286500-3-H

Safety Plan

Variable Dynamic Testbed Vehicle

K. Luckscheiter

FEBRUARY 1997

Prepared for:

Mr. Alan T. Marriott
Jet Propulsion Laboratory
MS 126412
4800 Oak Grove Drive
Pasadena, California 91109

Contract Number: 959915

ERIM P.O. Box 134001 Ann Arbor, MI 48113-4001

286500-3-H

Safety Plan

Variable Dynamic Testbed Vehicle

K. Luckscheiter

FEBRUARY 1997

Prepared for:

Mr. Alan T. Marriott
Jet Propulsion Laboratory
MS 126-112
4800 Oak Grove Drive
Pasadena, California 91109

Contract Number: 959915

TECHNICAL REPROT STANDARD TITLE PAGE

1. Report No.	2. Government Accession No.	3. Recipient's Catalog No.
286500-3-H		

4. Title and Subtitle	5. Report Date
Variable Dynamic Testbed Vehicle Safety Plan	February 1997
	6. Performing Organization Code

7. Author(s)	8. Performing Organization Report No.
K. Luckscheiter	286500-3-H

9. Performing Organization Name and Address	10. Work Unit No.
Environmental Research Institute of Michigan P.O. Box 134001 Ann Arbor, MI 481134001	Il. Contract or Grant No. 959915

12. Sponsoring Agency Name and Address	13. Type of Report and Period Covered
Jet Propulsion Laboratory 4800 Oak Grove Drive Pasadena, CA 91109	Plan February 1997
	14. Sponsoring Agency Code

15. Supplementary Notes

10. Abstract

This safety document covers the entire safety process from inception to delivery of the Variable Dynamic Testbed Vehicle. In addition to addressing the process of safety on the vehicle, it should provide a basis on which to build future safety procedures. The safety procedures will need to address not only testbed operational issues, but also vehicle configuration control and modifications.

17. Key Words	18. Distribution Statement
variable dynamic testbed vehicle, VDTV, safety-criticai items, hazard reduction, testing	Limited availability. Further distribution of this document available only through the Jet Propulsion Laboratory.

19. Security Classif. (of this report)	20. Security Classif. (of this page)	21. No. of Pages	22. Price
unclassified	unclassified	7	

CONTENTS

1.0 Introduction

This safety document will cover the entire safety process from inception to delivery of the vehicle. In addition to addressing the process of safety on the vehicle, it should provide a basis on which to build future safety procedures. The safety procedures will need to address not only testbed operational issues, but also vehicle configuration control and modifications.

2.0 Safety Critical Items (SCIs)

Due to the configuration of the safety systems on the VDTV, there are multiple levels of safety critical items. The safety process will address all levels; however, the highest level will garner the greatest attention, and the lowest level the least. The safety process will only focus on single-point failures. Multiple parallel failures are beyond the scope of the quest for proposal, or our specific proposal. However, the hierarchical nature of our software approach always puts the driver in the ultimate control position with the ability to override all by-wire systems. This, in conjunction with the performance identified in the rollover analysis and the test track operating scenarios, will provide a safe testbed vehicle for researchers to utilize.

2.7 First-Level SCIs

The first-level SCIs are the safety critical items that must not be modified or bypassed without a thorough safety analysis and full compliance to the configuration control process. These items are listed below. They include both mechanical and electrical subsystems.

Safety Critical Items - First Level	Function
1. Driver Safety Panic Button	Disable all by-wire control and revert back to mechanical/base functionality of subsystems.
2. Driver Seat Belt	Restrain driver in safe position-dependent on base vehicle design integrity.
3. Rollover Bar	Mechanical added-in increase in strength to protect occupants in case of vehicle rollover.
4. Halon Fire Control System	Manually controlled Halon fire control system to protect occupants in case of fire.
5. Fuel Cell	The production Taurus fuel system is well developed and thoroughly tested for functional performance, reliability, and crash integrity. Only if the fuel tank must be otherwise modified will we replace it with an automobile racing type fuel cell. Presently modifications are not planned in the fuel tank area; hence, a fuel cell is not anticipated.

6. Computer Watchdog Timer	High level separate computer function to monitor all by-wire activities and revert vehicle back to mechanical/subsystem control (similar to driver panic button) if errors are detected.
7. Safety Power Dump Subsystem	The subsystem, controlled either by the watchdog timer or the driver safety panic button, removes power fkom the by-wire systems and reestablishes mechanical linkages.

2.2 Second-Level SCIs

The second-level SCIs are items in which a failure can cause a safety critical scenario for which the first-level SCI will be called upon to handle. If it were not for the first-level SCIs, these items could cause critical failures. These safety critical items must not be modified without complying to the configuration control process. These are shown in the table below.

Safety Critical Items - Second Level	Function
1. ERIM Control Computer Subsystem	The central computer control system and interfaces.
2. CANDataBus	Connection of all subsystems to the control and watchdog computers.
3. ERM-Supplied Vehicle State Sensors	Feedback to the control computer of the control state of the VDTV.

Each of the above subsystems has some safety implications; however, the criticality is mitigated by the first-level safety systems.

2.3 Third-Level SCIs

Of the third-level SCIs shown below, items 1 through 6 are the VDTV added or modified "standard" Tier 1 Supplier products listed. All of these subsystems are production or near-production subsystems, and as such have sufficient design, FMEA analysis, and maturity to not be considered a first- or second-level SCI. Inherent in each of these systems arc internal safety features. These items, though considered inherently safe, come under safety configuration control procedures. These subsystems should not be modified, except by the appropriate Tier 1 Supplier.

Third-level SCI item number 7 is the laptop computer for vehicle parameter setup entry and VDTV system monitoring. There are two possible areas of safety concern. The first is that entered data might not be set to the control computer correctly. All parameters sent to the control computer will be echoed back to the operator. It is up to the operator to verify that what was entered is what is shown on the system display. The second arca of safety concern is the projectile aspects of the laptop should there be an airbag deployment. To mitigate this scenario, both front airbags will be disabled or

removed. The driver side airbag is also being disabled due to the possibility of an out-of-position laptop computer.

Third-level SCI item number 8 is the measurement subsystem provided by JPL. ERIM will work with JPL during the design review to ensure the system can safely be mounted in the VDTV and does not induce any undue safety hazard. If there is a catastrophic failure in the electronics of the subsystem, the worst scenario is that it takes down the CAN/J1939 data bus or causes errors on the bus. If it takes down the bus, the watchdog system will safe the VDTV after time out by forcing the vehicle into the primary mechanical control mode. If the measurement system is causing errors only on the bus, the control computer will detect these errors (error detection is embedded into the CAN interface circuits) and disable the by-wire systems and revert back to the primary mechanical control.

Safety Critical Items - Third Level	Function
1. TRW Front Steer-by-Wire Subsystem	Computer control of front wheel steering
2. TRW Rear Steer-by-Wire Subsystem	Computer control of rear wheel steering
3. TRW Steer Feel Subsystem	Computer control of steering feel feedback
4. Bosch Throttle-by-Wire Subsystem	Computer control of throttle position
5. Delphi Brake-by-Wire Subsystem	Computer control of braking
6. Delphi Roll-Control Subsystem	Computer control of active anti-roll bars
7. Laptop Computer	Operator/passenger control and display of by-wire functions of the VDTV
8. Measurement Subsystem	Acquiring, time tagging, and storing of vehicle data

2.4 Fourth-Level SCIs

In addition to the well defined top three levels of Safety Critical Items, there is a fourth level which relates to FMVSS Standards and the standard aspects of the base vehicle. Fourth-level SCIs are the base vehicle standard components that the manufacturer has designed and selected to meet FMVSS. Such items are listed in Table 3-1 of Exhibit I (page 23) along with the FMVSS standard. Since ERIM is basing the VDTV on a production Taurus, no special effort on ERIM's part will be expended to address these issues; we will rely fully on the inherent Ford Motor Company design. However, to identify possible deviations from the base design during the modification of the Taurus for the VDTV program, Table 3-1 will be addressed during the VDTV Design Review.

3.0 Rollover Analysis

The rollover analysis will be performed by Mechanical Dynamics Inc. using their ADAMS model of the VDTV. A worst-case scenario will bc run to evaluate the stability performance of the VDTV. The worst-case scenario will include vehicle setup with the highest performance tires, low damping, large roll, and so forth. This vehicle setup will be

selected from the allowed operational parameters of the VDTV systems. The driving scenario for the modeling will be the limit handling with cadence braking as shown in the UMTRI film describing the earlier NHTSA research. If an unstable situation is identified in the analysis, vehicle control strategy in the by-wire systems will be limited under software to prevent the vehicle from operating in this regime.

4.0 Hazard Reduction Activities

4.1 First-Level SCI Hazard Reduction Activities

The inherent design of the VDTV is where the hazard reduction activities have been implemented. The overall safety implementation is designed into the first-level SCIs. Therefore, the first-level SCIs are not just items that could cause critical safety scenarios if they failed, but are more importantly the primary VDTV safety systems. of the seven first-level SCIs, only the Driver Safety Panic Button, the Computer Watchdog Timer, and the Safety Power Dump Subsystem are active safety devices. To ensure the safety/hazard reduction aspects of these items, the Safety Engineer will provide the top-level safety design requirements (Exhibit I: Sections 3.4, 3.6.3, 4.4.1, and 4.5.1) to the subsystem designers. During the VDTV Design Review (and informally during the design process), the Safety Engineer shall review compliance to these safety requirements.

The highest level automatic safety system is the computer watchdog timer. This subsystem provides a real-time monitoring of the system. The hazard reduction activities will be the designing of the system as delineated in Section 4.4.1.2 of Exhibit I. The timer will check operation every 10 milliseconds or less. For safety critical data channels, the system will check high and low limits, and will check slope. All data will be over-sampled with respect to the Nyquist sampling frequency, so the slope check can perform some averaging to reduce noise. The implementation of this will be monitored during the design process.

The other first-level SCI items-the seat belts, the rollover bar, the Halon fire control subsystem, and the possible fuel cell-are passive safety systems with the safety aspects inherent in their design. No other external hazard reduction activity, other than using proven industry products and design, will be conducted. During the VDTV Design Review, the safety aspects will be discussed.

4.2 Second-Level SCI Hazard Reduction Activities

The second-level SCIs have minimal impact on safety due to the safety aspects of the first- and second-level SCIs. The second-level SCIs are the control computer, the CAN data bus, and the solid-state sensors. Failures in any of these systems will be caught by the computer watchdog timer, and any hazard will be reduced by putting the VDTV in the non-drive-by-wire mechanical primary mode. A possible safety issue is noise induced

by EMI/RFI; however, it is expected that this is more of a performance issue. To reduce hazards/problems in this area, the Safety Engineer will ensure that good design rules are used for the CAN/J1939 data bus, for grounding and shielding, and for power distribution.

4.3 Third-Level SCI Hazard Reduction Activities

The first-level hazard reduction activities occur at the first-level SCIs. The second most significant impact on overall VDTV safety occurs with the third-level SCIs The hazard reduction approach taken here is the selection of advanced-production or near-production Tier 1 Supplier products for the VDTV. The by-wire front and rear steering, the by-wire braking, the by-wire active anti-roll bar, and the by-wire throttle all fall into this category. They have been selected because the Tier 1 Supplier has already designed in hazard reduction, performed an FMEA analysis, and tested for safety. ERIM will not do incremental efforts in this area

5.0 Operational Testing Procedures

Operational safety test procedures will be developed to support the test track test environment. It will address, not only safety to the VDTV occupants, but also other test personnel and observers at the test site.

6.0 Post-Delivery Configuration Control of SCIs

Configuration control of the Safety Critical Items will be addressed with the configuration control of all of the vehicle items, not just the safety critical items.