N72-25987

SYSTEM SAFETY ENGINEERING IN THE DEVELOPMENT OF ADVANCED SURFACE TRANSPORTATION VEHICLES

Harry E. Arnzen
Grumman Aerospace Engineering Corporation

Presented at the

NASA Government-Industry
System Safety Conference

May 26-28, 197_

I. INTRODUCTION

This paper describes applications of System Safety Engineering to the development of advanced surface transportation vehicles. The concept of System Safety has matured with aerospace programs and is now contributing safety methodology to non-aerospace segments of our society. As a pertinent example, the paper describes a Safety Engineering effort "tailored" to the particular design and test requirements of the Tracked Air Cushion Research Vehicle (TACRV), developed by the Grumman Aerospace Corporation, under contract to the Department of Transportation. The test results obtained from this unique research vehicle, will provide significant design data directly applicable to the development of future tracked air cushion vehicles that will carry passengers in comfort and safety at speeds up to 300 miles per hour.

Part II of the paper summarizes the Safety Engineering efforts implemented during the TACRV design phases. A detailed outline of the significant safety provisions, incorporated during the design of TACRV, is included in Part III. The safety engineering effort applied during the design of the Tracked Air Cushion Research Vehicle reflects the experience gained from a wide range of operational systems designed and manufactured by the Grumman Aerospace Corporation. These include commercial and military aircraft, space vehicles, hydro-foils and an experimental scientific submersible. Incorporation of the appropriate features into the TACRV design provides the desired result of a safe research vehicle. Hazards to operating personnel have been reduced to a minimum.

Part IV of the paper describes System Program techniques and the analytical methodology that is applicable to public transportation systems of the future, derived as a "spin-off technology" from aerospace programs. Two typical tracked air cushion vehicles for future public transportation are illustrated in Part V and the related system safety objectives are highlighted.

II. TACRV SYSTEM SAFETY PROGRAM

- OBJECTIVES
- SCOPE
  DESIGN, MANUFACTURE AND TEST
- APPROACH AND METHODOLOGY
  DESIGN SAFETY CRITERIA AND GUIDELINES
  SAFETY REVIEWS
  DRAWING REVIEW AND SIGN-OFF
  SAFETY CONTROLS IN VENDOR SPECIFICATIONS
- MANUFACTURE PHASE MONITORING
- VEHICLE TEST CONSIDERATIONS

This part of the paper discusses the Safety Engineering Program implemented during the TACRV design and manufacturing phases, and reviews future test program considerations. The primary objective of this safety program has been to eliminate or reduce potential hazards associated with operation and maintenance of TACRV. Potentially catastrophic items were eliminated during early design. Critical hazards identified have been eliminated or reduced through use of safety devices, warning systems and/or precautionary procedures. In summary, the objectives of the program have been to establish requirements, procedures, and methods, to ensure personnel safety and minimum risk of damage, or degradation to equipment.

SCOPE OF PROGRAM

The scope of the TACRV Safety Program includes the active participation by Safety Engineers, design and systems personnel, in all phases of design. The significant program milestones and related system safety engineering tasks are illustrated in Figure 1. The Grumman approach to system safety is "the total integration of available skills and resources to achieve maximum safety assurance." Safety Program activities generated by this concept included:

- Performance of analytical studies to a practicable depth for hazard identification. These include preliminary (gross) hazard, hazardous failure-mode and systems integration studies on the vehicle, subsystems, crew station, wayside power and guideway/vehicle interfaces
- Participation of Safety Engineers at design reviews, safety reviews and informal inspections
- Recommendations for emergency systems, safety devices and/or emergency procedures, for identified potential hazards which cannot be eliminated
- Provide guidance and support to design personnel through development of safety design criteria and check lists "tailored" to the operating environment of TACRV

Many technical disciplines contributed to the safety assurance effort, including:

- Reliability/Maintainability - failure and maintenance studies.
- EMI - Safety inputs on vehicle grounding, internal bonding, dissipation of of electrostatic charges and lightning protection considerations.
- Power Plant - Crashworthy fuel system technology, thermal protection and combustion prevention considerations.
- Crew Systems Design - Human Factors aspects of Controls and Displays.
- System and Project Engineering; GAC System Safety Staff.

MANUFACTURE PHASE MONITORING

The system safety effort planned for the manufacturing phase of TACRV includes monitoring the vehicle assembly stages, equipment installation and systems checkouts. The purpose of this effort is to identify and correct any potentially hazardous interface conditions, between lines and equipments, that were not anticipated during the design phases. The safety engineer will make corrective action recommendations to the project engineer, whenever unsafe conditions are identified. In summary, the safety tasks will include the following:

- Observe acceptance tests of major equipments and propulsion systems, to verify compliance with safety requirements, before installation in the vehicle
- Monitor installation of all major systems and subsystems in order to identify potential ignition or combustion hazards, in each compartment, from possible leakage, chafing, and/or electrical shorts, due to close proximity of interfacing line connections or interference with vehicle structure
- Inspect turbofan engine installation to identify potentially hazardous conditions related to engine/vehicle integration. Examine engine control linkages for freedom of travel. Assure adequate thermal protection for equipments and lines in high temperature areas. Review all potential fluid leakage and drainage paths, in engine compartments
- Monitor installation and checkout of all emergency equipment (i.e., fire detection/suppression, caution/warning, etc.) and safety devices to verify failure-free operation
- Incorporate safety oriented requirements into each vendor specification and specification control drawing
- Conduct drawing review and sign-off on selected major installation drawings where safety provisions are involved
- Review of test plans, test reports and operating procedures to determine impact on safety. Review and evaluate precautionary procedures. Review all test failures for unanticipated hazardous conditions and recommend corrective action
- Develop a pre-accident plan for coordinated Grumman support in accident investigations
- During subsequent phases, System Safety will review all previous safety studies, develop operating and maintenance procedures and monitor vehicle test site operations

APPROACH AND METHODOLOGY

Although there are some differences in the Safety Engineering effort between Lunar Module, Military Aircraft, TACRV and similar advanced surface transportation systems, there are significant differences in the accident potential and the approach to practicable solutions to reduction or elimination of injury and damage to equipment. In addition, the level of risks that are acceptable in military and space operations are not acceptable in public transportation. This aspect is what we are ultimately dealing with, in our approach to achieving safety assurance.

In the absence of a formal system safety engineering standard, such as the military requirements of MIL-STD-882, ("System Safety Engineering Program for Systems and Associated Subsystems and Equipment; General Requirements for"), special attention was given to "tailoring" a system safety program to the specific needs of the TACRV Program. In lieu of costly and extensive systems safety analyses described in MIL-STD-882, all engineers and designers were provided with a "design safety criteria and guidelines" document, developed by the Safety Engineer, to enable all personnel to assist in hazard identification and elimination in the early phases of design. The majority of these "guidelines" has been previously established for use in the design of military and civil aircraft and spacecraft. The criteria were used continuously by design personnel as a check-off list during the vehicle and subsystems design.

Where critical hazards were identified, the Safety Engineer conducted accident and safety equipment research to review the "state-of-the-art" in safe system design and offer practicable recommendations. For example, TACRV has the combination of a large volume of JP-5 fuel for the turbofan with a 7000-volt LIM electrical propulsion system on board the

vehicle. Crew survival is now assured by incorporation of a crashworthy fuel tank and piping system. Another typical safety study involved evaluation of the required number, size and locations of doors and escape hatches to assure safe exit and/or rescue, under any conceivable mishap condition.

Drawing Review and Sign-Off

Drawing reviews were conducted during the early stages of systems and equipment design to identify and correct unanticipated hazards and to recommend appropriate emergency systems, fail-safe features and safety devices. Particular attention was given to review of critical systems that are employed during emergency situations. Typical examples of layouts and drawings reviewed for these systems and equipments included crew station, emergency controls, escape hatches, caution/warning, fire detection/suppression, vehicle grounding, brakes and fuel systems.

Effective control of design safety, for subcontractor supplied equipments, was established by incorporating safety oriented requirements into each Specification Control Drawing (SCD). Preliminary and final "SCD's" were reviewed to verify compliance, or make additions, to the safety requirements. These included such items as safety factors, leakage tests, proof tests, fail-safe and non-flammable requirements, where applicable. All "SCD's" required final sign-off by the Safety Manager.

Useful Inputs from Other Disciplines

Employment of the "Safety Criteria and Guidelines" document, prepared by the Safety Manager, enabled all design personnel to contribute safety assurance features throughout the design effort.

[illegible]

[illegible]

[illegible] prevention, detection [illegible] suppression [illegible] combustible materials, containment [illegible] electrical grounding [illegible] fire detection sensors and fire suppression [illegible] compartments [illegible] safe from fire hazards.

Fire Prevention

The approach to fire prevention was to minimize the use of combustible material and separate them from ignition sources. The major source of combustible materials in the vehicle is the engine fuel, type JP-5. Fire hazards in the use of this fuel are present during fueling and normal engine running.

Pressure fueling or defueling of the three tanks will be done only when the vehicle and fuel delivery system are properly grounded. The tanks are grounded through the vehicle structure. Prior to connecting the fuel delivery hose, a bonding cable is connected to both fueling truck and TACRV. Hence, the possibility of spark ignition, caused by the difference in static electricity potential, between the two vehicles, is eliminated. The possibility of fire in the compartments during

[illegible]

The fuel storage [illegible] explosion and flood suppression. [illegible] highly impact resistant, [illegible] coupled with breakaway [illegible] valves. Each cell has [illegible] port connections on the top of the [illegible] to preclude crash rupture and fuel spillage. Ventilation and drainage is provided in the compartments where fuel system components and lines are installed.

The selection of non-metallic materials has been made with combustibility as a prime factor. In general, FAA-approved materials have been used wherever applicable. Non-flammable material is used in the cabin for rugs, seat upholstery, thermal and acoustic insulation and wall liner.

Fire Detection

The two general areas where a fire is most apt to occur are in the engine nacelles and in the PCU compartment. Since a fire in either of

these areas would greatly endanger both crew and equipment, a fire detection system is located in each of the engine nacelles and in the PCU compartment.

The means for fire detection is an element which changes resistance with temperature. This element is a continuous cable which threads through each engine nacelle so that it will detect hot spots or high average temperature. The detection circuit is triggered when a temperature of 450°F is detected. When this occurs the Master Caution Lights flash, an audible alarm sounds and the appropriate warning light goes on. The fire detection circuits have a "press to test" feature which allows the operator to test the continuity of the sensing elements and output amplifier.

Fire Suppression

The means for fire suppression is through the release of bromotrifluoromethane (CF_3Br). This material is stored in bottles, in a liquid state, and when released forms a heavy blanket of inert gas which excludes oxygen from the fire zone. This gas is released into the nacelles by the operator who presses a switch which ignites a pyrotechnic valve. Once opened, this valve allows all of the gas to be expended. The pyrotechnic valve switch is located so that the operator's Fire Control "T" handle must be pulled out first. This assures the cut-off of fuel and hydraulic oil flow to the engine compartments before the fire suppressant gas is released.

Fire suppression in the LIM PCU equipment compartment will also utilize CF_3Br. Detection of a PCU fire will be displayed on the Operator's Caution and Warning Panel and will also initiate the Master Caution Lights and Audible Alarm.

NORMAL AND EMERGENCY BRAKING SYSTEMS

LIM Braking

The Linear Induction Motors (LIMs) are capable of exerting the highest braking force of all braking modes provided for the TACRV and will be the primary means of stopping. However, LIM braking is dependent upon picking up wayside power, and the proper functioning of PCU equipment and controls. Hence, loss of wayside power, or electrical failures aboard the vehicles, will render LIM braking completely ineffective. The Braking System has been designed to have multiple devices for supplying braking forces. This permits evaluation of braking effectiveness, and enhances the safety of the crew and equipment during testing. High speed testing on a relatively short length of guideway requires back-up braking modes. With exception of the friction brake pedal, all braking device controls are within reach of both operator and observer.

Friction Braking

Friction braking has several important advantages over LIM braking. It is not dependent on wayside power and it is less complex; thus, the probability of failure is reduced. The friction braking system is also equipped with redundant actuators. The main actuators get high pressure oil flow from the three engine-driven pumps. Friction braking is the main back-up for LIM braking at low speed, whereas the speed brake is used at high speed.

Speed Brake

An aerodynamic speed brake, located on top of the engine nacelles, produces a drag force that augments vehicle drag for normal braking.

Emergency Braking Modes

As a backup to normal braking modes previously described, there are a number of emergency modes which assure stopping when primary braking fails. The friction brake pads have redundant actuators which are deployed by flowing hydraulic fluid from a charged accumulator. Thus, loss of pressure in the main hydraulic system will not void the use of friction brakes. A drag chute is aboard for use in major emergencies where falure or late application of a primary mode require additional braking force. Release of the chute is manual, through a cable-pulled mechanical latch; reliability is thus enhanced due to the direct, positive control. Friction braking can also be accomplished by shutting off the three engines, which causes the levitation cushion skids to rub against the guideway. If all methods of braking fail to stop the vehicle before it reaches the end of the guideway, an arresting cable engages

the nose of the chassis. As the cable extends, energy is expended in a water brake at the side of the guideway.

ELECTRICAL HAZARD PROTECTION

The vehicle and associated electrical equipments have been designed to provide ground paths so that protection of operating and maintenance personnel is assured. Electrical equipment in the vehicle body is positively grounded with straps or with aircraft-type approved bonding. Body-to-chassis grounding is done with grounding straps near the fore and aft suspension points. The LIMs are grounded to the chassis structure and to the LIM rail when the vehicle is not under way. The vehicle will be grounded during fueling.

VEHICLE GUIDEWAY RETENTION

The vehicle levitation cushions are designed so that the top of the cushion structure will engage the guideway guidance panels if the chassis lifts.

SUSPENSION SYSTEM

The suspension system is designed so that loss of electric power to the Control Amplifier Unit will result in the reversion from active to passive suspension. Other failures, which may affect only one channel of the active suspension system, will not cause automatic switching to passive suspension. The operator can select, with a mode switch, "passive suspension". This switch puts all actuators in the passive mode, and assures a safe, well damped ride.

CAUTION AND WARNING SYSTEM

The TACRV has a caution and warning system which is similar to that used in commercial aircraft. Two master caution lights, located on top of the operator's control and display panels, flash in the event of a detected failure or unsafe condition. These master warning lights alert the operator and observer to visually scan the control panels for a lighted caution indicator which identifies the malfunction area. Fire warning is separate from the "Caution and Warning System". Individual fire alarm lights designate the compartment in which a fire is detected and a horn provides an audible alarm. The areas monitored are the PCU compartment and left, center and right engine compartments.

NORMAL AND EMERGENCY EXIT PROVISIONS

The personnel compartment has a total of six possible exits for its occupants. Doors are provided on each side of the vehicle for normal and emergency exit for all occupants. If the doors are inoperative, two escape hatches above the operator seats can provide a means of egress. The direct-vision windows, just aft of the windshield, are designed to slide back, also permitting egress as a last resort.

PERSONNEL COMPARTMENT AND CRASH SAFETY CONSIDERATIONS

The design of the personnel compartment employs features that are consistent with approved safety and human factors practices for commercial aircraft. The selection of aircraft-type seats, restraint harness, bird-proof windshield, and the arrangement of instrument panel, caution/warning panels and controls, all contribute to safe and efficient operation of the TACRV.

Seats and Restraint System

For maximum protection of occupants, approved-type aircraft seats are installed in the personnel compartment. Safety belts and shoulder restraint harnesses are installed on the seats for protection during emergency braking conditions. The standard aircraft restraining harness has a single-point release mechanism that is capable of instant release by the occupant or by rescue personnel. The shoulder harness is equipped with an inertia reel and cable mechanism which prevents forward pitching of the body during emergency braking. A ratchet mechanism, within the reel, restrains the shoulder in the last angular position of the body when a sudden stop occurs. This device reduces chance of crash-induced head injuries.

IV. SYSTEM SAFETY PROGRAM APPLICATIONS TO ADVANCED PUBLIC TRANSPORTATION SYSTEMS

- PROGRAM PARTICIPATION BY SYSTEM SAFETY
- SAFETY ANALYSES METHODOLOGY
- SAFETY REVIEWS

This part of the paper describes System Safety Engineering techniques and methodology that are applicable to advanced public transportation systems of the future, derived as a "spin-off technology" from aerospace programs. Although recent commercial and military aircraft designs have utilized the systems safety discipline, design of surface mass transportation systems and automobiles has not. The TACRV is pioneering in high speed - 300 MPH - surface transportation. This alone produces a whole new spectrum of hazard potentials requiring system safety analyses for the first time. Failure Effects Analysis, Hazard Mode Analysis and System Integration Safety Analyses are useful "spin-offs" from aerospace technology which are applicable here. There has never before been any requirements for such in-depth safety studies in surface transportation. Formal safety reviews can be anticipated to resolve or correct hazards identified in all systems within the vehicle, guideway and related power distribution systems.

The contents of this section are graphically illustrated in Figures 4, 5 and 6, to depict the elements of formal safety program planning based upon the approaches used on aerospace programs. Figure 4 presents the typical safety program milestones for a prime contractor's Program Plan. Figures 5 and 6 provide insight into system safety participation during the design, manufacture and testing phases of a typical transportation system.

Safety analyses methodology is illustrated in Figures 7, 8, 9 and 10, also included in this section. These charts indicate the aerospace "systems approach" for effective utilization and coordination of analytical efforts, that may be applied to future transportation systems.

Several representative "tracked air cushion vehicles" for future public transportation are described in Part V of this paper. The purpose is to enable the reader to visualize the innovative approach to vehicle design, wherein system safety applications are essential, in the interest of public safety.

Aspects on Safety Programs Planning, Participation and Analyses

Based upon the approach used in the aerospace industry, the planning guidelines for future safety plans will be derived from Government Standard MIL-STD-882 and from prior contractor's experience on similar programs. The formal safety programs which include the application of analytical techniques and scheduled safety reviews will identify and eliminate, or reduce potential hazards associated with operation and maintenance of the overall system. In many cases, the use of safety devices, emergency systems, warning devices, or procedural changes will be employed.

Subcontractors will be subject to specific design safety requirements in the appropriate specifications and contracts. As technical systems manager, the prime contractor monitors all safety efforts of each subcontractor, ensuring that these requirements are met. On major subsystems, subcontractors are required to submit safety plans describing in detail their system safety organization, scope and effort. These plans will be integrated with the prime contractor's plan to ensure a coordinated overall effort that will include the following activities:

- Develop a "System Safety Engineering Program Plan", (SSEP) and submit to the customer for mutual agreement on scope, schedule and cost
- Perform preliminary (gross) hazard studies and system analyses on the vehicle, subsystems, operator station configuration, wayside power and guideway

systems (reference Figures 4, 5 and 7)

- Perform failure mode analyses on major systems to ensure that system or equipment failures will not cause hazardous conditions (reference Figures 5, 8, 9 and 10)
- Provide guidance and support to design personnel through development of safety design criteria and check lists appropriate for each discipline
- Define both design and operating safety requirements for all normal and emergency systems operation (reference Figures 4, 5, 6, 7 and 10)
- Develop safety procedures for compliance by operating and maintenance personnel before and after each vehicle run, to reduce chance of accidents or injury (reference Figures 4, 5, 6 and 10)
- Perform safety reviews during acceptance testing to demonstrate that operating and emergency procedures are adequate (reference Figures 4, 5, 6 and 10)
- Participate in design reviews and conduct safety reviews (reference Figures 4, 5, 6, 7 and 9)
- Monitor all pre-production equipment and systems tests to identify unanticipated failures modes and make recommendations for corrective action (reference Figures 5, 6, 8 and 9)

During subsequent vehicle tests, all previous analyses will be reviewed to assess adequacy of emergency provisions, develop operating and maintenance procedures, and monitor final test and checkout operations (reference Figures 5, 6 and 8).

- SAFETY ANALYSES METHODOLOGY
  - OBJECTIVES:
    HAZARD IDENTIFICATION, ELIMINATION AND/OR COMPENSATING PROVISIONS
  - SAFETY ANALYSES UTILIZATION FLOW
  - PRIME AND SUBCONTRACTOR ANALYSES, A COORDINATED EFFORT
  - COORDINATION OF RELIABILITY "FMEA" WITH SYSTEM SAFETY "HMEA" ANALYSES

V. A LOOK AT FUTURE MASS TRANSIT SYSTEMS

- ADVANCED CONCEPT STUDIES
- SYSTEM SAFETY OBJECTIVES

ADVANCED CONCEPT STUDIES

The growing need to improve our nation's surface transportation systems is currently recognized. While improvement of existing modes is a logical step, we are also pursuing new and innovative concepts as the only means through which a dramatic upgrading of ground transport can be achieved. The tracked air cushion vehicle with linear induction propulsion is an excellent example of a developed concept that employs technology new to the transportation field. TACV promises a safe, fast, comfortable, all-weather, non-polluting alternative to present systems. Applications of this concept, in the near future, will provide a major first step toward gaining public acceptance of this new mode of travel. The TACV is considered to be an innovative approach to provide high-speed ground access to our airports, as well as a safe and comfortable means of inter-city mass transit, for the near future. Figures 11 and 12 illustrate typical development studies of the aforementioned Tracked Air Cushion Vehicles.

SYSTEM SAFETY OBJECTIVES

The system safety objectives that are considered uppermost in the TACV System and all new modes of transport development, are as follows:

- The system must ensure safety of passengers, operators and maintenance personnel
- The system should not create or appear to create a hazard to the community, its environment, its children, or its animals
- The operational reliability must be sufficiently high and recovery from failures that do occur must not present a potentially hazardous condition to people, equipment or other means of transport close proximity to the system
- The system should not pollute the operating environment with exhaust or excessive noise

In summary, the primary objectives of the System Safety Engineering Programs planned for new modes of public transportation, include the following:

- Identify potential hazards by analytical methods and by equipment test surveillance
- Determine hazards effects on passenger and public safety
- Develop corrective and/or preventative measures
- Identify rescue requirements peculiar to new transportation system
- Establish safety guidelines for design, test operation and maintenance phases of vehicle life cycle
- Identify need for technology development and additional study where safety assurance appears uncertain

VI. SUMMARY AND CONCLUSIONS

SUMMARY

The concept of System Safety Engineering has matured with aerospace programs and is now contributing safety assurance methodology to the non-aerospace segments of our society. As an appropriate example, a Safety Engineering effort discussed in this paper, has been "tailored" to the particular design, schedule and operating requirements of the Tracked Air Cushion Research Vehicle (TACRV). The safety considerations used during the design of TACRV are the result of experience gained from a wide range of aircraft, space vehicles and experimental systems designed and manufactured by the Grumman Aerospace Corporation. The incorporation of the appropriate features into the TACRV design provide the desired result of a safe research vehicle with minimum hazard to operating personnel.

In many cases, materials and hazard control techniques developed in our aerospace programs are being applied to advanced surface transportation systems. Typical examples in TACRV are use of non-flammable materials, system hazard and human factors studies, redundant systems for critical control functions, and fire-proofing of fuel and propulsion systems.

It is anticipated that many of the approaches to safety assurance described in this paper will be directly applicable to future public transportation systems and vehicles as a "spin-off technology" from the aerospace industry.

In summary, the significant safety features provided to compensate for potential hazards identified on the aforementioned TACRV, include the following:

POTENTIAL HAZARD CATEGORY	COMPENSATING SAFETY PROVISIONS
Fire and Toxic Smoke	• ECS Fresh Air Supply System, Two Sliding Windows, Two Overhead Hatches • Fire Detection and Suppression System for Critical Areas • Non-Flammable Materials in Personnel Compartment • Fire Shut-Off Valves for Fluids
Explosion	• Crashworthy Fuel Tank and Lines; Fuel Tanks Assembled with Reticulated (Porous) "Safety Foam" • Fuel Tanks Isolated From Crew • Drainage and Ventilation in Fuel Area
Emergency Stopping and Crash Condition Hazards	• Aircraft Seats, Safety Belts, Shoulder Harnesses and Inertia Reels • Padded Instrument Panel Visor • Two Doors and Two Escape Hatches

POTENTIAL HAZARD CATEGORY	COMPENSATING SAFETY PROVISIONS
Brake Failure Emergencies	• Friction Brake Backup System • Drag Parachute • Arrestment Cable System • Settle Vehicle on Cushion Skids
Critical Systems Failures (i.e., Fluid Power, Electrical, Turbofan [illegible]ines, etc.)	• Caution and Warning System Located on Operator's Panel
Electrical Shock to Personnel	• Vehicle Grounds Externally to LIM Rail When Vehicle Stops, Plus External Grounding Cable Provided • [illegible]ernal Vehicle Bonding and Grounding [illegible]ents
Bird Strike Hazards to Crew	• Birdproof Aircraft Wind[illegible]
Fog, Rain or Ice on Windshield	• Electrically Heated Aircraft Windshield
Secondary Suspension System Malfunction	• Operator can Switch From Active to Passive Suspension System
Vehicle Leaves Guideway	• Positive Retention of Vehicle Provided by Air Cushions Extended Under Guideway Side Rails

CONCLUSIONS

Judicious use of System Safety Engineering techniques during early phases of design can yield a highly effective safety assurance program in terms of accident prevention, avoidance of costly changes and assurance of safe operation and maintenance, throughout the life cycle of the system.

Timeliness of Safety Engineering studies is an essential factor for early identification and elimination of potential hazards and latent design deficiencies. By this approach, the appropriate safety devices, emergency systems and fail-safe features can be readily incorporated during the initial design stages.

The Grumman approach to system safety is "the total integration of available skills and resources to achieve maximum safety assurance". Safety program activities generated by this "system approach" and total team effort yield an effective program without costly duplication of efforts.

As we pioneer into higher speed concepts of surface transportation, extensive application of in-depth failure and hazard mode analyses, systems integration analyses and formal safety reviews can be anticipated, in the interest of passenger and community safety.

VII. REFERENCES

1. Military Standard MIL-STD-882; "System Safety Engineering Program for Systems and Associated Subsystems and Equipment; Requirements for."

2. "AFSC DH 1-6 System Safety Design Handbook": Published by USAF Hdq. Air Force Systems Command; Wright Patterson AFB, Ohio 45433.

3. HARRY E. Arnzen, "Implementation of Prime and Subcontractor System Safety Engineering Programs"; Grumman Aerospace Corporation, Bethpage, New York, June 12, 1970.

4. "System Safety in Transportation"; System Safety Society, Washington, D.C. Chapter Newsletter, 18 March 1971.

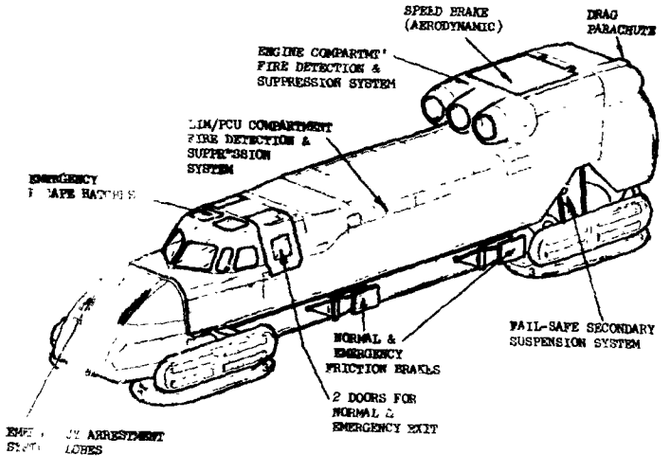
5. "System Safety Engineering"; Approach Magazine, Pages 38-42; Published by Navy Safety Center, Norfolk, Va., March 1970.

6. Harry E. Arnzen, "Failure Mode and Effect Analysis: A Powerful Engineering Tool for Component and System Optimization"; - 5th Reliability & Maintainability Conference; Annals; AIAA/SAE/ASME; New York, July 18, 1966.

7. "Proceedings of USAF - Industry System Safety Conference, Las Vegas, Nevada"; Published by Directorate of Aerospace Safety, Norton AFB, California; 25-28 February 1969.

8. Roy Harris, "Preliminary Hazard Analysis", TRW Systems Corp., Redonda Beach, California; Proceedings of USAF - Industry System Safety Conference, Las Vegas, 25 February 1969.

9. The Boeing Company, "Fault Tree for Safety", DG-53604, November 1968.



TRACKED AIR CUSHION RESEARCH VEHICLE SAFETY PROVISIONS

FIGURE 3

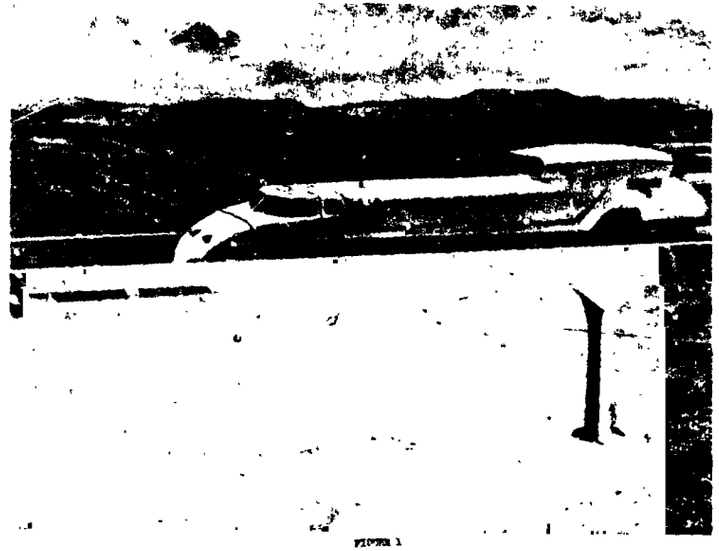
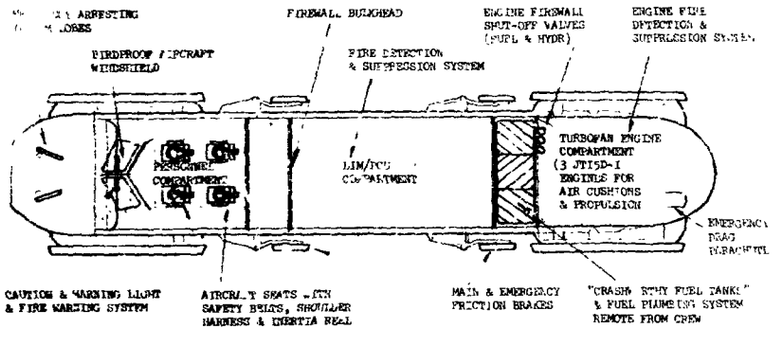


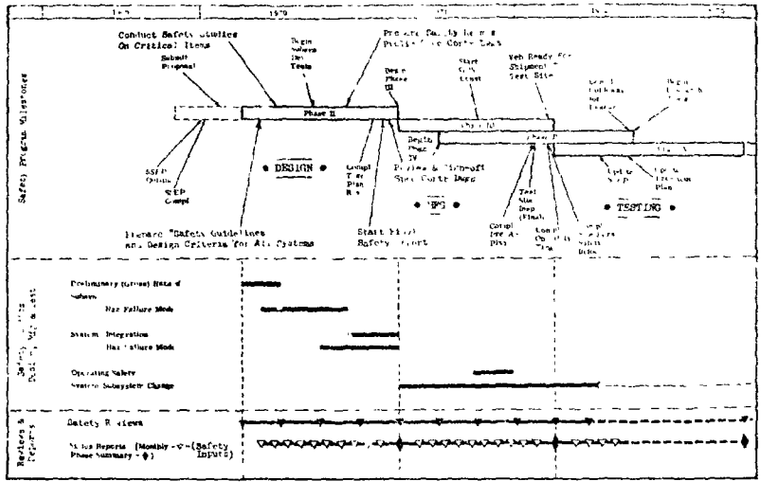
FIGURE 1



TOP VIEW

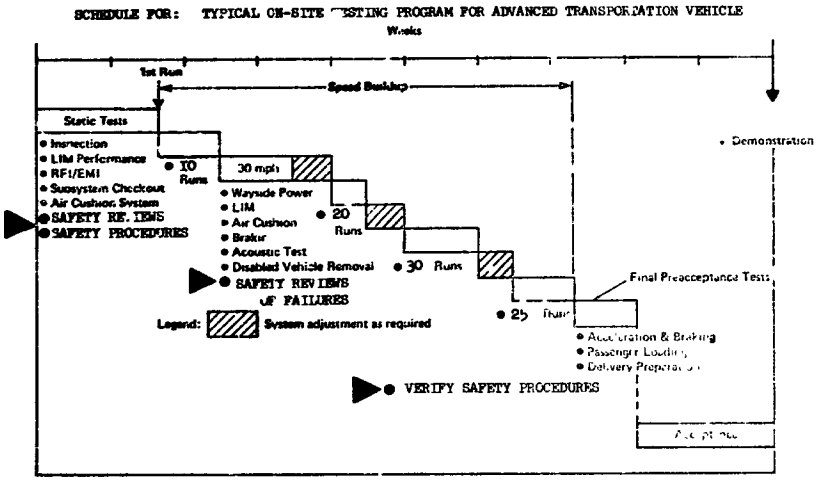
● TRACKED AIR CUSHION RESEARCH VEHICLE SAFETY PROVISIONS

FIGURE 4



SYSTEM SAFETY ENGINEERING PROGRAM MILESTONES FOR TACV

FIGURE 2



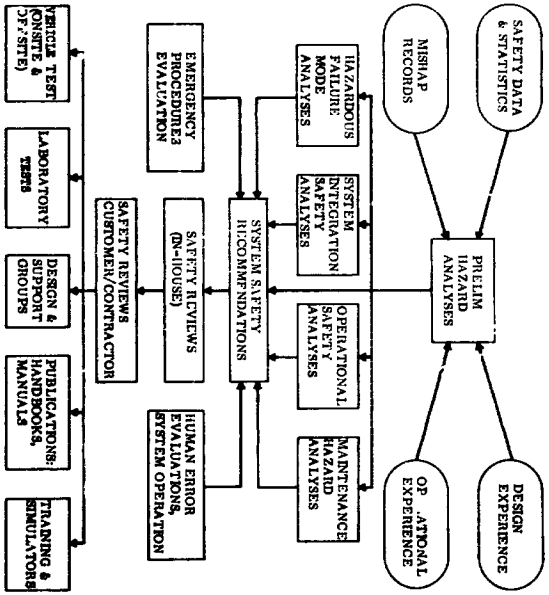
● SYSTEM SAFETY ENGINEERING PARTICIPATION IN TEST PROGRAM

FIGURE 7

SAFETY PROGRAM TASKS	6 MONTHS	12 MONTHS	18 MONTHS
1. APPROVAL OF "PROGRAM PLAN" (SSEP)	▲		
2. PRELIM HAZARD ANALYSIS	▲ START ▲ UPDATE	▲ UPDATE	▲ COMPLETE
3. SYSTEM SAFETY ANALYSIS	▲ START	▲ UPDATE	▲ COMPLETE
4. SUBSYSTEM SAFETY ANALYSIS	▲ START	▲ UPDATE	▲ COMPLETE
5. INFORMAL SAFETY REVIEWS ("IN-HOUSE")	▲ PERIODICALLY - EACH SUBSYSTEM & SYSTEM		▲
6. FORMAL SAFETY REVIEWS (CUSTOMER/CONTRACTOR)	▲ QUARTERLY	▲ QUARTERLY	▲ QUARTERLY
7. MONITOR ALL "IN-HOUSE" TESTS	▲ AS TESTS ARE CONDUCTED		▲
8. MONITOR SUBCONTRACTOR SYSTEM SAFETY PROGRAMS	▲ START/THROUGHOUT PROGRAM		
9. MONITOR VEHICLE TEST PROGRAMS/ONSITE & OFFSITE	▲ START/THROUGHOUT PROGRAM		
10. PREPARE SAFETY "CAUTION/WARNING" PUBLICATIONS FOR OPERATORS, CREW, MAINTENANCE & TESTS PROCEDURES		▲ START	COMPLETE ▲

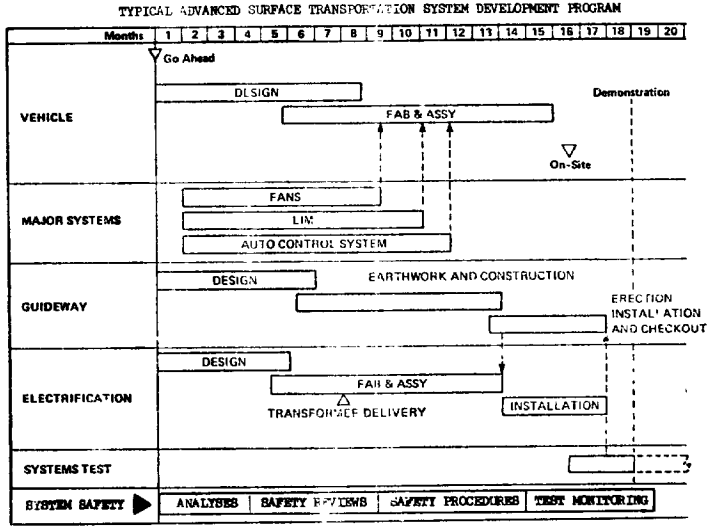
● TYPICAL SAFETY PROGRAM MILESTONES FOR A PRIME CONTRACTOR BASED ON AEROSPACE PROGRAM PLANNING GUIDELINES

FIGURE 5



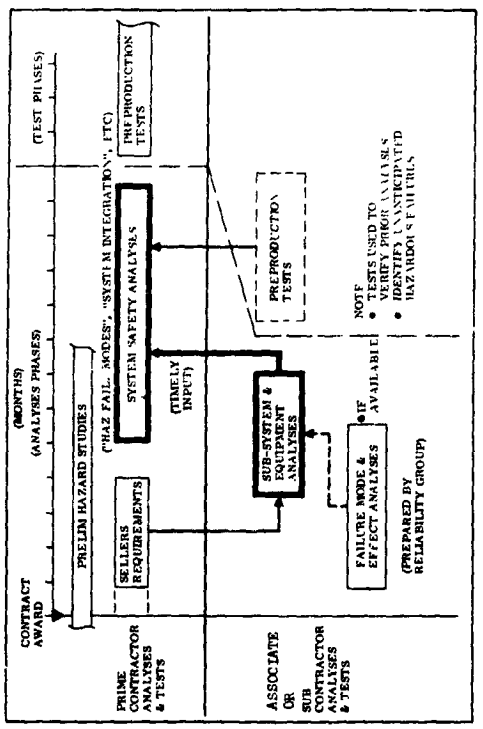
● SYSTEM SAFETY ANALYSES UTILIZATION FLOW CHART

FIGURE 8



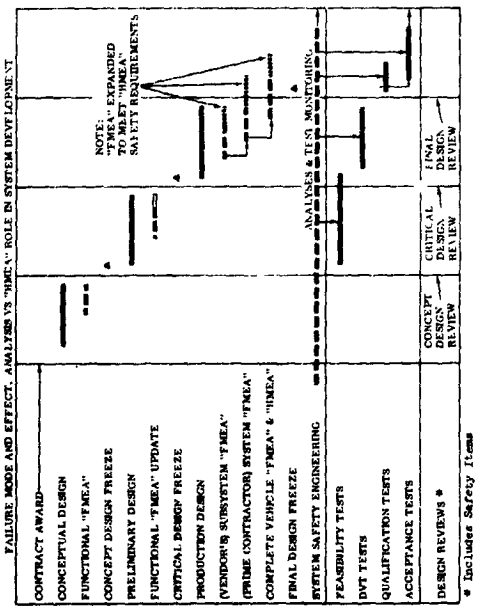
● SYSTEM SAFETY PARTICIPATION DURING DESIGN AND MANUFACTURING

FIGURE 6



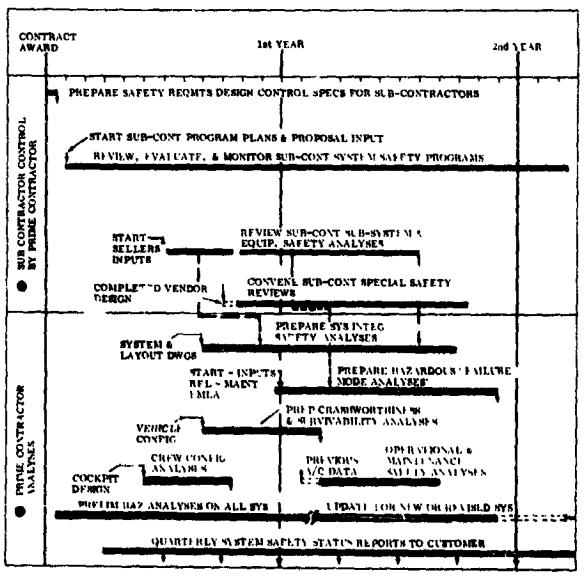
● USE OF PRIME AND SUBCONTRACTOR ANALYSES AND TESTS AS A COORDINATED EFFORT

FIGURE 9



● PREPARATION OF "FAILURE MODE AND EFFECT ANALYSES" AND "HAZARD MODE ANALYSES" AS A COORDINATED RELIABILITY/SAFETY EFFORT

FIGURE 10



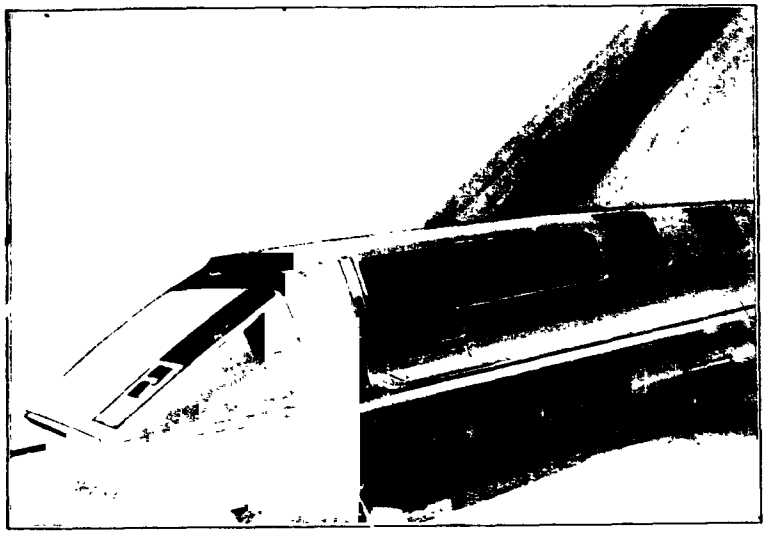
● TYPICAL AEROSPACE PROGRAM PLANNING CHART FOR COORDINATING PRIME AND SUBCONTRACTOR ANALYTICAL TASKS

●● SERVES AS A GUIDE FOR PLANNING NON-AEROSPACE SYSTEM SAFETY PROGRAMS

FIGURE 11

LOCKHEED-GEORGIA CO., VIBRATION OF JACT

FIGURE 12



LOWEY-SMAITH INC. VISUALIZATION OF TACV

FIGURE 13

SESSION VI

QUESTIONS AND ANSWERS

JERRY LEDERER: Mr. Arnzen: If you have those two high speed tracked vehicles going to opposite directions and apparently very close together according to the slide, what do you do about the negative pressure between the two vehicles, aren't they going to be drawn together? Question No. 2 - The Airlines have for years used JP-4 for safety What do you use JP for? No. 3 - In connection with the bird strike on the windshield, are you considering the possibility of things like icicles hanging down from bridges hitting the windshield too. They can be pretty tough.

MR. ARNZEN: In regard to the first question, this is a necessary portion of wind tunnel research. I believe you struck on a very good point: the bow wave from one vehicle would impart a shock wave against the opposing vehicle coming in the opposite direction. I believe this would be an essential part of the wind tunnel work to study this interaction. Conceivably it could be a violent whack and you might call it similar to two snow plows passing each other with a three-foot gap. The wind tunnel data would indicate the optimum distance. Conceivably, it might be better to put one guideway on one side of a turnpike, whether it be an interstate parkway or priority real estate already assigned, and perhaps the wind tunnel data would tell us it should go on the opposite sides. In regard to the use of the fuel. These particular engines, the engine manufacturer recommended use of this, this is not our selection although one fuel would be slightly less volutable than the other, we think we have eliminated the volutable problem by the non-destructive crashworthy tanks, the well-ventilated compartments of these tanks, the isolation from vapor even getting into lem compartment and the overboard venting procedures during refill. We are aware of many precautions which have to be taken in handling this fuel. The last question in regard to bird strike damage, on Gulfstream 1 and 2 we have conducted tests with 15 lb. birds and this is interesting. You actually can encounter certain birds up as high as 30,000 feet. Destructional integrity is such of these crash resistent windshields that they will take bird strikes. However, the gentlemen who referred to the transit program and the various problems presented came up with something interesting which we have to put in our cap. Bricks dropped by children from overpasses, icicles and things of that sort, warrant new and fresh consideration. There will be a whole new spectrum of hazards--a whole new ball game and I think that is a good question.

QUESTION: Mr. Driver, everyone has a car so everybody is an expert. Assuming that speed of course is by definition a problem on the road, in the diagrams that you showed I saw nothing being done about what might be described as too much engine and not enough bumper. Is anything being done in that area or contemplated?

MR. DRIVER: We have out now a notice that controls rulemaking which addresses the problem of speed control. It identifies speed warning and speed control, they are two separate functions. One to advise the driver that he is going too fast and the other one is to keep his car from going too fast, either by virtue of control of horsepower or by virtue of a speed control device like a governor. In the area of bumpers, amazingly enough most of the bumpers that you now have will not survive a two-mile an hour impact, without humping the front end. I have had personal evidence and I guess most of you have had also. We are now proposing a five and a ten mile an hour bumper however the bumper is just the first thing to get hit and is just a part of the total energy absorption system that we are trying to develop for a vehicle. This will include not only "energy absorbing bumpers" but also "energy absorbing front ends." For example, the hinge front end, Ford now calls it the X-member. Shock continuation through the entire body frame plus

the passive restraint to keep you where you should be so you can ride down the G forces instead of smacking up against the interior of the vehicle at High-G forces. We think we are taking a systems look at it. Those two you mentioned are a part of the total problem.

R.M. WILMOTTE: This is really a comment about a statement of Mr. Williams. The comment I want to make is in connection with operating correctly the first time. I think there is a danger in referring to doing anything correctly. There is always a residual failure, a residual uncertainty and that comment has influences if you say that you have done something correctly the first time. It influences two groups; one management, the manager says well now I can do what I want I have no dangers, but there is always a probability of a danger. The second is the operating level I'll give you the example of the well documented zero defect propaganda. I'll quote a comment from a manufacturing engineer manager whom I held very highly. His statement was something like this; After the President had made his one-half hour speech saying we must have zero defect in this company etc., there was an improvement in his shop for something like two weeks and then it fell back, not to where it was, but something to worse than it was. What were reasons? The reasons are rather interesting. He said, before that speech I used to know pretty well where in my shop the troubles came, and I was generally told about them in some way or other. After that speech there was a very wonderful cooperation among the workers that they wouldn't tell me where the troubles were and I couldn't find them anymore. From that point of view the product of my shop dropped. I heard that specifically from this individual but I also heard a confirmation of that in other places so I would like to give a warning, the possibility of using in any form, that anything can be perfect or that anything can be done right the first time has associated with it certain dangers.

The next thing that I want to say concerns Mr. Driver. I am always interested in the relationship between an activity that looks as though it was self-contained but never is. It is always connected with some other activity. You've been concentrating, and I'm sure you know what I say is quite obvious to you and you know it thoroughly, but your description refers entirely to the saving, the safety of life, I'll say or reduction of accidents. You cannot isolate that from the cost. Politically we say to save a life is worth an infinite amount of money, well, that just isn't true because we never do that. In the case of automobiles you have two ways of obtaining a price for safety. One is by taxing in which the federal government or the state governments impose a regulation, impose a tax and pay for some things such as improving the road bed. The other is to impose a structure in the equipment which costs something and is politically easier to handle because it merely is represented in a price which the buyer doesn't know specifically how much of that is for safety and how much is for better paint or something. Besides the price angle, there is the pollution angle. Does the safety requirement that you put on increase pollution? I suggest that generally it does. The real problem, I give you an example that came rather interestingly; There were a number of accidents on tractors and the tractor manufacturer improved his tractor in order to reduce the accidents and indeed it was a pretty good improvement but strangely enough the number of accidents remained the same. Why? Because the operators of the tractors now used it in more dangerous conditions because there were less accidents. Until the number of accidents drew up to about the same as they were before then they stopped endangering the equipment. There is a strong tendency which I think is very much to the point of the automobile process. You will find over the years that the accident rate strangely enough has remained remarkably constant with all kinds of changes that have been put in. It is true that recently there has been a decrease. But there were decreases like that as something happened and for a while it decreased; but there is a tendency to go back. In other words, I think that probably we are generally increasing the speed of our automobiles up to the point that we don't like to get killed anymore. That is, we hear of our friends or people know of someone who has been killed in an automobile accident. If we hear too

much of that then we drive more carefully. If we hear less of that we drive less carefully. We speed up and there is a tendency to, I think you'll find some literature on the subject, for humans to build up their danger up to a certain point and strangely enough that point is very much the same in all kinds of accidents. In the case of automobiles and where we put heavier bumpers and reduce the accident rate because of something of this kind, you are likely to find over the years, if the philosophy I am describing is correct, you will describe over the years, first of all a increare in weight of automobiles which will use more gasoline for more pollution. Secondly, a higher speed because there are few accidents, therefore, we want to build up the accidents and one of the benefits of course of all this is that you want to balance not only the accident rate but the price. The pollution and the value of the automobile. Namely reducing time and under the strange pressure that our society and civilization has built, time seems to be not necessarily measured in dollars but I don't have time to do what I want to do therefore I want to go fast.

MR. DRIVER: I'll respond yes. No. 1 on cost to save. I quite agree that there is a cost penalty for practically any innovation or anything new. In our case what we try to do is to institute a performance of clamor with such an effective lead time that it can involve only redesign of an existing piece of equipment. Like redesign of a brake instead of add on of another piece of equipment. This cuts the cost down quite a bit. In addition, some of our performance requirements involve the elimination of some parts of the vehicle and the substitution, say the elimination of two pieces of equipment and the addition of one piece of equipment so that in many cases the cost is balanced off. We do run safety cost benefit analysis in each case to determine and we hate to equate the life to a dollar but you have to do it sometime and we take a good hard look at what are we getting for our money. If we institute safety device or safety requirement No. 1, approximately how many lives are we going to save, how many injuries are we going to reduce. How many crashes are we going to avoid? We equate that with how much it is going to cost you as a consumer per vehicle to get that. Then we take a look at those figures. If they are in the red it doesn't mean we won't do it. I'll give you a very concrete example. The furor about power windows. A safety standard came out on power windows, it required certain minor changes to the power window system, in actuallity the number of lives lost as a result of improper action of power windows was low but those that happened to get killed happened to be kids and one of them happened to belong to somebody in pretty high places. The same thing of school bus standards, you have many more school kids getting killed in automobiles than you have getting killed in school buses but what do we do for automobiles to protect children, what do you do for a school bus when something happens. In summary, we are doing something and we are trying to implement it in such a way that the cost is minimized. In terms of increase in pollution, the only standard that I know of that pertains to pollution in our particular case is one that reduces it and that is the one on the fuel tank for example. The fuel tank is no longer vented to the atmosphere and if I remember my figures right from when I was working on the low pollution automobile about 15% of your vehicle pollution is plain ole evaporation out of the fuel tank. I admit that if we would come out and require that vehicles have bigger engines and lower rpm etc. and give more exhaust out of the exhaust you might be adding to pollution, I'll just quarrel with you on that a little bit that's all.