed difference at collision.

RESPONSES:

DRIVER: Takes over the longitudinal control and brake.

(SS3.66) Trailing vehicle of a platoon loses tracking control while the platoon is moving along the transition lane.

NORMAL EVENT: S3.40
FUNCTIONS: OF8
CONSEQUENCES: The vehicle could collide with the vehicles on the manual lanes, a barriers, or one end of a barrier. It could even stray into the automated lanes through the gate. Subsequent collisions, possibly serious, could occur.

RESPONSES:

DRIVER: Takes over the steering control.

(SS3.67) Trailing vehicle of a platoon loses all automatic control while the platoon is moving along the transition lane.

NORMAL EVENT: S3.40
FUNCTIONS: OF8, OF9; OF5, OF6, OF7

CONSEQUENCES: The vehicle could collide with the vehicles on the manual lanes, a barriers, or one end of a barrier. It could even stray into the automated lanes through the gate. It could collide with the platoons and vehicles in the transition lane. Subsequent collisions are possible, some of which may be serious.

RESPONSES:

DRIVER: Takes over only the steering control.

Failure events occurring while a platoon is moving along an automated lane are similar to those occurring while a platoon is moving along a transition lane except that (i) the former events are simpler in that they do not involve manual vehicles but (ii) they occur while the platoon is confined in the barriers on both sides. Therefore, we omit their discussion.

(SS3.68) Vehicle fails to deplatoon on the transition lane so that two vehicles cannot detach from each other on the transition lane.

NORMAL EVENT: S3.41
FUNCTIONS: OF12
CONSEQUENCES: The two-vehicle platoon cannot return to the manual lanes from the transition lane.
RESPONSES:
PLATOON: The failure occurs on the following vehicle. Slow down the two-vehicle platoon and stop. (Since the following vehicle has failed already, it (i.e. the two-vehicle platoon) should not be brought back to the automated lanes and be driven to a repository for automated vehicles.)

(SS3.69) Driver is not ready to take over control on the transition lane but the driving has been changed back to the manual mode anyway.

NORMAL EVENT: S3.42 & S3.43
FUNCTIONS: OF21
CONSEQUENCES: This is a very dangerous situation. The vehicle is not controlled at all. All kinds of serious collisions could occur.
RESPONSES: No recourse unless the system can detect the unusual behavior of the undriven vehicle and resume automatic control.

(SS3.70) Driver is ready to take over control on the transition lane but the control cannot be returned to the manual mode.

NORMAL EVENT: S3.42 & S3.44
FUNCTIONS: OF21
CONSEQUENCES: The driver cannot take over control at all.

RESPONSES:

OTHERS: System instructs and drives the vehicle to a nearby automated vehicle repository. (Note that an alternative response would be to stop the vehicle gradually using the automated braking on the transition lane. If after the stop the control cannot be taken over either, turn off the ignition and restart the vehicle. The assumption here is that the vehicle will then restart in the manual driving mode instead of automatic.)

(Exit **System** — from an Automated Off-Ramp:)

(SS3.71) Vehicle fails to deplatoon on the automated off-ramp so that two vehicles cannot detach from each other.

NORMAL EVENT: **S3.46**
FUNCTIONS: **OF12**
CONSEQUENCES: The two-vehicle platoon, even the front vehicle, cannot return to manual control.
RESPONSES:

OTHERS: The system instructs and drives the two-vehicle platoon to the automated vehicle repository.

(SS3.72) Driver is not ready to take over control on the automated off-ramp, but the control is switched back to manual anyway.

NORMAL EVENT: **S3.47 & S3.49**
FUNCTIONS: OF21
CONSEQUENCES: "Run away"
RESPONSES:

DRIVER: No recourse. (If vehicles can be switched into automated driving mode on the automated off-ramp, the driver can request a transition into the automated driving mode and have the vehicle driven to the repository automatically. However, the assumption here is that the driver is attentive enough to make such a transition request. This may not be likely given the fact that the driver had just failed the test for readiness to resume vehicle control. Yet another possible response would be to automatically switch the driving mode to automatic once erratic vehicle behavior on the transition lane is detected by the vehicle itself.)

(SS3.73) Driver is ready to take over control but the control cannot be switched to manual.

NORMAL EVENT: **S3.47 & S3.48**
FUNCTIONS: **OF21**

CONSEQUENCES: The vehicle will be driven to the repository automatically.
RESPONSES: **No** responses necessary.

(SS3.74) Driver is not ready to take over control and the vehicle fails to enter the automated vehicle repository at exit point.

NORMAL EVENT: **S3.49**
FUNCTIONS: **OF5** - V1, **V4, V6**
OF6 - V1, **V4, V6**
OF8 - V1, **V3, V6**
OF11 - V1, **V3, V6,** (RC3, RC8a, RC13)
CONSEQUENCES: Collisions.
RESPONSES: **No** recourse.
(An alternative response:
DRIVER: Takes over total control if he/she becomes ready for control resumption. Note that the condition may be unlikely given the fact that the driver had just failed the readiness test.)

(All Phases of **Normal** Operation:)

(SS3.75) While moving on the AHS, vehicle detects component failure via the **on-board** monitoring function.

(Note: The operation of an operational function hinges upon its supporting components. However, redundancy for reliability will be built in. Therefore, a component failure may not lead to the failure of the supported operational function. **Also,** the failure of one component may be compensated by the other working components in the system. For example, the automatic steering may be powerful enough to overcome the steering force brought on by the burst of a front tire.)

CONSEQUENCES: Although the component failure will not lead to the failure of any operational or elemental functions, any additional component failures could.

RESPONSES:

VEHICLE & PLATOON & OTHERS:

The response depends on the severity of the component failure. Possible responses include: (system) driving the vehicle out of the automated lanes and then having the driver take over total control. traffic slow-down for a safe control resumption within the automated lanes. or gradually stopping the automated traffic for a removal towing).