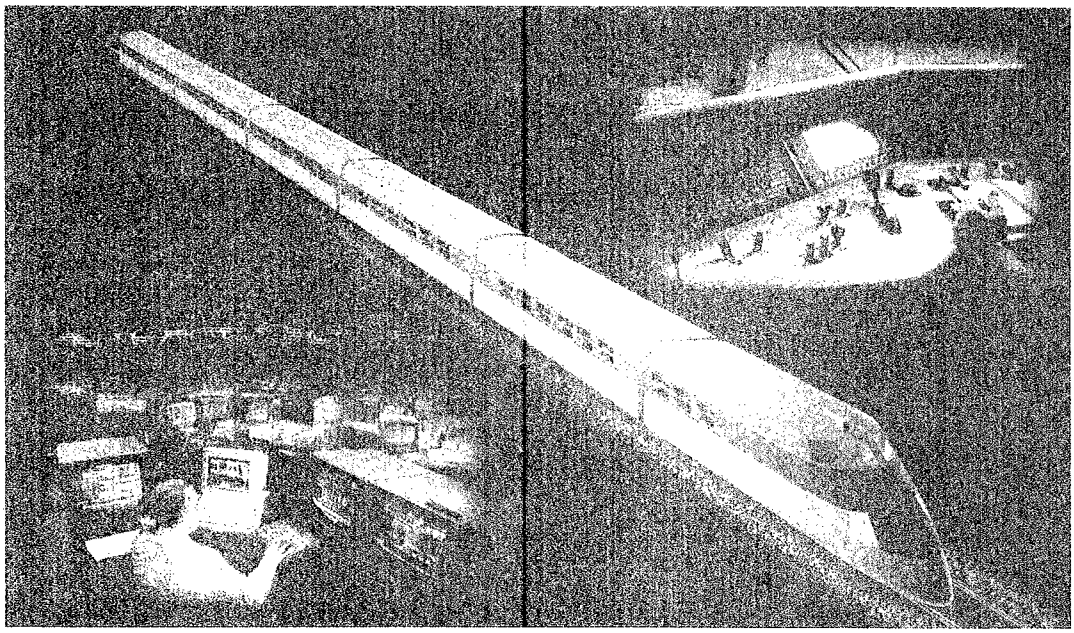
U. S. Department
of Transportation
**Federal Railroad
Administration**

Safety of High Speed Guided Ground Transportation Systems

Office of Research
and Development
Washington, D.C. 20590

Human Factors Phase I: Function Analyses and Theoretical Considerations



DOT/FRA/ORD-94/24
DOT-VNTSC-FRA-94-4

Final Report
October 1994

This document is available to the public through the National Technical Information Service, Springfield, VA 22161

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	October 1994	Final Report August 1992 - April 1994

4. TITLE AND SUBTITLE
Safety of High Speed Guided Ground Transportation Systems - Human Factors Phase I: Function Analyses and Theoretical Considerations

5. FUNDING NUMBERS
RR493/R4021

6. **AUTHOR(S)**
T. Sheridan, E. Lanzilotta, S. Askey

7. PERFORMING ORGANIZATION **NAME(S) AND ADDRESS(ES)**
Human-Machine Systems Laboratory*
Massachusetts Institute of Technology
Cambridge, MA

8. PERFORMING ORGANIZATION REPORT NUMBER
DOT-VNTSC-FRA-94-4

9. **SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)**
U.S. Department of Transportation
Federal Railroad Administration
Office of Research and Development
400 7th Street, SW
Washington, DC 20590

10. SPONSORING/MONITORING AGENCY REPORT NUMBER
DOT/FRA/ORD-94/24

11. SUPPLEMENTARY NOTES
*under contract to: U.S. Department of Transportation, Research and Special Programs Administration, John A. Volpe National Transportation Systems Center, Cambridge, MA 02142

12a. DISTRIBUTION/AVAILABILITY STATEMENT
This document is available to the public through the National Technical Information Service, Springfield, VA 22161

12b. DISTRIBUTION CODE

13. ABSTRACT (Maximum 200 words)

Although the speed of guided ground transportation continues to increase, the reaction time as well as the sensory and information processing capacities of on- and off-board operators remain constant. This report, the first of two examining critical human factors issues in future high-speed rail systems, focuses on the implications of this disparity on safety. It discusses the human factors aspects of French, German, and Japanese high-speed rail systems. It reviews salient human factors literature relevant both to human-machine functional allocation and safety in rail systems, and makes comparisons to similar aspects of operating aircraft, nuclear power stations, and other complex systems. Function analyses for high-speed train cab operation and dispatching centers are presented in the form of flow diagrams. Scenarios of abnormal conditions are suggested. Finally, the report addresses human-machine allocation and automation in controlling future high-speed trains, including the safety implications of various levels of automation.

14. SUBJECT TERMS
Human factors, transportation, automation, safety, high-speed trains, maglev, human-computer interaction, supervisory control, function allocation, function analysis, decision aids

15. NUMBER OF PAGES
104

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	

METRIC/ENGLISH CONVERSION FACTORS

ENGLISH TO METRIC

LENGTH (APPROXICUTE)

1 inch (in) = 2.5 centimeters (a)
1 foot (ft) = 30 centimeters (cm)
1 yard (yd) = 0.9 meter (m)
1 mile (mi) = 1.6 kilometers (km)

AREA (APPROXIMATE)

1 square inch (sq in, in^2) = 6.5 square centimeters (cm^2)
1 square foot (sq ft, ft^2) = 0.09 square meter (m_2)
1 square yard (sq yd, yd^2) = 0.8 square meter (m^2)
1 square mile (sq mi, mi^2) = 2.6 square kilometers (km^2)
1 acre = 0.4 hectares (he) = 4,000 square meters (m^2)

MSS - EIGHT (APPROXIMATE)

1 ounce (oz) = 28 grams (gr)
1 pound (lb) = .45 kilogram (kg)
1 short ton = 2,000 pounds (lb) = 0.9 tonne (t)

VOLLUE (APPROXIMATE)

1 teaspoon (tsp) = 5 milliliters (ml)
1 tablespoon (tbsp) = 15 milliliters (ml)
1 fluid ounce (fl oz) = 30 milliliters (ml)
1 cup (c) = 0.24 liter (1)
1 pint (pt) = 0.47 liter (1)
1 quart (qt) = 0.96 liter (1)
1 gallon (gal) = 3.8 liters (1)
1 cubic foot (cu ft, ft^3) = 0.03 cubic meter (m^3)
1 cubic yard (cu yd, yd^3) = 0.76 cubic meter (m^3)

TEMPERATURE (EXACT)

[(x-32)(5/9)] ^oF = y ^oC

METRIC TO ENGLISH

LENGTH (APPROXICUTE)

1 millimeter (mm) = 0.04 inch (in)
1 centimeter (an) = 0.4 inch (in)
1 meter (m) = 3.3 feet (ft)
1 meter (m) = 1.1 yards (yd)
1 kilometer (km) = 0.6 mile (mi)

AREA (APPROXIMATE)

1 square centimeter (cm^2) = 0.16 square inch (sq in, in^2)
1 square meter (m^2) = 1.2 square yeards (sq yd, yd^2)
1 square kilometer (km^2) = 0.4 square mile (sq mi, mi2)
1 hectare (he) = 10,000 square meters (m^2) = 2.5 acres

CUSS - EIGHT (APPROXIMATE)

1 gram (gr) = 0.036 ounce (oz)
1 kilogram (kg) = 2.2 pounds (lb)
1 tome (t) = 1,000 kilogram (kg) = 1.1 short tons

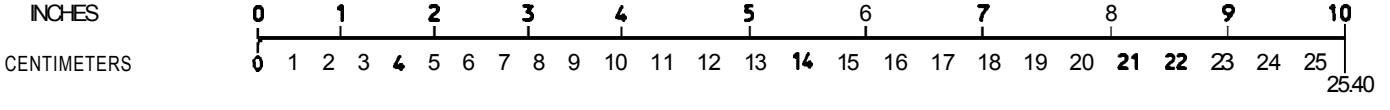
MLLUE (APPROXIMATE)

1 milliliters (ml) = 0.03 fluid ounce (fl oz)
1 Liter (1) = 2.1 pints (pt)
1 liter (1) = 1.06 quarts (qt)
1 liter (1) = 0.26 gallon (gal)
1 cubic meter (m3) = 36 cubic feet (cu ft, ft3)
1 cubic meter (m^3) = 1.3 cubic yards (cu yd, yd^3)

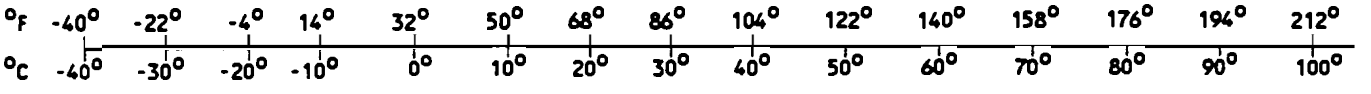
TEMPERATURE (EXACT)

[(9/5) y + 321 ^oC = x ^oF

WICK INCH-CENTIMETER LENGTH CONVERSION



WICK FAHRENHEIT-CELSIUS TEMPERATURE CONVERSION



For more exact and or other conversion factors, see NBS Miscellaneous Publication 286, Units of Weights and Measures. Price $2.50. SD Catalog No. C13 10286.

PREFACE

This is an initial report on an ongoing research program at the U.S. Department of Transportation's (USDOT's) John A. Volpe National Transportation Systems Center in collaboration with the Human-Machine-Systems Laboratory at the Massachusetts Institute of Technology. This work is supported by the USDOT's Federal Railroad Administration (FRA) Office of Research and Development as part of its program to assess the safety of high-speed train systems and to prepare for appropriate regulatory action should such systems be introduced in the United States.

The implications of higher speeds for the role of the operator (locomotive engineer, conductor, or dispatcher) on-board and at central control are being investigated, including allocation of tasks to human and machine. This report contains preliminary human factors considerations regarding high-speed ground transportation and related technologies, analyses of on- and off-board tasks, and theoretical considerations of safety.

As vehicle speed increases, the reaction time as well as the sensory and information processing capacities of on- and off-board operators remain constant. The history of railways teaches many lessons on the danger of developing the machine without considering the operator. For example, when the speed of the early steam engines approached 130 km/h (80 mph) in the mid 1870s, reliance remained on the locomotive crews' ability to stop a train with nothing more than a manual tender brake and the cooperation of the brakemen using hand brakes. The introduction of the Westinghouse continuous automatic compressed-air brake came too late for many. Similarly, it took many a derailment until it was realized that locomotive engineers needed a speedometer to observe speed restrictions. To prevent such problems, a switch from conventional to high-speed rail needs to be regarded as a qualitative change that not only exacerbates many existing human factors problems, but also adds new ones. Consequently, adjustments must be made to help the operator keep up with the machine.

The question of which adjustments best compensate for the discrepancy between vehicle and operator "speed" requires thorough examination, however. Whether considering an increase in automation or the provision of information processing or sensory aids to help operators cope with the new demands, the potential for creating new human factors problems while resolving old ones has to be taken into account. This project is an effort to prevent such errors when introducing high-speed guided ground transport in the United States.

ACKNOWLEDGMENTS

The authors are indebted to many people who contributed to this effort. In France, Annick Bachelard, Jacques Balause, Olivier Berzane, Daniel Gauyacq, Jean-Michel Gayon, Jean-Pierre Houillon, Bruno Kampmann, Jean-Pierre Macaire, Paul Monserié, Raymond Moulin, and others of Société Nationale des Chemins de Fer Français (SNCF) arranged a week of very helpful discussions and head-end rides for us on the Train à Grande Vitesse (TGV.) Mme. Régine Vadrot and Capt. Kheireddine Belguedj of Aeroformation in Toulouse are also to be thanked for arranging an informative visit to discuss training and automation for the new Airbus A330/340 aircraft. In Germany, Dr. Lutz Bauer and Michael Seemann of Deutsche Bundesbahn (DB) provided similar favors for the Intercity Express (ICE). Dr. Wolf Raasch was most gracious in showing some of us around the Emsland test site of the TR-07 Maglev as well as providing a test ride. Riidiger Wiedenmann of TUV Rheinland kindly arranged the visit. In Japan, Makoto Shimamura, Hiroshi Nagaoka, and many others of East Japan Rail arranged visits to the EJR Safety Laboratory, training facilities, and some head-end rides on the Shinkansen.

In the United States, we are grateful to Don C. Scott, R.S. Strachan, John Lightner, Stephen Urban, Steven Jones, and other staff of Amtrak for head-end rides on Amtrak, visits to control centers, and helpful discussions. At the Washington Metro, we would like to thank Deputy General Manager of Operations, Fady P. Bassily, for fruitful discussions. Finally, the authors especially wish to thank Mr. Arne J. Bang of Federal Railroad Administration, and Dr. Donald Sussman, Mr. Robert Dorer, and Dr. Judith Biirki-Cohen of the John A. Volpe National Transportation Systems Center for their continuing interest and a great deal of assistance in the execution of this work.

TABLE OF CONTENTS

TABLE OF CONTENTS (continued)

TABLE OF CONTE TS (continued)

LIST OF ILLUSTRATIONS

LIST OF TABLES

ABBREVIATIONS AND TERMINOLOGY

The abbreviations and terminology defined by Battelle Corporation in its ***Glossary of Terms*** (Luedeke 1992) have been used wherever applicable. While most of the following terminology are directly from (Luedeke 1992), the authors have modified and added some definitions which are marked with a "*".

ATC	Automatic Train Control — The method for automatically controlling train movement, enforcing train safety, and directing train operations.
ATO	Automatic Train Operation — The portion of an ATC system that performs any or all of the functions of speed regulation, programmed stopping, door control, performance level regulation, and other functions normally assigned to the locomotive engineer, conductor, or train attendant.
ATP	Automatic Train Protection — The portion of an ATC system that ensures safe train movement by a combination of train detection, train separation, overspeed protection, and route interlocking.
Block	A length of track of defined limits, the use of which by trains and engines is governed by block signals, cab signals, or both.
Block Signal	A fixed signal at the entrance of a block to govern trains and engines entering and using that block.
Block Signal System	A method of governing the movement of trains into or within one or more blocks by block signals or cab signals.
Braking Distance	The maximum distance on any portion of any railroad which any train operating on such portion of railroad at its maximum authorized speed will travel during a full service application of the brakes, between the point where such application is initiated and the point where the train comes to a stop.
Cab*	The section of the power car of a trainset where the locomotive engineer works.
Cab Signal	A signal located in the engine control compartment or cab indicating a condition affecting the movement of train or engine and used in conjunction with interlocking signals and in conjunction with or in lieu of block signals.
Central Control*	That place where train control, train supervision, or dispatching is accomplished for the entire transit system; the train command center.

Civil Speed	The maximum speed allowed in a specified section of track or guideway as determined by physical limitations of the track or guideway structure, train design, and passenger comfort.
Coded Track Circuit	**A** track circuit in which the electrical energy is varied or interrupted periodically to generate signals from wayside to train.
Conductor*	The individual in charge of the train crew.
Consist	The makeup or composition (number and specific identity) of a train of vehicles.
DB	Deutsche Bundesbahn (German National Railway).
Dispatcher*	The person who plans, monitors, and controls the routing (meets, passes, etc.) of trains.
Dispatching Center*	The location where dispatchers work; could be a central room or wayside tower control locations.
Dynamic Braking*	**A** method of braking an electrically-powered train in which the motor is used as a generator and the kinetic energy of the apparatus is employed as the actuating means of exciting a retarding force.
Emergency	**A** condition which could cause bodily harm or severe physical injury to persons, and/or serious damage to equipment.
Emergency Braking	Irrevocable open-loop braking to a complete stop, at the maximum safe braking rate for the system (typically at a higher rate than that obtained with a service brake application).
Emergency Stop*	The stopping of a train by an emergency brake application which, once initiated, cannot be released until the train has stopped.
External Environment*	Anything external to a given trainset (e.g., track, wayside signal, object on the track, heavy wind, etc.)
Fail-safe	**A** characteristic of a system or its elements whereby any failure or malfunction affecting safety will cause the system to revert to a state that is known to be safe.
Fail-Soft	Pertaining to a system or component that continues to provide partial operational capability in the event of certain failures: for example, a traffic light that continues to alternate between red and green if the yellow light fails.
Failure	The inability of a system or component to perform its required functions within specified performance requirements.

Failure Mode	The physical or functional manifestation of a failure. For example, a system in failure mode may be characterized by slow operation, incorrect outputs, or complete termination of execution.
Fault	A defect in a hardware device or component, or an incorrect step, process, or data definition in a computer program.
Fault Tree Analysis	An analytical technique, whereby an undesired system state is specified and the system is then analyzed in the context of its environment and operation to find all credible ways in which the undesired event could occur.
Flow Chart	A control flow diagram in which suitably annotated geometrical figures are used to represent operations, data, or equipment, and arrows are used to indicate the sequential flow from one to another.
Function	A defined objective or characteristic action of a system or component.
GPS	Global Positioning System, a latitude-longitude location system provided by orbiting satellites.
Grade Crossing	A crossing of highways, railroad tracks, other fixed guideways, pedestrian walks, or combinations of these at the same level.
Guideway*	The surface or track, and its supporting structure, in or on which guided vehicles travel and which provides passive lateral control.
Hazard	An existing or potential condition that can result in an accident.
Headway	The time separation between two trains traveling in the same direction on the same track, measured from the instant the head end of the leading train passes a given reference point until the head end of the train immediately following passes the same reference point.
High-Speed Rail	A rail transportation system that operates at speeds in excess of 198 km/h or 125 mph.
HSGGT	High-Speed Guided Ground Transport.
ICE	Intercity Express — a high-speed train developed for German Federal Railways.
Interlocking	An arrangement of signals and signal appliances so interconnected that their movements must succeed each other in proper sequence and for which interlocking rules are in effect. It may be operated manually or automatically.
LCD*	Liquid crystal display.

LED*	Light emitting diode.
Locomotive Engineer*	The person who operates the train and monitors key safety systems.
Maglev	Magnetic levitation, usually used to describe a guided transportation system using magnetic levitation and guidance.
Magnetic Levitation	Levitation of a vehicle by magnetic force; it may be either by magnetic attraction or repulsion.
Malfunction	Any anomaly or failure wherein the system, subsystem, or component fails to function as intended.
Objective Function*	A function of several variables that defines the tradeoff among those variables to determine the relative goodness of system states.
Operator*	A person involved directly with a key aspect of train operation such as a locomotive engineer, train conductor, train attendant, or dispatcher.
Optimal Control*	A process that maximizes some explicit objective function.
Overspeed	In excess of maximum allowable safe command speed.
Pantograph	A current collecting apparatus having a long contact shoe which glides perpendicular to the underside of an overhead contact wire.
Recovery	The restoration of a system, program, database, or other system resource to a state in which it can perform required functions.
Redundancy	The existence in a system of more than one means of accomplishing a given function.
Regenerative Braking*	A form of dynamic braking in which the kinetic energy of the electric motor and driven machinery is returned to the power-supply system.
Reliability	The ability of a system or component to perform its required functions under stated conditions for a specified period of time.
Resistive Dynamic Braking*	Dynamic braking in which the energy is dissipated in an electrical resistance.
Risk*	A measure of the combined likelihood and severity of an accident or an undesirable event.
Risk Analysis	The development of a quantitative estimate of risk based on engineering evaluation and mathematical techniques for combining estimates of incident consequences and frequencies.

Route Integrity	The condition whereby a track or guideway section is safe for the entry and passage of a train.
Safety*	Judgment of acceptability of risk.
Service Braking	Any non-emergency brake application of the primary braking system.
Severity	The degree of impact that a requirement, module, error, fault, failure, or other item has on the development or operation of a system.
Shinkansen*	Japanese high-speed train.
Simulator	A device, computer program, or system that behaves or operates like a given system when provided a set of controlled inputs.
SNCF	Société Nationale des Chemins de Fer Français (French National Railways).
Software	Computer programs, procedures, rules, and possibly associated documentation and data pertaining to the operation of a computer system.
Specification	A document that specifies in a complete, precise, verifiable manner the requirements, design, behavior, or other characteristics of a system or component, and often, the procedures for determining whether these provisions have been satisfied.
Speed Control	The function of adjusting the instantaneous vehicle speed to a given speed level.
Speed Profile*	A plot of speed against the distance traveled or to be traveled.
State	The set of values of salient variables which characterize the condition of a system.
Switch Point	A movable tapered track rail, the point of which is designed to fit against the stock rail.
Switch (Track)	A pair of switch points with their fastenings and operating rods providing the means for establishing a route from one track to another.
Testing	The process of operating a system or component under specified conditions, observing or recording the results, and making an evaluation of some aspect of the system or component.
TGV	Train à Grande Vitesse (French high-speed train).
Track Circuit*	An electrical signal circuit of which the rails of the track form a part.

Validation	The process of evaluating a system or component during or at the end of the development process to determine whether it satisfies specified requirements.
Verification	The process of evaluating a system or component to determine whether the products of a given development phase satisfy the conditions imposed at the start of that phase.
Wayside Control	**A** "command and control system" whereby electronic and/or mechanical devices alongside the guideway execute all or part of the necessary decisions inherent in command and control of the vehicles.
Wayside Equipment	Train control or movement apparatus which is located along the track or wayside (as opposed to the control center or other remote location).
Wayside Signal	**A** signal of fixed location along the track right-of-way.

---

* Item defined by the authors.

EXECUTIVE SUMMARY

In consideration of the already existing high-speed rail systems in Europe and Japan, it is anticipated that speed capability of passenger rail systems in the United States will increase significantly. It is also expected that new technology developments in sensors and high bandwidth communications through satellites and other means will enable the continuous, relatively precise measurement of train position and other state variables and the relay of information between trains and dispatching centers. Further, more accurate dynamic models are expected to become available and enable computation and control that can result simultaneously in on-time performance, improved safety, and reduction of energy cost.

This report, the first of two examining critical human factors issues in future high-speed rail systems, focuses on the human factors considerations that are important to maintain safe operations. It compares human factors aspects of high-speed train developments of the French TGV, the German ICE, and the Japanese Shinkansen. It reviews salient human factors literature and consultations relevant to both human-machine allocation and safety in rail systems, and makes comparison to similar aspects of operating aircraft, nuclear power stations, and other complex systems. The report presents function analyses for high-speed train cab operation and dispatching centers in the form of functional flow diagrams, and presents scenarios of abnormal conditions. Finally, the report addresses human-machine allocation and automation in controlling future high-speed trains, including the safety implications of various levels of automation.

Generally, to ensure route integrity, automatic interlocking systems developed for conventional passenger rail and urban mass transit systems have been adopted for High-Speed Guided Ground Transport (HSGGT). Wayside signals have been replaced or at least augmented by in-cab signaling, and in some cases the signal status is relayed back to dispatching centers. All systems operating at speeds exceeding 200 km/h (125 mph) have automatic train protection systems to monitor speeds and apply brakes as necessary to enforce safe speed. All have some form of device to monitor the alertness of the locomotive engineer and brake the trains if alertness criteria are not met.

With respect to the allocation of tasks to human and machine we found many interesting parallels to recent technical developments in commercial aviation, nuclear power generation, and similar high technology industries built around human-operated systems that serve the public. Issues of how to define safety and how far to go with automation are common, and in many cases these other industries have gone much further with automation while still maintaining excellent safety records. All of them, including HSGGT, are moving toward "glass cockpits" (computer-generated displays of integrated information).

Based on review of the literature, inspections of the French TGV, the German ICE, and the Japanese Shinkansen equipment, as well that of Amtrak, and extensive discussions with SNCF, Deutsche Bundesbahn, East Japan Rail, and Amtrak, we found both similarities and differences in approaches to human factors and automation in high-speed rail systems. All of these systems

continue to insist that a locomotive engineer be present in the cab, be familiar with the route geometry, and actively operate the train or at least continuously monitor as cruise control is employed for selected stretches of the route. However, on the ICE the existence of regenerative braking encourages more frequent use of cruise control while the locomotive engineer performs system management, while on the TGV the use of resistive dynamic braking encourages frequent coasting. In other more subtle ways the ICE seems to be automating more extensively, while the TGV and Shinkansen on-board control systems tend more toward aiding the "in-the-loop" locomotive engineer.

Our report presents an approach to function analysis through use of logical flow diagrams, and applies this, with examples, both to driving a high-speed train and to making dispatching decisions. Such analysis has been used extensively in the fields of aviation and nuclear power to understand the human-machine interactions and identify where equipment failures and human errors could have the most effect on system safety. This preliminary analysis identifies two additional problems that are exacerbated by higher vehicle speeds: sensing/communication delays and human decision latency, either or both of which could lead to command and control instability. Associated with this function analysis we outline sixteen classes of accident scenario which might be examined in greater detail, for example through running human-in-the-loop experiments using a trainset and/or dispatching center simulator.

The report goes on to provide a theoretical discussion of safety in terms of current notions of risk, probability, consequences, and utility (i.e., ultimate positive or negative value of consequences). Theories of human error definition and causation are reviewed, as well as generally recommended strategies for reducing human error. A Markov network approach to modeling safety is suggested, in particular the potential dynamic evolution of risk triggered by an equipment failure or human error.

Eighteen specific rail safety issues exacerbated by higher speed are mentioned, together with salient possibilities for technology transfer. These include delay and instability in command and control loops; preview and braking distance; accommodation of low speed passenger and freight trains; danger to and warning of maintenance crews; in-cab signaling; locomotive engineer view ahead; headway control and interlocking using discrete blocks vs. "moving blocks"; locomotive engineer alertness measures; speed-control decision aids and displays; in-cab display of other rail traffic; integrated "system health" displays for locomotive engineers and passengers; computer-based emergency procedures keyed to alarms; event-based vs. symptom-based emergency procedures; required pre-trip testing of brakes; computer-graphic schedule maps for dispatchers; enhanced large-screen displays for dispatching centers; "telepresence" inspection of remote locations on trainset or track; and design of systems and training of locomotive engineers and dispatchers to enhance cognitive consistency between their mental models and reality.

Finally, the report raises the ultimate questions of how much automation to plan for in future HSGGT systems, the degree to which optimal thrust and brake profiles can be determined and executed by computer, and whether or not to keep the locomotive engineer. In addition to current manual control with traditional displays, there are now options for manual control with display aiding; manual control with display aiding and modest automatic control options; and fully

automatic control with various emergency override controls by a locomotive engineer in the cab, elsewhere in the train (locomotive engineer/conductor), or in a centralized dispatching center (dispatcher). In selecting among these options, relevant considerations are basic system features and constraints (of the track, trainset, communications, etc.); proper view of the operator (locomotive engineer, conductor, or dispatcher) with regard to capability and reliability; introduction of new tasks for the locomotive engineer brought on by the automation; public perception and anxiety; and legal liability. An important factor to be considered when selecting among these options is the degree and type of maintenance required to maintain system safety. The question of maintenance has many human factors implications that we are planning to address in the near future.

The next step in our project is to develop and apply techniques for evaluating human-computer allocation, display of integrated information for decision-aiding, and analysis of safety and risk in dynamic evolution of failures/errors and recovery in **HSGGT** systems.

We find that the trend toward 'human supervisory control" or 'human centered automation" — humans aided by computers for information and planning, and implementation of control decisions through computer intermediaries — is highly applicable to future **HSGGT** systems. The new cooperation between human and computer does not require locomotive engineers or dispatchers to be computer programmers, but does insist on a higher level of training and technology literacy. We envision an evolutionary approach, beginning with a locomotive engineer aided by well engineered decision aids, and progressing to the locomotive engineer's discretionary use of automatic control. Finally, a commitment to full automation would occur only after passing though the earlier stages with demonstration of reliability of each new step and with sufficient public acceptance.

1. INTRODUCTION

1.1 BACKGROUND

High-speed rail technology offers great promise for future intercity passenger transportation. Both highway and air corridors between urban areas are rapidly reaching saturation, with limited possibilities for building additional highways or airports.

High-speed intercity rail systems are both popular and efficient in several developed countries. The Train à Grand Vitesse (TGV) in France, the Intercity Express (ICE) in Germany, and the Shinkansen in Japan are examples of high-speed trains in everyday revenue service. The speeds of these systems, currently in the range of 200 to 320 km/h (124 to 199 mph), continue to increase. Several nations have already experimented with magnetically levitated (maglev) systems, the German TR-07 being the furthest along in development, with speeds potentially far greater than conventional steel-wheel-on-rail systems (up to 500 km/h, i.e., 311 mph).

Although rail technology for revenue service was developed largely in the United States, high-speed passenger rail development here has lagged behind that in Europe and Japan. However, there is current interest in building several demonstration and revenue high-speed rail systems in the United States based on French and German technology and possibly that of Japan, Sweden, and other foreign technologies.

There are, as with any foreign technology, issues related to the adaptation of such technology in the United States. Among them are the questions of function allocation between human and machine, and the associated safety issues. These may require the development of regulations for the design and operation of high-speed trains due to the effects induced by "high speeds." The demands placed on a train system by such high speeds cannot be met only by altering the design, but will also require adaptation of the function allocation in the cab because of the following:

1. Higher speed means greater kinetic energy of any collision (by the square of the velocity) and therefore exacerbates the severity of an accident. As pointed out by the study on collision avoidance and accident survivability (DOT/FRA 1993a), "… the results of a collision at high speed, over 200 km/h (125 mph), would result in severe damage to several vehicles or vehicle sections, and multiple fatalities. These results suggest that it is not possible to ensure survivability in high-speed collision with any reasonable vehicle design philosophy, and the safety emphasis in High-Speed Guided Ground Transportation (HSGGT) systems must be on the avoidance of such accidents."

2. Higher speed also reduces the allowable response time for external environment-related events. Therefore, assuming a locomotive engineer is to be responsible for speed control, higher speed will:

   a. increase the cognitive workload per unit time,

   b. require displays which are quick and easy to interpret, and

c. pose greater demands on the locomotive engineer to anticipate or be aware of the potential dangers and be able to make quick and appropriate control decisions.

3. Higher speed makes it more difficult for the locomotive engineer to see any wayside signals or other objects at the waysides, other visibility factors being equal. This, in turn, requires more in-cab information on a high-speed train than on a conventional train. Indeed, one major developer and user of high-speed trains, Société Nationale des Chemins de Fer Français (SNCF), has determined that the maximum speed for accurate perception of wayside signals by a locomotive engineer is 220 km/h (137 mph). This situation, along with minimum stopping distances of 4 to 5 km (2.5 to 3.1 miles) for operation at 300 km/h (186 mph) (DOT/FRA 1991b), suggests the necessity of a cab-based information system with reliable advanced information about the wayside for both the locomotive engineer and the automated systems.

1.2 PURPOSE AND ASSUMPTIONS

This report is part of a larger project to consider human factors and safety issues in HSGGT passenger rail systems. The purpose of this report is to assess the problems of safety as they relate to human factors in future high-speed passenger rail transportation systems in the United States, and to make recommendations to cope with such problems.

The report makes the assumptions that the following technologies are well developed and currently available for application to high-speed trains:

1. Global Positioning System (GPS) and radar systems based on the Doppler principle to locate trains continuously to within a few meters;

2. Reliable high-bandwidth communications between the train and the centralized dispatching and control centers;

3. Sensors capable of continuously monitoring the condition of locomotives, passenger cars (brake status, wheel slippage, etc.), and the state of track (including switches, bridges, tunnels, etc.);

4. Computer-based vehicle dynamic models and simulations capable of predicting relations among force, energy, speed, position, and time for trains moving on specific tracks;

5. Artificial intelligence, expert systems, fuzzy logic, neural nets, and other advanced computational technology for application to identification and diagnosis of problems, control of trains, and decision aids to operators.

The relevance of these technologies for human factors and safety will be discussed.

There are many aspects of human factors and ergonomics which we are not considering in any detail in this report, such as the traditional aspects of detailed design of displays, controls, and operator workplaces. Nor are we considering, to any significant extent, the selection and training of operators. However, it should be noted that the results of this work may have

implications in these two areas. We are focusing primarily on human roles and the allocation of functions to the operator versus automation to enhance safety in high-speed rail systems.

1.3 CONTENTS

Section 1 provides some background on high-speed train developments around the world, states the purposes and assumptions of this research, and describes the organization of the report.

Section 2 reviews literature we have read and consultations we have made relevant both to human-machine allocation and safety in general and to high-speed rail systems in particular.

Section 3 first presents function analyses for high-speed train cab operation and dispatching centers in the form of functional flow diagrams. This section also presents scenarios of abnormal conditions (which will be used for simulation and human-in-the-loop experiments later in this project but will not be reported here).

Section 4 discusses a variety of human error and safety issues specific to high-speed rail systems.

Section 5 addresses the issue of human-machine allocation in controlling future high-speed trains, including the safety implications of various levels of automation.

Finally, Section 6 summarizes and presents our current conclusions and recommendations regarding human-machine allocation and safety issues on high-speed trains.

2. REVIEW OF LITERATURE AND CONSULTATIONS

2.1 CURRENT STATUS OF SIGNAL AND TRAIN CONTROL SYSTEMS

To address human-machine allocation in future high-speed trains, we can draw from the experiences with current signal and train control technology. There are three primary functions of a HSGGT signal and train control system (DOT/FRA 1993a, Amtrak 1992):

1. ***Ensure route integrity.***

   Purpose: This function ensures that only safe movement authorities can be issued to a train. A safe movement authority consists of the following three conditions (DOT/FRA 1993a):

   a. The track or guideway to be traversed is clear of other trains or vehicles, or any obstruction;

   b. The necessary switches are properly aligned; and

   c. No conflicting movement authorities have been issued.

   Method: The equipment that ensures route integrity is called an ***interlocking*** in traditional railroad terminology. An interlocking is an arrangement of signals and signal appliances so interconnected that their movements must succeed each other in proper sequence and for which interlocking rules are in effect (Luedeke 1992). Until the 1980's, all interlockings consisted of hard-wired relay logic (as early as the 1850's for mechanical interlockings (GRS 1979)). However, most new installations and upgrades of signal systems use software-controlled microprocessor systems. Key inputs to the interlocking system are the locations of all relevant trains, the current movement authorities, and the status of switches relevant to the interlocking.

   An interlocking may be operated manually or automatically. Automatic interlockings are activated by the presence of anything (usually a train or engine) that shunts any of the track circuits that are part of the interlocking. Such an automatic interlocking usually is designed (wired or programmed) to operate so that the first train to arrive locks out opposing signals on the conflicting route(s) and then causes signals for the first train's route to be cleared (GRS 1979).

   Status in HSGGT systems: In general, automatic interlocking systems developed for the conventional railroad and mass transit industries have been adopted by HSGGT systems. Except for emergency low-speed operations after a relevant equipment failure, manual performance of this function (ensuring route integrity) is unheard of on a HSGGT system (DOTIFRA 1993a).

2. ***Communicate movement authorities to locomotive engineer or on-board control system.***

Purpose: This function ensures that safe movement authorities issued from the interlocking systems are conveyed correctly to the vehicle motion controller, be it a locomotive engineer in the cab, a dispatcher in a fixed control center, or an Automatic Train Operation (ATO) system.

Method: On a traditional railway, this is done by the locomotive engineer's observation of wayside signals and, in some cases, of in-cab signals. On automated and semi-automated rapid transit systems, an ATO system replaces the locomotive engineer's direct observation functions by receiving movement authorities automatically and acting accordingly.

Status in HSGGT systems: In HSGGT systems, wayside signals are supplemented or replaced by in-cab signals or displays. In some automated cab-signaling systems, the communication system provides feedback to the dispatching center on the status of the signal or instruction transmission.

3. ***Enforce safe speed.***

Purpose: This function ensures that movement authorities and speed limits are always obeyed, whether the vehicle is under manual or automatic control.

Method: This function is usually carried out by an Automatic Train Protection (ATP) or an Automatic Train Operation (ATO) system. Such a system automatically supervises the locomotive engineer's actions and initiates braking if speed limits or signal indications are not observed.

Many conventional rail systems lack any kind of safe-speed enforcement, relying completely on the judgment and capabilities of the locomotive engineer.

Status in HSGGT systems: All HSGGT systems operating at speeds over 150 km/h (95 mph) are equipped with a comprehensive ATP system that enforces speed limits and train control instructions. Such an ATP system ensures safe train movement by a combination of train detection, train separation, overspeed protection, and route interlocking (Luedeke 1992). The overspeed protection takes the form of either automating safe-speed enforcement actions or automatically monitoring the locomotive engineer's actions to minimize the risk of human errors that may lead to a collision or derailment.

Many ATPs (for example, those on the ICE and the TGV — see Section 2.4.1.3) cannot be overridden by the locomotive engineer until after the emergency braking activated by the ATP brings the train to a full stop.

There are two general types of ATP systems, distinguished in terms of how information is transmitted from wayside to the train (intermittently and continuously). A brief comparison between these two types of ATP systems follows:

a. **Data frequency:** Intermittent ATP systems transmit a "packet" of data to a train as it passes a wayside beacon. In contrast, continuous ATP systems maintain constant guideway-to-train communication, whereby updated data can be transmitted to the train at any time.

b. **On-train equipment:** Both types of ATP systems require certain on-train computers for monitoring the train's movement against the speed limits. If these specific speed limits are exceeded, braking action is initiated by the ATP system. In some cases, these computers calculate the braking action required to meet an anticipated speed limit, and automatically initiate braking if the locomotive engineer fails to maintain the train within the allowed speed envelope.

c. **Wayside equipment:** For intermittent ATP systems, beacons are intermittently placed along the track wayside, while for continuous ATP systems, coded track circuits are used to transmit data from the guideway to the train. Coded track circuit systems of this type are used on the Japanese Shinkansen, the French TGV Atlantique and Sud-Est lines, and many mass transit systems.

d. **Data complexity:** The data transmitted via intermittent ATP systems typically include line speed limits and required speed at the next signal. If these specific speed limits are exceeded, braking action is initiated by the ATP system. The traditional form of continuous ATP using coded track circuits to transmit data has very limited capacity, typically a small number of signal or "permitted speed" indications. More sophisticated continuous ATP systems have now been developed, such as the German LZB (for Linienzugbeeinflussung) and the French TVM430 systems, which have a higher data capacity than traditional coded track circuits.

Pros and Cons: Intermittent ATP systems are relatively economical and interface well with existing signaling systems. However, they are not well suited to high density operation where trains follow one another at close headways, such as on a mass transit system, because a train can respond to a changed situation only after it reaches the next beacon.

In contrast, continuous ATP systems can be designed to have large data capacity. Such systems are under development in Germany and France, as mentioned earlier. In addition, two-way communications (by the German LZB) and some elements of ATO can also be accomplished with a continuous ATP system (DOT/FRA 1993a).

2.2 SAFETY OF HIGH-SPEED RAIL SYSTEMS

Lowrance (1976) defines the 'determination of safety as an effort which requires both an assessment of risks and a value judgment of taking risks. He further classifies the component of risk assessment as a scientific activity, while the value judgment is deemed to be an economic, sociological, and/or political endeavor. In related work, Marshall (1982) gives a good overview of some risk assessment techniques, such as Failure Mode and Effects Analysis (FMEA), event tree analysis, and fault tree analysis.

The study of high-speed rail safety was initially based on review of the existing safety documentation published by the U.S. Department of Transportation. Bing (DOT/FRA 1993a, 1993b, 1993c, 1993d) has provided one of the most comprehensive reviews on the subject. In this report, a specification for high-speed guided ground transportation system collision avoidance and accident survivability is developed in a four-step process: evaluation of the collision threat, detailed review of the state of the art in collision avoidance, detailed review of the state of the art in accident survivability, and development of a proposed specification for collision avoidance and accident survivability. Particularly of interest are the sections which discuss the identification of potential accident scenarios, recommended guidelines for collision avoidance and accident survivability, and the definition of equivalent safety.

In other related reports, Dorer (1991, 1992) studies the German approach to safety, particularly in the Transrapid system. Bing et al. (1990) make a detailed study of the signal and control systems required in the German Transrapid Maglev systems. All of these documents were extremely useful, as they identified the known safety issues, as well as the traditional approaches to satisfying the safety requirements, with extension to higher speed Maglev systems.

Safety in highway transport is an important related field, and there was substantial investigation into the literature in this area. There exist several key compilations on the efforts of highway safety research (Forbes 1972, Stammer 1988, Goedken 1985). Much of this work involved interesting discussions regarding safety legislation and research goals.

In an effort to apply systems and control engineering principles to the study of safety in high-speed guided transport, an intensive review of appropriate control engineering texts was conducted. These included books by Friedland (1986), Gelb (1974), Karnopp and Rosenberg (1975), and Ogata (1990). Operation of high-speed guided transport is felt to have many parallels to aircraft operation. McRuer et al. (1973) provide a good resource for human behavioral models in controlling aircraft, as well as analytical methods for characterizing this type of behavior. In particular, their work provides important insight into the interface between operators and air vehicles. Wiener et al. (1988) contains pertinent information on the human factors issues in flight systems. Also of related interest are the parallels drawn with teleoperation (Sheridan 1992).

To gain greater insight into the human operator and the models of human behavior, we reviewed key texts on human factors and human-machine systems (Sanders and McCormick 1987, Sheridan and Ferrell 1974, Salvendy 1987). In addition, work by Reason (1990) provides insight into the understanding and classification of human error patterns. However, notably absent throughout all of these documents was a concise definition of safety. Also absent was a prescribed methodology for measuring risk or validating the safety issues. We believe that assessment of risk, particularly from the perspective of the actions of an element (human or computer) which has some range of control in an HSGGT system, is a very important component of this research.

2.3 FUNCTION ALLOCATION AND RELATED HUMAN FACTORS

The problem of function allocation between human and machine has always existed in any human-machine system design. Perhaps the first formal treatment of function allocation was made by Fitts (1951). His method consisted of a general list of functions performed better by machines than humans, and vice versa. A function was allocated to either the machine or the operator, whichever was better at performing this function according to the "Fitts list" or some elaborated version thereof.

Such comparisons serve a useful role in at least an elementary way (Chapanis 1965), and are valued for delineating characteristic abilities of humans and machines to perform broad classes of functions (Meister 1971). However, for various reasons, the Fitts list has had little practical impact on engineering design. First, the allocation criteria are overly general and non-quantitative; in addition, they assume that functions will be performed by either humans or machines. Second, the allocation is necessarily static; once implemented, it is largely situation-independent and unchanging with time, and therefore does not permit systems engineers to exploit the flexibility of applying computers in system design. Third, the allocation does not consider human and economic factors of the design (Jordan 1963, Chapanis 1965, Price 1985, Sanders and McCormick 1987, Rieger and Greenstein 1982, Greenstein and Lam 1985).

Jordan (1963) believes that the concept of comparing humans and machines is erroneous. These criteria are deemed futile because humans and machines are not comparable, but complementary. Humans and machines can perform complementary activities to fulfill functions. Since a function can be decomposed into tasks or subtasks, work may be divided at the task or subtask levels in the hierarchy of system operations. The tasks or subtasks may be performed by humans or machines. This criticism seems to support the first limitation.

In view of the limitations of human-machine comparisons according to the Fitts list, some methodologies have been proposed to compute, using some formula, the suitability of human performance against that of a machine, for any particular function (Price and Pulliam 1983). These methodologies presumed that human performance data would exist from which the performance of humans could be predicted and compared with engineering predictions for a machine. This formula would depend on the availability of quantified data on human performance; data that could be calibrated to the specific conditions of a new design. According to Price and Pulliam (1983) and Price (1985), however, such data may never exist. The complexity of real work settings, which involve numbers of human and machine variables that are beyond practical listing and computing, suggests that functions cannot be allocated by formula. The allocation process must rely on expert judgment as the final means for making meaningful decisions; allocation of function is as much an art as a science.

Although there are no clear-cut guidelines for making specific allocation decisions, Price (1985) suggests four rules for arriving at a hypothetical allocation:

1. ***Mandatory allocation.*** Some functions or portions of functions may have to be allocated to the human or the machine because of system requirements (e.g., a human must be present to override automation, if necessary), hostile environments, safety considerations, or legal or labor constraints. Mandatory allocations should be identified and made first.

2. ***Balance of value.*** Determine a hypothetical allocation based on the relative "goodness" of humans or machines as performers of the intended function. This is basically a process of comparing the relative goodness of humans and machines for a given function. Instead of using a Fitts list, the allocation is determined by estimating values of performance goodness and representing them as a point in a two-dimensional decision space (human performance versus machine performance). Depending on the location of the point in decision space, the function could be allocated to humans, machines, or neither. In the last case, it is suggested to redefine the system requirements or constraints, or treat the function as a case of mandatory allocation and allocate to the acceptable alternative.

3. ***Utilitarian and cost-based allocation.*** In utilitarian allocation, a function may be allocated to humans simply because human beings are present and there is no compelling reason why they should not perform the work. The relative cost of human and machine performance must be considered, and allocations can be made on the basis of least cost.

4. ***Affective and cognitive support allocation.*** The final rule recognizes the unique needs of humans. Allocation decisions may have to be revised to provide affective and cognitive support for the humans in the system. ***Affectivesupport*** refers to the emotional requirements of humans, such as their needs to do challenging work, to know their work has value, to feel personally secure, and to be in control. ***Cognitive support*** refers to the human need for information so as to be ready for actions or decisions that may be required. The human must maintain an adequate "mental model" of the system and its condition in order to take control in an emergency. Another consideration in cognitive support is that the human be given sufficient activity to ensure alertness.

Price finally suggests that the rules outlined above should be viewed as a reasonable starting point with the understanding that the detailed decisions still depend on the judgments of experts. The authors think, however, that Price's view that function allocation ultimately relies on the judgments of experts may be too pessimistic about possible developments of analytical tools for aiding function allocation. Note that Price's approach still bears limitations similar to those of the Fitts method. In fact, Fitts said that using the criteria in his list as the sole determinant of the allocation of functions was to lose sight of the basic nature of a system containing humans and machines (Fitts 1951).

Thus function allocation in designing a human-machine system is still an ***ad hoc*** procedure and few application papers or documentation exist, especially as related to high-speed trains.

2.4 HUMAN ROLES IN HSGGT SYSTEMS: SPECIFIC PRACTICES

2.4.1 Comparative Review: TGV, ICE, and Shinkansen

This section reviews major high-speed train systems of the world: the Train à Grande Vitesse (TGV) of France, the Intercity Express (ICE) of Germany, and the Shinkansen of Japan. The review focuses on comparing the TGV with the ICE in terms of various human-machine system aspects. Where information is available, the Japanese Shinkansen train is also compared. The aspects under discussion are:

- braking system,
- speed control,
- monitoring manual control by automatic systems,
- routine locomotive engineer tasks,
- cab signaling system: information from the wayside to the train,
- cab signaling system: information from the train to the wayside,
- wayside signals,
- displays on locomotive engineer's console,
- maintenance monitoring system,
- alerter system,
- voice communication system,
- emergency train control by passengers,
- locomotive engineer selection and training, and
- dispatching center.

2.4.1.1 Braking System

There are significant differences in braking systems between the TGV and the ICE trains. While both trains have pneumatic and electro-pneumatic braking capabilities, the ICE is equipped with dynamic regenerative brakes, which allow the kinetic energy to be transformed into electric energy and returned to the power grid (DOT/FRA 1991a). In contrast, the TGV is equipped with resistive dynamic brakes, which implies that power is not fed back into the catenary; instead, resistor grids mounted in the roof enclosure of the power cab are used to dissipate the

braking energy (DOT/FRA 1991b). These differences contribute to the different speed control strategies in the two types of trains, which will be discussed in the following section'.

Testing and operation of the braking systems on the ICE and the TGV are computer assisted in a similar manner. For both trains, brake system tests are automated, and all brake systems are continuously monitored with the information relayed to the locomotive engineers via a computer screen at their console. The ICE's brake monitoring is also tied into the consist-maintenance monitoring system. The latter monitors on-board subsystems (e.g., braking and control systems) for their operational states. Under certain conditions, the monitored information is relayed to the wayside via data radio links for maintenance purposes. Thus, any brake component failures or operational problems will be reported to the ICE's maintenance facility by its consist-maintenance monitoring system prior to the train's arrival at the next maintenance facility (DOTIFRA 1991a).

Brake system failures are handled differently by the TGV and the ICE. Both the TGV and the ICE expect the locomotive engineer to continuously monitor the display of the brake system status and to respond appropriately to exceptions as they occur. In case of reduction of braking capability during a run, the ICE provides the locomotive engineer with computerized operation assistance. In addition, the locomotive engineer is to enter the changes in braking capability into a computer. This information is then transmitted to the wayside for maintenance planning. Moreover, after the change in braking capability is entered, the computer automatically compensates for any reductions in the braking capability in terms of available braking profiles and thus the maximum speed permitted by the Automatic Train Control system. On the TGV, written speed reduction tables are used instead of a computerized operation aid to reduce maximum operational speed for various combinations of brake system failures (DOTIFRA 1991b).

2.4.1.2 Speed Control

Although all train systems under discussion are equipped with an ATP system, there are significant differences in the degree of automation implemented. Operation of the ICE, for example, is considerably more automated than that of the TGV. Three operational methods are available on the ICE (DOTIFRA 1991a):

1. Fully automated speed control with ATP.

2. Cruise control with ATP. This control mode is set by manually selecting a target speed and then allowing the speed control to meet the target speed (much like the cruise control in automobiles). In fact, in this control mode the locomotive engineer uses the Automatic Speed Control by selecting a speed and letting the power and propulsion system automatically maintain that speed via various microprocessor controls tied into the power and braking systems.

---

† **Note that the ICE is also equipped with electromagnetic rail brakes. The electromagnetic track brakes are designed for possible retrofit to eddy current brakes in the future (DOT/FRA 1991a).**

3. Fully manual control with ATP. Manual operation utilizes the control system information on the console for guidance.

It is observed by Sussman (1993) that the ICE locomotive engineers use cruise control frequently, which is feasible in practice owing to the regenerative braking capability of the ICE. Such a style of driving is also encouraged by the function allocation design of the ICE train operation: the presence of sophisticated diagnostic tools and the requirement that primary attention be given to in-cab signals over wayside ones (or to in-cab signals which override wayside signals). Naturally, the cruise-control driving style and the function allocation design of the ICE operation foster much "head down time" on the part of the locomotive engineer. Therefore, it is appropriate to say that he or she is more of a supervisor than a direct manual locomotive engineer.

In contrast, manual control is the prevailing operation mode on the TGV (Sussman 1993, DOTIFRA 1991b), with computer monitoring and assistance. Under normal conditions, the TGV locomotive engineer is in charge of the controls of the trainset. He or she controls acceleration and deceleration of the consist (via applied traction power or resistive dynamic braking) by rotating a horizontal wheel on the console. This wheel, known as a ***traction controller,*** uses the rotational position to indicate the intensity of the function. A separate control permits the locomotive engineer to set the brakes on all cars in the consist via the electro-pneumatic brake pipe system. Pure pneumatic braking serves as a back up (DOTIFRA 1991b).

The Shinkansen is similar to the TGV in that the prevailing operation mode is manual control with computer monitoring and assistance. The locomotive engineer's job is to keep the train speed just below the speed limit by 2 to 5 km/h. Essentially, he or she uses two hand controls, a brake and a power control, one in each hand.

2.4.1.3 Monitoring Manual Control by ATP System

As mentioned before, all three types of trains, the ICE, the TGV, and the Shinkansen, have Automatic Train Protection (ATP) systems on board for monitoring the locomotive engineer's manual control (DOTIFRA 1991a, DOTIFRA 1991b). The specific conditions for activating the ATP vary across the different systems. For the TGV, if the locomotive engineer exceeds the maximum speed permitted by the signaling system, the ATP system will initiate an emergency braking action. The overspeed tolerance varies from 10 to 15 km/h (6 to 9 mph) with respect to the instance speed limits. The Automatic Surveillance System on board the TGV, which checks for the locomotive engineer's response as well as speed limit conformance, can be overridden in the event of a failure, if at least one other crew member is present in the cab (DOTIFRA 1991b).

The ICE on-board computer calculates two speed curves to guard the locomotive engineer from overspeeding in the manual control mode: the monitored speed limit curve, and the nominal speed curve. The former represents the use of emergency braking in order to reduce the speed to a certain level at a distance ahead; the latter represents a lower operational braking rate. If the train's speed exceeds the nominal speed curve, the locomotive engineer is warned of the overspeed. However, if the train's speed reaches the monitored speed limit, the speed control system initiates an emergency application of the brakes. During constant speed sections of the

nominal speed curve, the monitored speed limit is 8.75 km/h (5.5 mph) above the nominal speed.

In terms of ultimate control authority, locomotive engineers of both the ICE and the TGV have limited control once emergency braking is initiated. For the TGV, once an emergency braking action is activated, the locomotive engineer cannot intervene or reset the system until the train comes to a complete stop. For the ICE, in an emergency the locomotive engineer has available a brake valve directly connected to the brake pipe and can initiate emergency braking independent of all the automated systems.

2.4.1.4 Routine Tasks of Locomotive Engineer

Pre-run tests are similar for both the TGV and the ICE, and all are assisted by computers. In particular, before every run the ICE locomotive engineer keys in the train identification number, maximum speed, train length, and status of the braking systems. Similarly, before each run of a TGV Atlantique trainset, the TGV locomotive engineer tests the brake pipe for continuity and the friction brakes for a successful set and release. Upon boarding the TGV Atlantique, the locomotive engineer keys into the TORNAD network (TGV Atlantique on-board data processing network) to check items such as train lighting, air conditioning, door-closing mechanisms, and passenger information systems. This network also monitors the braking system and cab signal self-diagnostic system and records any failures found. The ICE has similar computer-mediated diagnostics available.

The primary task in train operation is speed control. As discussed in the speed control section, the ICE is equipped with more automatic control capability for train operation than the TGV. The ICE is equipped with three modes of speed control of which cruise control is most frequently used, while the TGV is mainly operated under manual control.

During a run of the ICE, the locomotive engineer monitors the states of the braking systems, the control systems (if non-manual control mode is used), and the passenger comfort systems. The on-board computers and diagnostic tools provide operation aid under abnormal conditions (Sussman 1993). Similarly, during a run of the TGV, the TORNAD system provides real-time system status of on-board equipment, announces faults if they occur, and presents computerized troubleshooting of failures to determine the correct remedial action (DOT/FRA 1991b). For example, the brakes are automatically monitored approximately once a minute (DOT/FRA 1991b, 17) and their status, for each car and truck, is relayed to the locomotive engineer via the computer screen located on the console. The locomotive engineer is expected to monitor the automated system that displays the status of the braking system and to respond appropriately to abnormal states as they occur.

For the Shinkansen, the locomotive engineer's operation procedures are a little different from those on the TGV and the ICE. When wayside signals are observed, for example, he or she overtly points and comments verbally (they are trained to do this as mnemonics). The locomotive engineers on the Shinkansens are said to have no responsibility for observing the track ahead and for stopping if something is on the track. If there is a breakdown in a tunnel, emergency procedure requires the train to proceed to the end of the tunnel before stopping. It

should be noted, however, that ICE locomotive engineers assess the situation and proceed to a predetermined stopping point outside of the tunnel if appropriate.

2.4.1.5 Cab Signaling:System: Information from Wayside to Train

Safety-relevant information sent from the wayside to the ICE trains includes:

- the distance to the next required stopping point,
- the braking curve to be utilized, and
- the traveling direction.

The control equipment on board the ICE train uses this information to determine where the train should be on the curve relative to the stopping point. Thus, the actual train speed to be achieved and the necessary braking or power commands are determined via on-board logic. The speed control system resides entirely on the train (DOTIFRA 1991a).

Other information sent from the wayside to the train that is necessary for effective ICE train control includes:

- target speed in 5 km/h (3.1 mph) increments,
- target distance,
- line gradient, and
- civil speed restrictions (i.e., related to track parameters).

Each ICE train on the line receives wayside information at least once every second. In case of a cab signaling system failure, if the failure affects the data related to control, the system reverts to a non-automated control mode.

The data transmission on the TGV Atlantique is not as extensive as that on the ICE. The signaling system on TGV Atlantique (named TVM300, and in use on TGV Paris-Southeast as well) depends on alternating current audio-frequency coded track circuits for track-to-train communication. Up to 18 channels are available. While traversing each block, the train receives data from the coded track circuits indicating the maximum speeds in both the current and next blocks (DOT/FRA 1991b). Block lengths are approximately 2 km and are marked on the wayside. The TGV also intermittently transmits additional information (such as absolute stopping points and pantograph up or down commands) to the train via inductive loops at key locations in the center of the track (DOTIFRA 1991b).

The difference between the TGV and the ICE in the content of information transmitted is mainly due to the system design differences. The regenerative braking facility on the ICE, as well as the ICE's speed control capabilities being more automated than those on the TGV, account for more speed-related information transmitted from wayside to the ICE train. The two pantographs on a

TGV power car resulting from its two-voltage power system;, and the dispatching center's control of electric power, explain the need of transmitting commands for TGV pantographs (DOTJFRA 1991b).

A more advanced train signaling system, the TVM430, has been developed for the TGV Nord (DOT/FRA 1991b, DOT/FRA 1993a, Guilloux 1992, Guilleux, 1992). This system utilizes microprocessor interlocking and digital track-to-train communications both through the rail and with intermittent transponders. The greatly increased data transmission capacity allows for more precise monitoring of speed and location of the train, and, therefore, shorter headways.†† The stepped speeds used on the TGV Southeast and Atlantique for individual blocks can be modified, and speed reduction within a block is more precisely monitored via a continuous speed curve than via step functions.

A future cab signaling system, called ASTREE, is being developed by the French National Railways (SNCF). The ASTREE system is a highly automated train control system anticipated to be installed in TGV trains before the year 2000. It equips every train with Doppler radar to update position via accurate speed determination along the track. It does not depend upon the standard block signaling and interlock policies, but incorporates a "moving bubble" for separation between trains and the interlock determined by continuous communication between trains and dispatching centers. However, it should be noted that the system implementation details and the resultant human factor implications are not known at this time. The same information, of course, could be provided by GPS (if GPS could always be counted on to be available).

2.4.1.6 Cab Signaling System: Information from Train to Wayside

Safety-related information sent from the ICE train to the wayside includes train identification and location confirmation (and correction if necessary), data about the train's braking capabilities, and details such as train number and train length. As mentioned before, the locomotive engineer inputs any changes in the braking capability of the train into the on-board control unit, which then transmits the updated information to the wayside control elements for maintenance purposes. Information that is not subject to change is transmitted only when the train enters a new central control area (DOT/FRA 1991a).

In comparison, the TGV is not equipped with similar data transmission capability. However, SNCF plans to provide the ability to pass the monitored information to the wayside via a radio-based data link to enhance maintenance planning and access consist status at the dispatching center (DOT/FRA 1991b).

---

† 'The roof equipment on the TGV Atlantique includes two pantographs, one for 1.5 kV dc and the other for 25 kV ac. Except for the Tours bypass used in mixed traffic, all high-speed lines in France are electrified with 25 kV ac." (DOT/FRA 1991b, p. 11)

†† TMV430 offers 3 minutes headway at 320 km/h (198 mph) on TGV Nord. TVM300 offers 4 minutes headway at 300 km/h (186 mph).

2.4.1.7 Wayside Signals

On ICE lines, wayside signals are generally omitted because all the necessary information for safe train operation is transmitted via the cab signaling system. However, wayside signals are installed at interlockings and stations for emergency use or for use by other trains that are not equipped with a cab signaling system (DOTIFRA 1991a). On TGV high-speed dedicated lines, wayside signals are not provided (DOTIFRA 1991b). However, TGVs are operated at speeds of up to 220 km/h on some SNCF lines that contain only wayside signals.

2.4.1.8 Displays on Locomotive Engineer's Console

There are various types of speed displays on the TGV Atlantique locomotive engineer's console. The permitted speed (or the target speed at the next marker, if a speed reduction is required) is digitally displayed in the cab (DOTIFRA 1993a). Display color and shape coding for the permitted speed has also been used to convey certain speed commands (DOTIFRA 1993a). The speed of the train is displayed by a linear analog needle. The cruise control speed set by the locomotive engineer is displayed by a rotary analog display (DOTIFRA 1991b). In addition, the locomotive engineer's computer display screen can display the current speed of the train via a bar graph. If the "control" speed is exceeded, an automatic brake application, controlled by an ATP system, is made. The "control" speed is 15 km/h (10 mph) above the maximum speed allowed in the block (for speeds between 160 and 300 km/h, between 100 and 187 mph) (DOTIFRA 1991b).

For the ICE, braking and control system information is available to the locomotive engineer and in some cases is relayed wayside via data radio links for maintenance purposes. Various passenger comfort systems such as lights and air conditioning can also be monitored and controlled remotely (DOTIFRA 1991a).

2.4.1.9 Maintenance Monitoring System

Besides scheduled maintenance and inspection, pre-run and ***en route*** inspection reflect different automation levels between the TGV Atlantique and the ICE. Both trains have continuous performance monitoring of critical components through the train diagnostic and reporting system. However, the ICE goes a step further in that any failures are communicated to the Hamburg maintenance facility ***en route*** so that they can be repaired expediently before the train is dispatched on its next trip. This is managed by its consist maintenance monitoring system.

In contrast, the TGV Atlantique does not have the instantaneous failure report to maintenance centers. However, in the future, SNCF plans to provide the ability to pass this information to the wayside via a radio-based data link to enhance maintenance planning at the central control facility (DOTIFRA 1991b).

In addition, both TGV and ICE trains are cycled through a self-test procedure prior to being dispatched, increasing the likelihood of the train completing its scheduled run (DOTIFRA 1991a).

2.4.1.10 Alerter System

Both the ICE and the TGV are equipped with an alerter system (also called *deadman* control) that monitors the locomotive engineer's vigilance. On the ICE, the alerter system will initiate a controlled service braking procedure of the train anytime the locomotive engineer fails to touch the foot pedal or hand reset for more than 24 seconds. At that time, an alarm sounds and flashes, and the locomotive engineer has 5 seconds to respond. If no response is made within this period, controlled emergency braking is automatically initiated by the ATP system (DOTJFRA 1991a). If this system fails, the presence of a conductor is required for the locomotive engineer to resume service operation (Sussman 1993).

In comparison, the TGV alertness measuring system requires the locomotive engineer to make a foot pedal movement greater than some threshold within each successive period of about one minute. If the locomotive engineer fails to do this, he or she has 2.5 seconds after a warning signal to depress a console push button or make contact with electrodes on the speed control. If the locomotive engineer does not respond, the emergency brakes are applied and he or she cannot recover control of speed until the train has fully stopped (DOTJFRA 1991b).

2.4.1.11 Emergency Train Control by Passengers

Neither TGV Atlantique nor the ICE has an emergency brake valve for passengers to operate. System designers felt that such a brake valve may not be the safest solution to the problem, and that the risk of trains being uncontrollably stopped in tunnels or other potentially unsafe areas outweighed the advantages of such an ability. Instead, the emergency control devices (handles or buttons) located in the cars can be used by passengers to alert the locomotive engineer and crew immediately about the location of the emergency. The operating procedure is for the crew to ascertain the problem and develop the best response (DOTJFRA 1991a, DOTJFRA 1991b).

2.4.1.12 Locomotive Engineer Selection and Training

Operators for both the TGV and the ICE are drawn from the ranks of the most experienced engineers on SNCF and DB. For the ICE, in-depth technical knowledge of the ICE power unit is required of all locomotive engineers. The locomotive engineer must qualify on all levels of locomotive operation before operating an ICE and, until recently, he or she had to be a qualified electrical or mechanical technician. The focus is on learning the equipment, particularly the function of power units. Engineers are qualified by equipment rather than route. In comparison, for the TGV, locomotive engineers are selected through quantitative measurement of psychomotor or cognitive aptitudes and on estimates of personality and "sociability" developed through objective scaling techniques (Macaire 1991, 1992a, 1992b, Fayada 1992, Federici 1992, Pourdieu 1992).

The following three types of training facilities exist:

1. A "cutaway" of real equipment which is used for training the locomotive engineer on the dynamic characteristics of some system (e.g., a mechanical or electrical response as a result of a control input);

2. Simulations on desk-top personal computers to train the locomotive engineer on the required responses, (e.g., to in-cab and external signals). Computer graphics have been used to provide symbolic representations of the real tasks;

3. Sophisticated moving-base simulators with computer generated "out-of-the-window" views. The graphics simulation provides high-fidelity representations of the real world (Sussman 1993).

We are aware of the first two forms of simulation facilities being used for training ICE locomotive engineers, and the third for TGV locomotive engineers. All three of the training techniques are appropriate for different aspects of training.

Shinkansen locomotive engineers are selected and trained by the regional companies in Japan. They are required to take government license exams. East Japan Rail's (in the Tokyo area) 10,000 operating staff receive a two-day refresher course every two years. Training for new locomotive engineers is six months in duration, including time in an elaborate simulator.

SNCF, in particular, seemed aware of human factors considerations. It has an ergonomics staff of approximately one hundred persons and offers regular ergonomics courses to operating personnel to enhance their awareness of safety and human factors.

2.4.1.13 Dispatching Centers

The definition of roles of dispatchers and automation in the dispatching centers is similar for the TGV and the ICE. Dispatching on each TGV line is controlled from separate central locations. Routing of TGV trains is computer-supported with manual override capability by the dispatcher. Routing is normally predetermined.

These centralized control centers can control the electric power for the high-speed lines and can cut power at any point on the catenary at any time by de-energizing the power section in which the point is located. They also monitor hot bearing detectors for bearing temperature history and rate of rise in addition to absolute temperature.

ICE train operations are monitored from a central control point, but regularly scheduled traffic is handled automatically at a decentralized level. The central traffic control intervenes only when disturbances occur (DOT/FRA 1991a).

The Shinkansen dispatching center, unlike those of the TGV and the ICE, can stop the train in an emergency by braking, though all three can cut power from the dispatching center. The locomotive engineer cannot override the dispatcher's actions. All three systems are also equipped with ATP systems that automatically stop the train if the speed limit is not obeyed. If the dispatching center equipment has failed totally or in a way that requires dispatchers to leave the premises (e.g., fire), there are backup control boards for monitoring and emergency action. Dispatching center personnel are not licensed as the locomotive engineers are. In Japan, Shinkansen dispatchers are superior in technical training and general qualifications to those for non-Shinkansen dispatching centers.

2.4.2 Maglev

The German TR07 Maglev test facility in Emsland reveals striking structural differences between magnetically levitated trains and conventional trains in track, trainset, and right-of-way facilities. All of the track is elevated, and while this need not be so, maglev track is thought by many to be more dangerous and vulnerable than conventional track and would have to be protected in any case. TR07 signaling is in-cab. With regard to the cab design and driving policies, DB staff commented to us that they are using the same philosophy with respect to human-machine interactions as prevails on the ICE.

2.4.3 Brief Summary

A common philosophy, especially of the TGV and the Shinkansen, seems to be:

1. A locomotive engineer must be in the cab;

2. It is preferred for the locomotive engineer to drive the train with assistance of and monitoring by automatic train protection systems.

The roles of the locomotive engineer and levels of automation on high-speed trains differ between the TGV and the ICE, depending on the basic system features of the train. The regenerative braking capability on the ICE encourages the frequent use of cruise control and frees the engineer from manual control to perform system management and diagnostic duties. This tends to keep the focus of the engineer inside the cab. The function allocation design for ICE operation (which provides fully automatic and cruise control as well as fully manual control, but also imposes new diagnostic tasks) tends to increase the locomotive engineer's "head down time." This parallels what has occurred in aviation, namely that more complex displays impose more "head down time" than before.

The resistive dynamic braking system on the TGV Atlantique, on the other hand, discourages the frequent use of cruise control due to its economical inefficiency, and leads to a different mode of manual coasting according to written coasting instructions. Cab displays are less sophisticated than those on the ICE. The function allocation design for the TGV (which provides less automation than the ICE) requires the locomotive engineer's active involvement in speed control.

A well experienced TGV locomotive engineer, in answering an interview question regarding whether driving has become more difficult and more complex, said "Yes and no. There are more safeguards for traffic and for passengers, but it is still the driver who controls and monitors them, and since there are more of these, you need a greater amount of attention." (The French Railway Review, 1992) Therefore, it is important that function allocation and driver-aiding technology be designed to be user-friendly and not pose excessive demand for driver "head down time."

3. FUNCTION ANALYSIS AND ACCIDENT SCENARIOS

3.1 FUNCTION ANALYSIS

3.1.1 Function Analysis in Practice

The purpose of a function analysis is to identify or define the functions a system must perform to meet its objectives. This analysis, in turn, may be used to identify which functions should be automated and which should be performed by humans, which are likely to be easy and which are likely to be difficult. It can serve as a basis for writing procedures and designing displays, controls, and workplaces for the humans in a system.

Typically, function analysis is presented as a hierarchy from high level functions to lower level sub-functions (sometimes called tasks), and so on down to however many levels seem appropriate. It is done by inference, considering whatever information sources are relevant; there is not (and cannot be) an algorithm for performing function analysis. The function analysis for high-speed train operation is shown in the functional flow diagrams throughout the remainder of this section.

Different viewpoints on function analysis abound. According to (Sanders and McCormick 1987), function analysis initially should be concerned with what functions need to be performed to fulfill the objectives, and not with the way in which the functions are to be performed (such as whether they are to be performed by humans or machines). We generally subscribe to these views. At the same time, it must be noted that whenever a subgoal is specified as a path to a greater goal, that is tantamount to specifying a way to the goal, and the finer the breakdown the more it looks like specification of a way (or how). In any case, the what should be sought as much as possible initially.

3.1.2 Functional Flow Diagrams

The function analysis for a HSGGT system is performed via hierarchical functional flow diagrams. A given function is decomposed into several functions (or task steps) of approximately the same importance or relevance, and each of these sub-functions is further decomposed into several functions or steps. The ordering of these hierarchical units can be thought of as a tree structure, with each branch having one or more sub-branches emanating from it.

A function can be thought of as a task unit, which is comprised of a collection of activities that occur with some notion of order (i.e., certain activities may be required to take place before others). In addition, a function may require input information for the successful completion of the task, and may provide new output information at the completion of the task.

The functional flow diagrams shown in this section (Figures 3-2 to 3-19) employ a standardized legend (shown in Figure 3-1) which is intended to indicate the hierarchical ordering throughout the series of diagrams. For example, a rectangular box indicates a function which is performed by

either a human or a machine, with no further task decomposition provided. The heavy framed variant of the function block indicates that the function is decomposed further into lower-level functional units, and this lower-level functional decomposition is shown in a separate diagram. To indicate the reverse direction in the hierarchical ordering, the function boxes shown with dotted edges are referencing a function which is at the same or higher level in the hierarchy. A function box with a shaded interior indicates that the function to be performed involves complex decision-making.

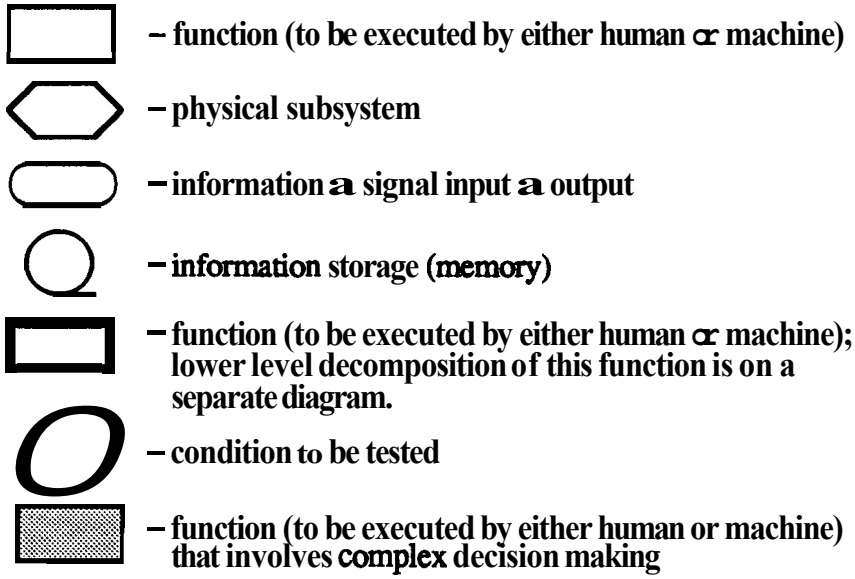


Figure 3-1. Legend for Functional Flow Diagrams

Other legend shapes include a stretched hexagon to represent a physical subsystem, a rounded rectangle to represent an informational input or output (signal), and a circle with a tail to represent some form of information storage (memory). In addition, standard signal flow elements are used to show signal and decision flow, such as the use of the tilted square for indicating a conditional decision.

Each of the function flow diagrams has a header at the top that includes a number and a title of that figure. The number in the header represents its position in the hierarchy. The title in the header corresponds with the label in its function box in the next higher level. For example, the diagram with the header "1.3.6 Manual Control" in Figure 3-8 represents a sub-branch in the locomotive engineer operation branch, which can be found as a single function element in the diagram "1.3 Speed Control" in Figure 3-7. This scheme allows rapid orientation within the hierarchy from any diagram in the function analysis.

The overall operation of a HSGGT system is divided into two broad functional classes: vehicle control and centralized control. Vehicle control is defined as the operation and control of a vehicle from within the vehicle, and represents the operational function that is performed by either a person or an automatic machine, depending on the particular function allocation design.

Throughout this document, the person carrying out these tasks is referred to as the locomotive engineer of the vehicle. In the functional flow diagrams, the functions associated with the vehicle control are under the hierarchical branch number 1, labeled "Function Analysis for Vehicle Control" as shown in Figure **3-2.**

Centralized control is defined as the operation and control of the system elements which are fixed to the wayside. These elements, which are controlled during system operation, include track switches and signals. In addition, centralized control can be interpreted to include higher-level management functions such as train scheduling, route planning, and consist planning. The personnel typically involved with this broad range of activities include dispatch operators, dispatch managers, and scheduling managers. This set of activities could logically be termed "environment control," as it involves control of those elements that represent the environment of the vehicles. It could also be termed "wayside control" for the same reasons. For the purposes of the function analysis, we will refer to this functionality as dispatch control, and it will include only those functions that are actively controlled throughout system operation. As such, dispatch control will explicitly not include the functions of route or consist scheduling. The functions associated with dispatch control are under the hierarchical branch number 2, labeled "Function Analysis for Dispatch Control" as shown in Figure 3-11.

3.1.3 Function Analysis for Driving a High-Speed Train

In the following function analysis, the operation of a high-speed train is modeled as a system of event-driven control loops, **i.e.,** the various events determine the control actions. The primary control loop is identified as continuous speed control, while the secondary control loop consists of handling all other discrete events that either directly or indirectly influence the primary speed control task, including environmental factors (hills, wind, etc.). These secondary tasks are sometimes induced by abnormal situations.

In this analysis, the term ***other subsystems*** refers to any of the on-board systems which are monitored, such as traction system, braking system, air conditioning system, passenger information, etc. ***External events*** could be signal indications or speed limits from wayside, observed object on track, or anything that may directly or indirectly influence the decision associated with the desired momentary speed. ***Speed-control events*** refer to changes in the speed command data that are received from the wayside **(i.e.,** signal changes).

It is assumed that the speed control loop is in operation any time the vehicle is in motion. In other words, we assume that, at all times during the vehicle motion, there is some controlling element (human or automation) which will be charged with the task of setting the thrust and brake controls to follow some form of speed command. In addition, we also assume that there is some form of control which is continuously available to recognize and respond to some defined set of abnormal events.

To model the system as event-driven, it is assumed that there is functionality available to sense some defined set of events. Furthermore, it is assumed that there is the capability to recognize, categorize, and prioritize these events as they occur. These events will then be distributed to

either the "speed control" loop or the "other subsystem event" control loop, as appropriate. Thus, the event handler takes the form of a higher priority control loop, which is always available when required, i.e., upon the occurrence of an event. This event handler models the locomotive engineer's "situation awareness."

As shown in Figure 3-2, the overall operation of a given trainset begins with the pre-trip checkout (function 1.1). During this phase, the systems of the train are tested and verified as operating properly. Similarly, after a particular shift is complete for a locomotive engineer or vehicle, a post-trip checkout is performed (function 1.5).

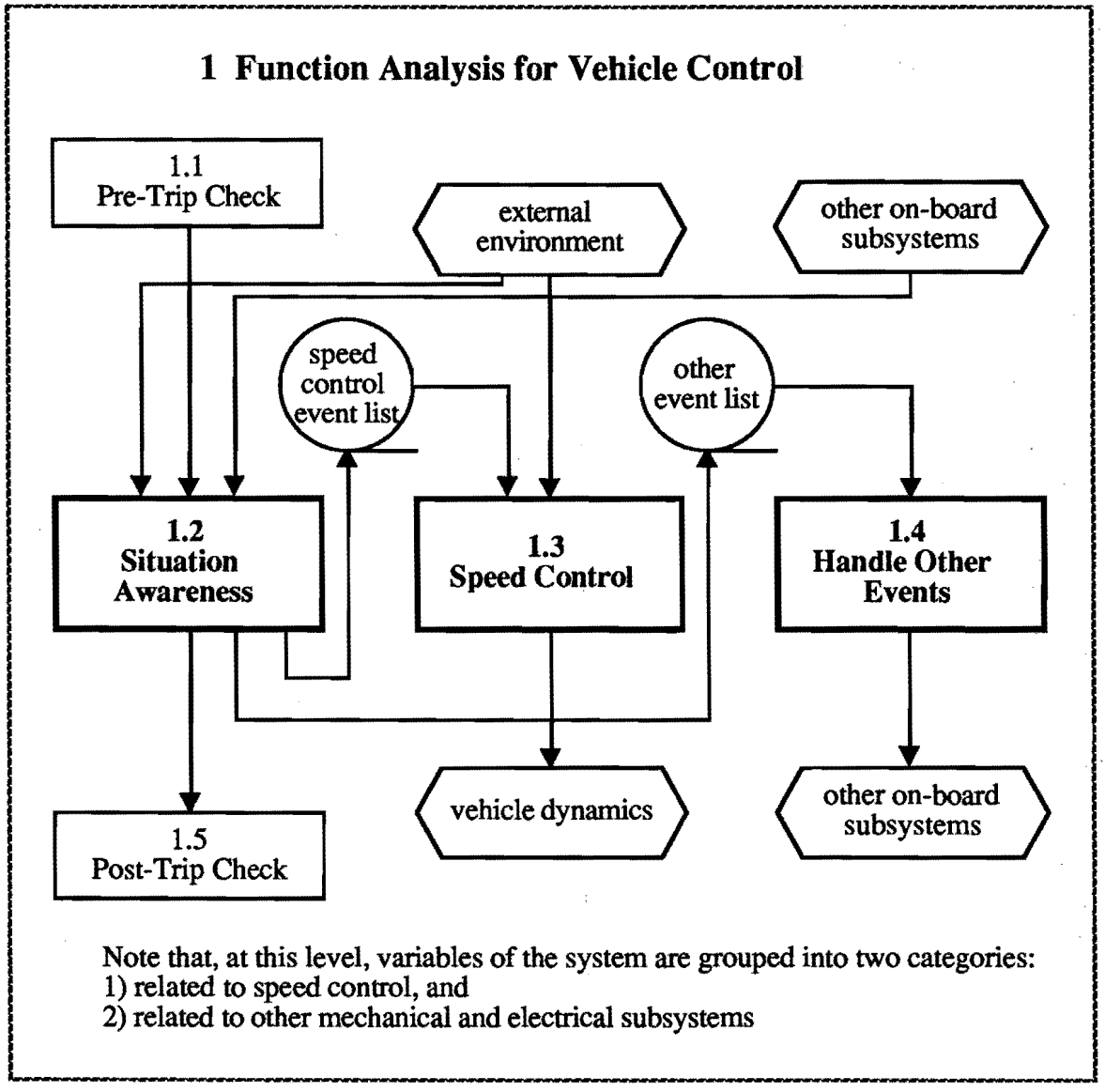
During the regular operation of the vehicle, the functional duties of the locomotive engineer are modeled as three distinct control loops which operate in parallel. As mentioned above, the "situation awareness" is the overall coordinator of the events that occur to and around the vehicle, and is shown as function 1.2 in Figure 3-2. The continuous speed control functionality is shown as function 1.3. The "other event" handler is shown as function 1.4. These three functional units operate concurrently and represent the multi-tasking nature of operating a rail vehicle. The paths between these functional elements do not represent procedural flow, but rather represent information which is transferred between the functional units. This information is transferred via "speed control events" and "other events."

A more detailed breakdown of the situation awareness function is shown in Figure 3-3. In this functional unit, all activities are focused on the sensation, prioritization, and distribution of system events. The three task units at the top (1.2.1 Check for External Events, 1.2.2 Check for Speed-Control Events, and 1.2.3 Check for Other Subsystem Events) represent the sensing functions. These are grouped together, since they are not necessarily executed in any particular order. (In fact, they will sometimes be executed only when required, at other times in a pattern of sampling.) Grouping these together indicates that they have equal importance, and that they are all ready at the same time (i.e., concurrently). Any of these functions may start a sequence of task steps if an event is sensed. In that regard, these units can be considered to be asynchronous in operation.

If an event has been received by function 1.2.3 (Check for Other Subsystem Events in Figure 3-3) it is passed to function 1.2.4, which has the responsibility of diagnosing the event. This diagnosis serves to identify the source of the event (i.e., which subsystem is at fault) and the cause of the event (i.e., the fault within that subsystem). The output of the diagnosis is combined with the outputs of functions 1.2.1 (Check for External Events in Figure 3-3) and 1.2.2 (Check for Speed-Control Events in Figure 3-3), and is fed to functions 1.2.5 and 1.2.6 (Post Speed-Control Event and Post Other Subsystem Events in Figure 3-3), which serves to prioritize the incoming events in relation to the events that are already waiting in the queue to be serviced.

After the prioritization of the new event, and subsequent insertion into the event list, the entire list is reviewed. If there is an event at the top of the list which requires some modification of the speed-control strategy, it is passed to the speed-control function via the local event list. If not, the event is passed to the local event list for the "other event" handler.

Note that there are conflicting needs for the local event lists that exist between the situation awareness function and the other two control functions. The "speed control" function needs the



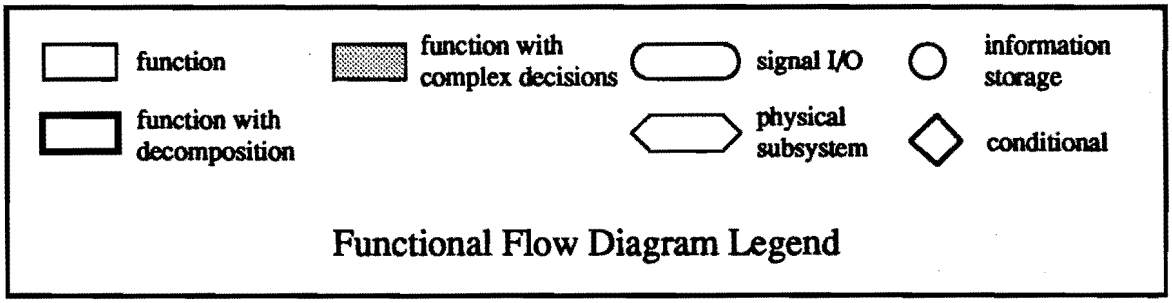


Figure 3-2. Functional Flow Diagram: Function Analysis for Vehicle Control

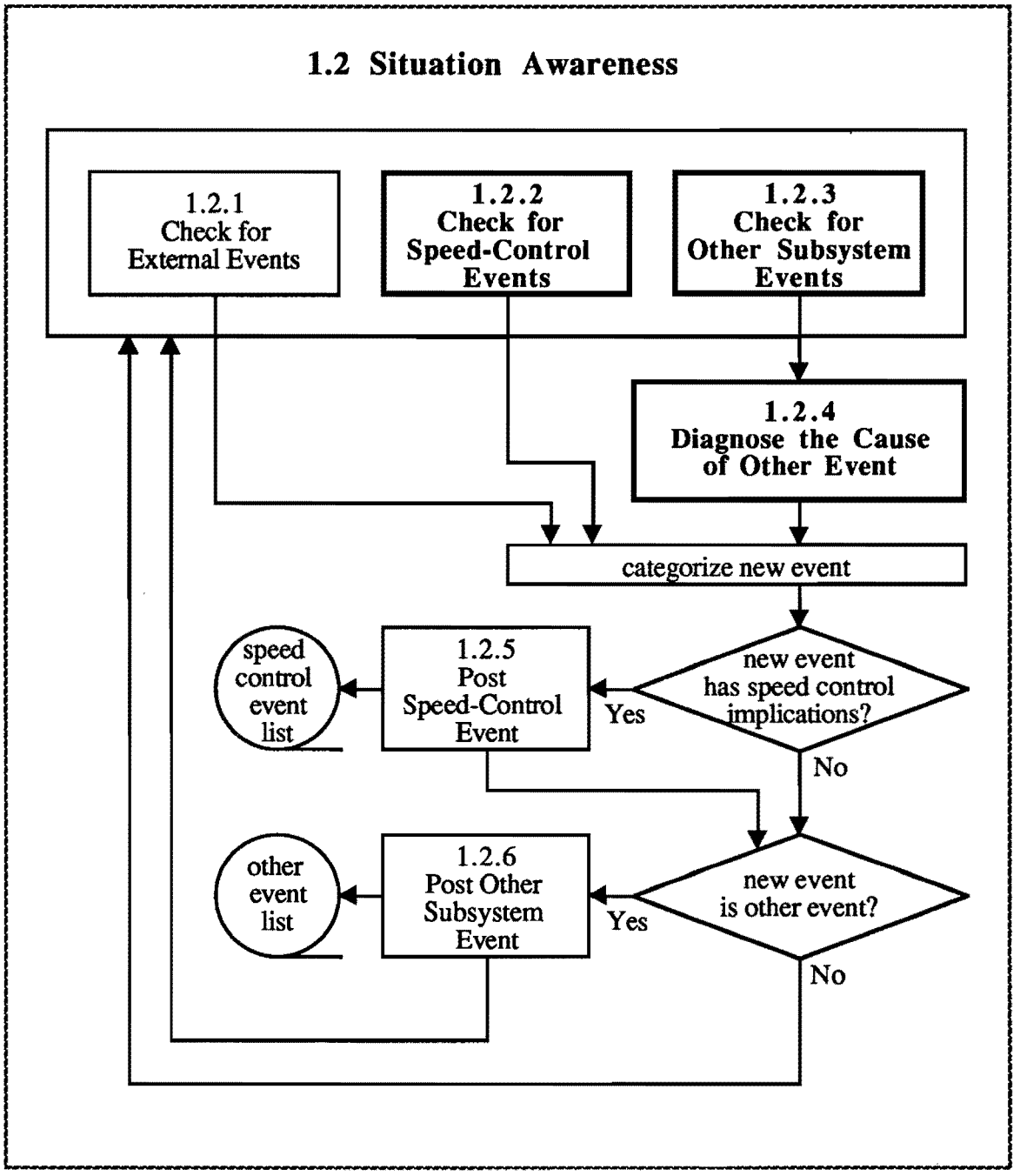


Figure 3-3. Functional Flow Diagram: Situation Awareness

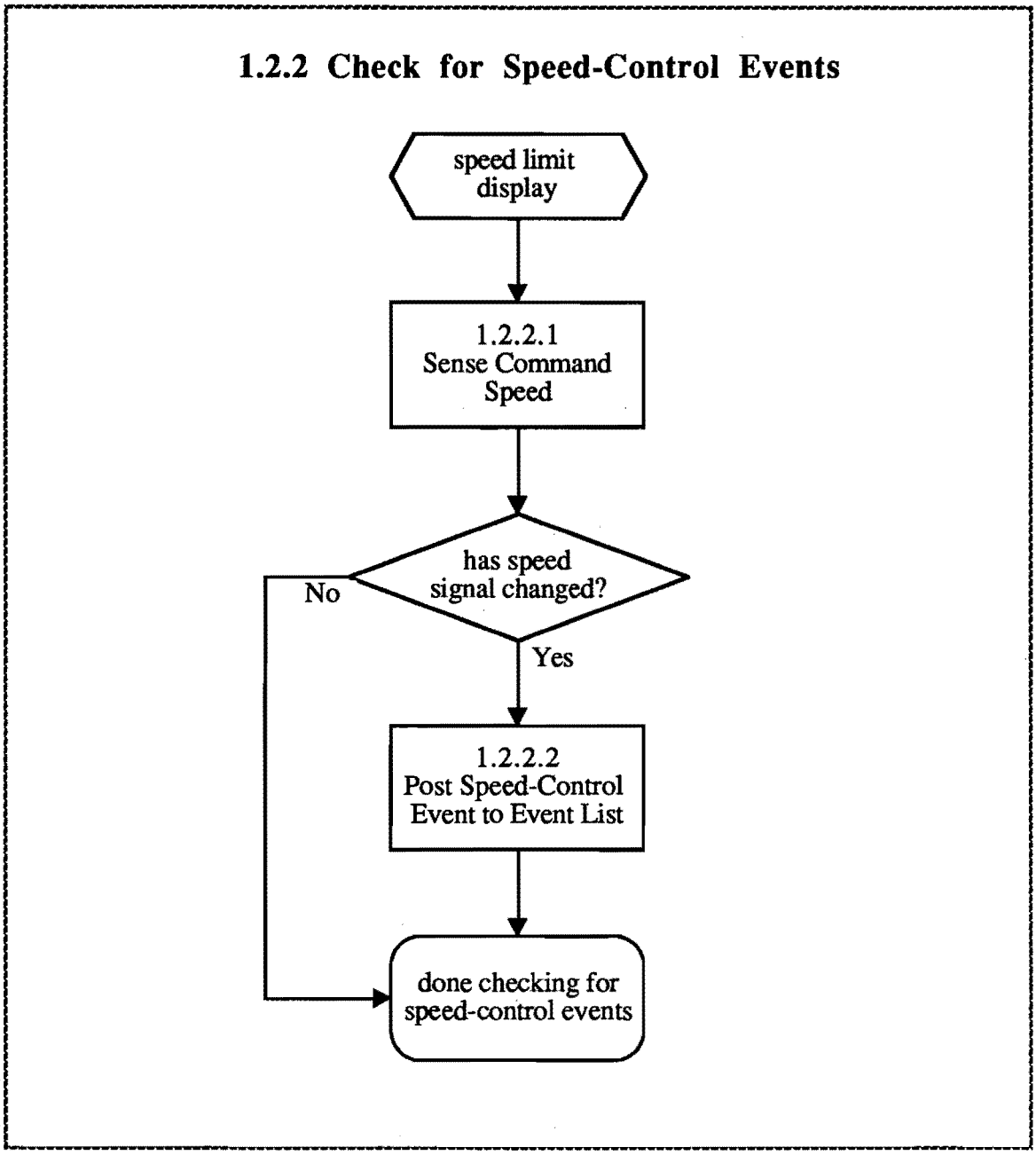
most up-to-date command speed information, so the situation awareness function will place all of the speed control-related events on this event list. However, the "other event" handler wants to handle the most important event that is presently posted. Therefore, in order to reduce the memory requirements of that particular functional module, we will model the system such that the situation awareness unit will only post one event at a time to this function — the most important event. If a new event occurs that is of higher priority than the currently enqueued event (which has not been handled yet), the situation awareness function has the capability to replace the currently enqueued event with the newer, higher priority event.

It should also be noted that this model of situation awareness retains the preemptive nature of the human function. The processing actions of interpreting and prioritizing an event happen asynchronously, and are triggered by the first sensation of that event. However, the sequence of events can be interrupted, and subsequently postponed, if an event of greater urgency occurs before the first event has been completely handled by this stage. For example, let us imagine that the locomotive engineer has noticed that a fault indicator is lit, but has not yet found the source of the fault. During the process of diagnosing the fault indication, he or she then gets notification of an obstruction on the track. In this case, the diagnosis of the fault lamp would be postponed until the obstruction had been completely handled. This preemptive nature is a key feature of the situation awareness model.

Decomposing the elements of function 1.2, let us look at Figure 3-4 (function 1.2.2, Check for Speed-Control Events), Figure 3-5 (function 1.2.3, Check for Other Subsystem Events), and Figure 3-6 (function 1.2.4, Diagnose the Cause of Other Event). Function 1.2.2 (Figure 3-4) monitors the speed limit indicator, and compares the current indication with the last known speed command. If there has been a change in the speed command, a speed control event is posted. In function 1.2.3 (Figure 3-5), state indicators for a set of on-board subsystems are monitored. Each of the subsystem indicator outputs is compared to a range of values which is considered normal for that subsystem measurement. If the indicated value is outside the bounds of acceptability, an abnormal state event message is posted. In function 1.2.4 (Figure 3-6), the incoming event is checked. If the originating subsystem is not known, the event is compared to a list of possible subsystems. Once the faulty subsystem is known, the event is compared to a list of possible faults and expected indications for that particular subsystem.

Figure 3-7 shows the decomposition of the function labeled "1.3 Speed Control." In this function, information about the external environment state, the dynamic state of the train, and the state of other subsystems on the train, along with information regarding the rules of operation, are fed into function 1.3.2. This function uses this information to determine the desired speed of the train. Function 1.3.3 previews the desired speed, and, in the following two conditional blocks, the decision is made whether to utilize cruise control (function 1.3.4), automatic control (function 1.3.5), or manual control (function 1.3.6). Each of these functions has the capability of controlling the dynamic motion of the vehicle.

Figure 3-7 also shows some of the key elements of the human-machine interface for automation in vehicle speed control. While the vehicle is in a manual control mode, the functional flow is around the large loop. The operator waits for a speed control event, which is an indication that there may be a change of speed required. When the event is received, he or she uses information



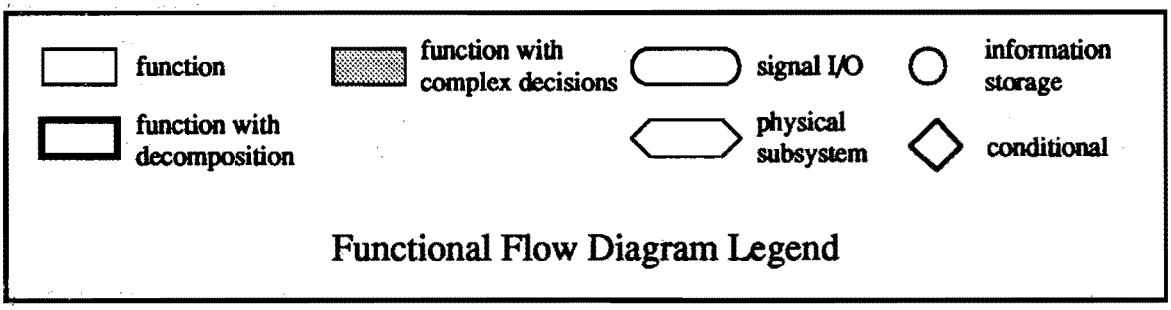
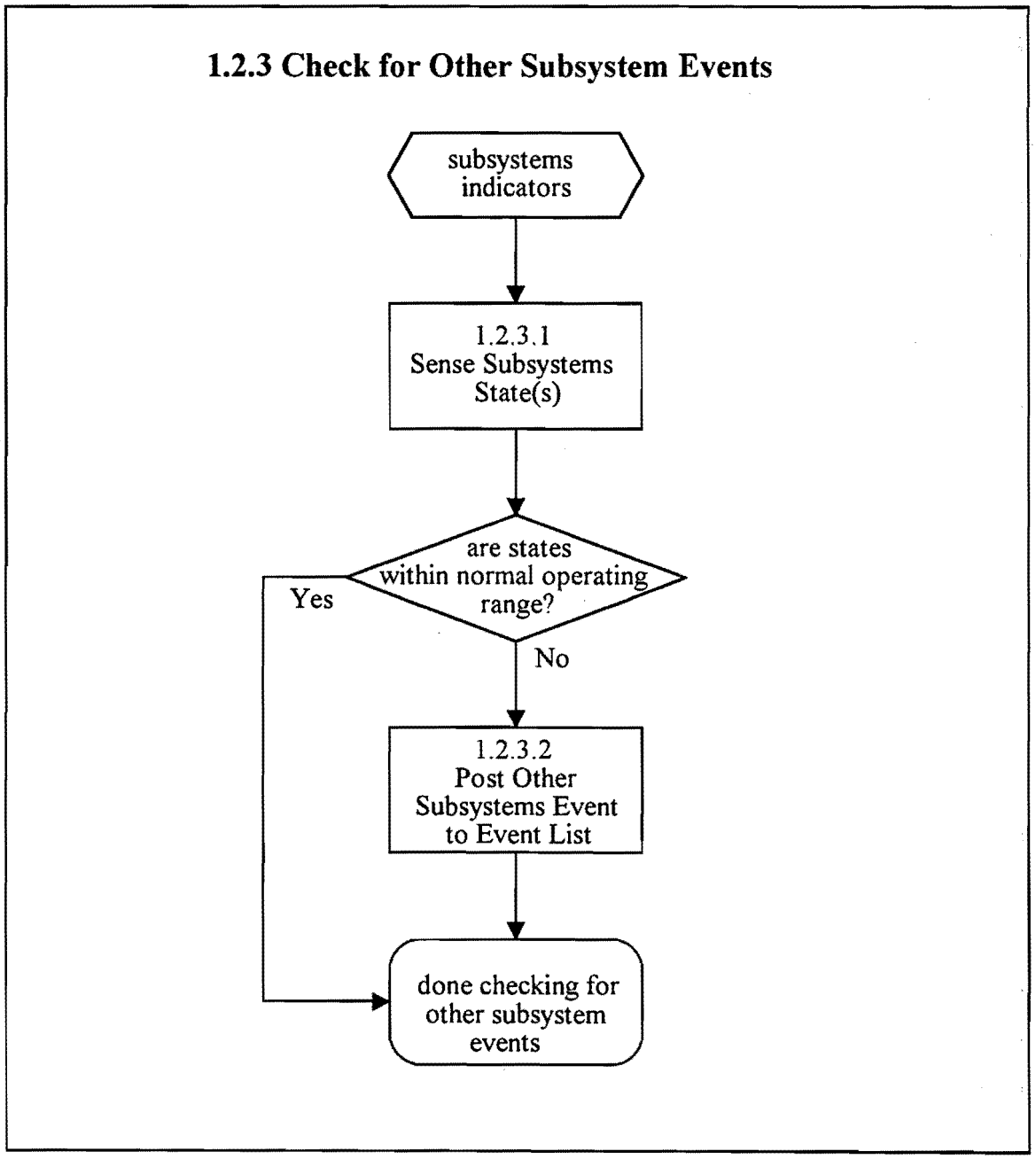


Figure 3-4. Functional Flow Diagram: Check for Speed-Control Events



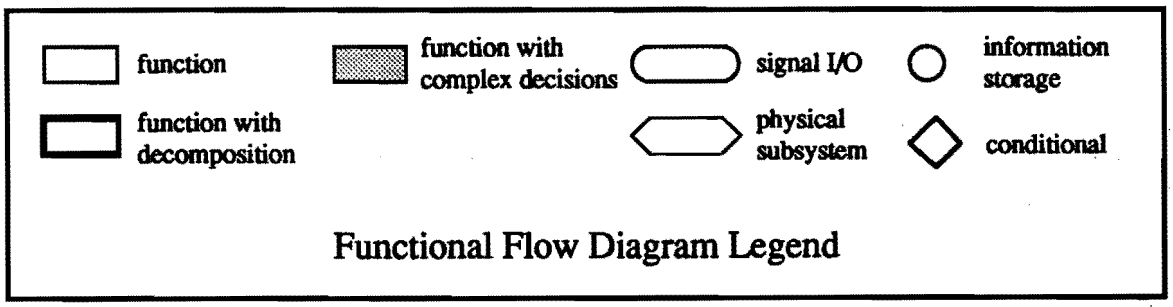


Figure 3-5. Functional Flow Diagram: Check for Other Subsystem Events

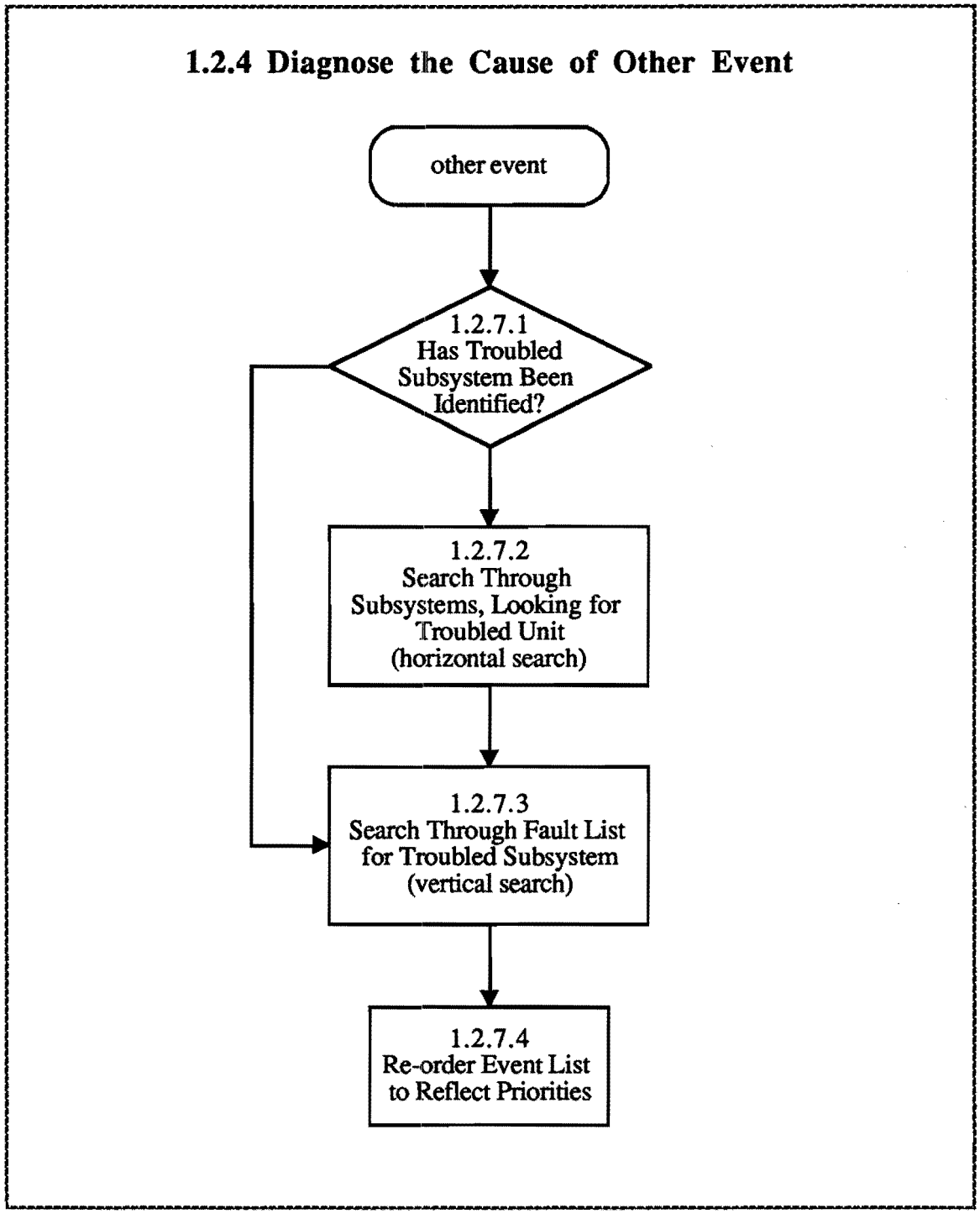


Figure 3-6. Functional Flow Diagram: Diagnose Cause of Other Event

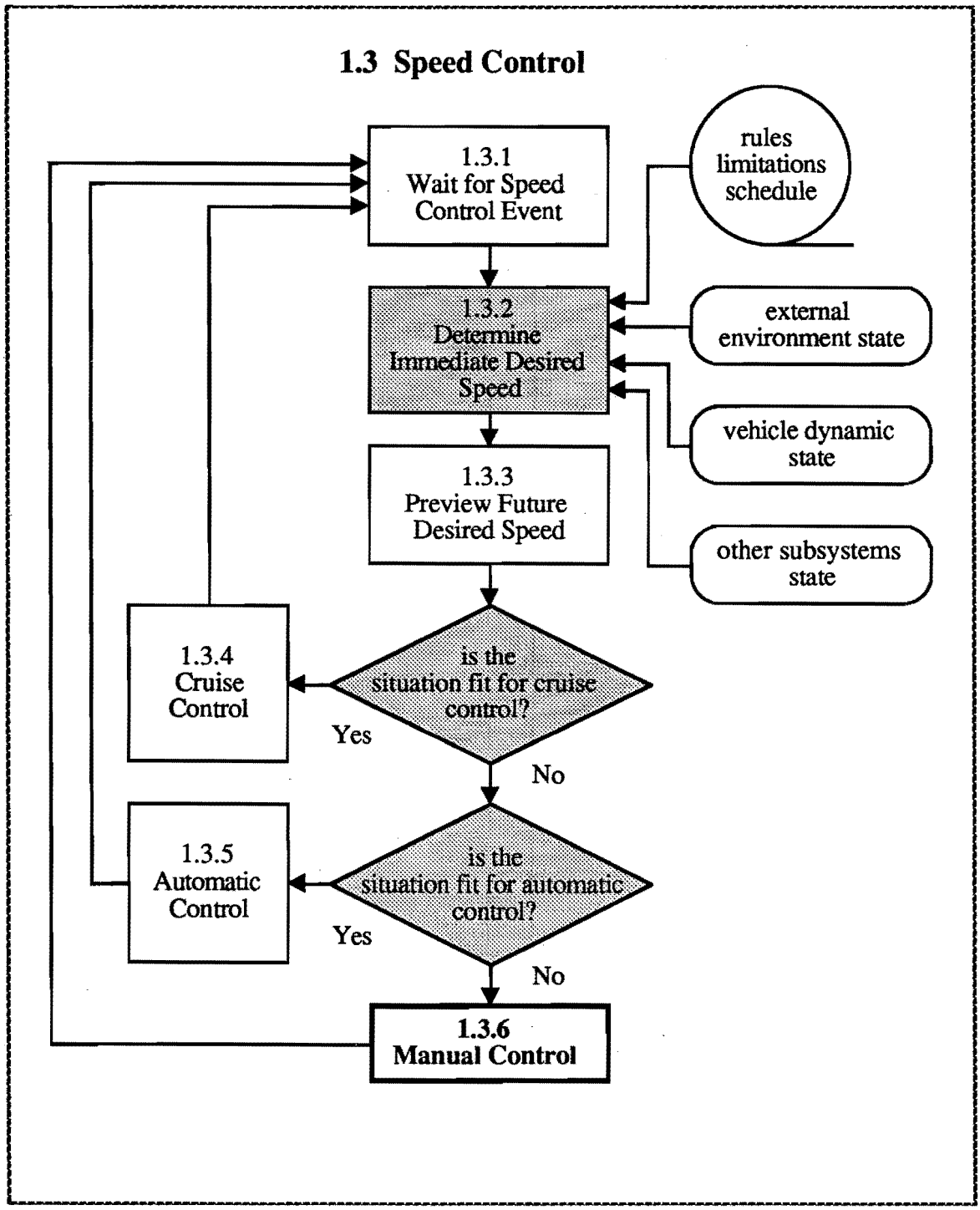


Figure 3-7. Functional Flow Diagram: Speed Control

about the train and the environment (extemal environment state, vehicle dynamic state, and the state of other subsystems), along with the operating rules and regulations, to determine the appropriate speed for the current conditions. The operator also previews the future speed control needs, to the best of his or her ability. At that point, a decision is made whether to continue with manual control or to use one of the automated modes. If a decision is made to continue in manual mode, the operator then takes the steps necessary to control the speed of the train (as shown in function 1.3.6 Manual Control). If, instead, the operator elects to start one of the automatic modes, he or she does so, but then returns to function 1.3.1 to wait for the next speed control event. At the subsequent arrival of speed control events, the operator again decides whether to remain in the automatic mode or to revert to a manual mode.

Figure 3-8 shows the decomposition of' the function labeled "1.3.6 Manual Control." In this function, the information input is the desired speed. Function 1.3.6.1 is the observation of the speed deviation of the vehicle from the desired speed. From this determination, the locomotive engineer will determine the amount of required thrust or braking (function 1.3.6.2), and will apply that thrust or braking (function 1.3.6.3).

In Figure 3-9, the decomposition of the function labeled "1.4 Handle Other Events" is shown. In this functional block, the inputs are an event, the cause of that event, and the corresponding subsystem state. Using this information, a number of criteria are applied to the event, with potential action taken if a particular condition is true. For example, if the event requires a control adjustment, the function labeled "1.4.2 Adjust Relevant Controls" is called into action. The actions listed are controls adjustment, communication with dispatcher, communication with conductor, communication with maintenance, or communication with a passenger.

3.1.4 Example

To illustrate how the function diagrams can be used to analyze a scenario, an example scenario "Object Intrusion" is analyzed as follows. Let us assume that a train is in operation, and at this point there are already two events in the event list which have occurred: "passenger ill in car 3" and "minor brake pipe leakage in car 5." We will also assume that the top event is "passenger ill in car 3" and is currently in the process of being handled. At the point in time when we enter the scenario, the on-board signaling system indicates that an object intrusion has occurred about 3 miles in front of the train's direction of travel.

As a result of this occurrence, we have a change in the external environment which is sensed by a track-obstruction-detection instrument and relayed into the cab for the locomotive engineer or the automatic controller. In the cab the awareness of this event in the cab occurs through function "1.2.1 Check External Events."

This newly found event should be queued in the "event list" by functions "1.2.5 Post Speed-Control Event" and "1.2.6 Post Other Subsystem Event." Based on the priority of this event, as listed by the relevant operation rules, the "object intrusion" event should be placed at the head of the event list. Following the functional flow diagram of function 1.2 (Figure 3-3), the next condition to be tested is "should the speed be changed due to the occurrence of this top event?'

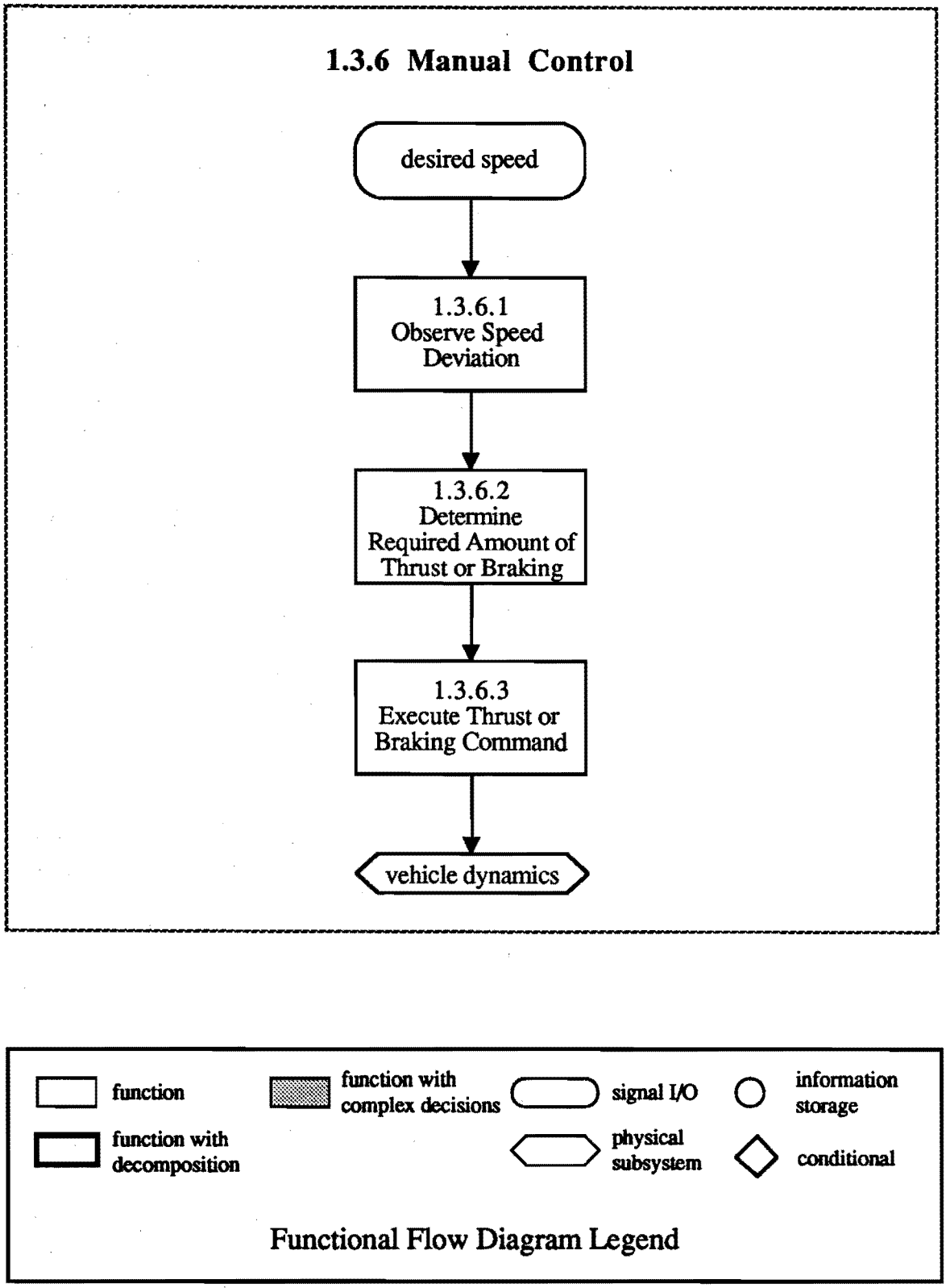


Figure 3-8. Functional Flow Diagram: Manual Control

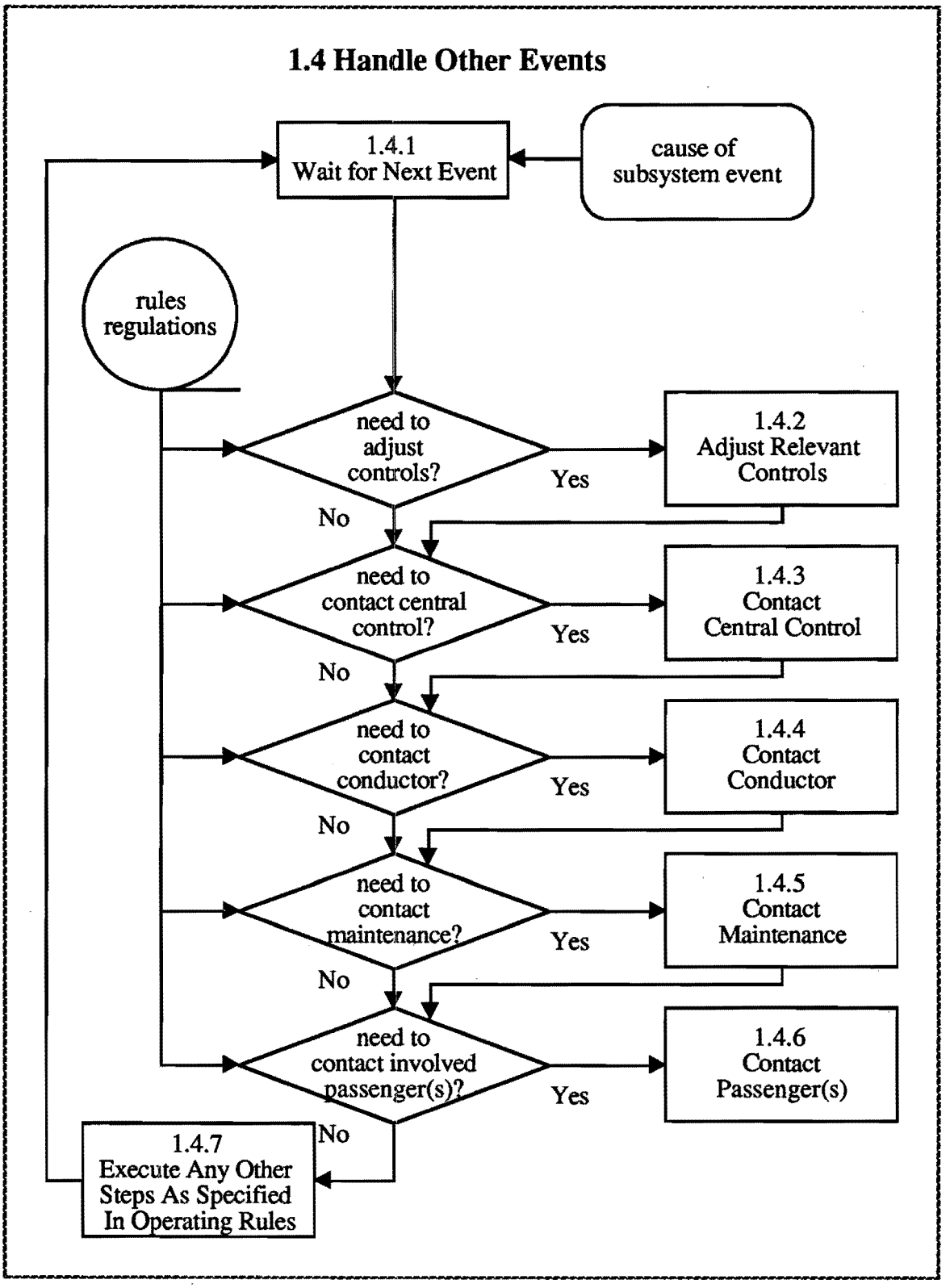


Figure 3-9. Functional Flow Diagram: Handle Other Events

For this case, the answer is "yes." The next condition to test is "does handling this speed control event involve handling other subsystem event?" The answer is "no" since this event can be handled by speed control alone. This will lead the functional flow of this scenario into the function labeled "1.3 Speed Control" (Figure 3-7).

Continuing in the flow diagram of function 1.3 (Figure 3-7), the next operation to perform is determination of the current desired speed under the new event. Based on the stored rules information, the decision will be to stop the train before reaching the obstructed location. The desired preview speed will be a speed reduction profile. The next step is a decision regarding the appropriateness of cruise control to perform the desired speed reduction. Considering that cruise control is constant-speed control, this would not be appropriate. The subsequent step is a determination of the propriety of the use of automatic control. Depending on the level of automation available in the train, the answer could be "yes" or "no."

If automatic control is not appropriate, the locomotive engineer controls the speed of the train according to the flow diagram of function 1.3.6 Manual Control (Figure 3-8). The locomotive engineer needs to closely monitor the current speed of the train and "calculate" its deviation from the desired speed and the braking amount needed. As the braking is applied, the train slows down. This change in the vehicle dynamics, in turn, influences the "External Environment," i.e., the distance (and rate of change) between the train and the object.

Then the whole cycle of awareness, decision making, and speed control and/or event handling repeats. When the cycle repeats, other events may develop (e.g., on-board air-conditioning system breaks down). These events are placed in the event list with the appropriate priority. In the case of handling an object intrusion condition, many events will have a lower priority than collision avoidance. Therefore, the next cycle of speed control decision is similar to what is described above. One cycle of this "object intrusion" event handling is illustrated in Figure 3-10.

3.1.5 Function Analysis for Dispatching Center

Figures 3.11 through 3.19 comprise the function analysis for the task of environment control. This task is typically performed by one or more dispatchers. Environment control is defined as all control actions that affect the system environment in which the HSGGT vehicle operates. This includes the track, switches, signals, and any other related components.

Prior to the advent of centralized control and command systems, this function had been performed by personnel located in dispatch towers distributed throughout the system. Since the implementation of centralized control stations, most (if not all) of this function is carried out by a group of people operating from a central location. In this type of operation, any remaining tower operators in the system operate at a level below the dispatcher. This means that centralized controllers use the tower operators as system sensors for situation awareness data. In addition, the controllers provide directives to the tower operators, based on the current knowledge of the system state. Eventually, it is expected that there will be no tower operators. The tasks carried out by the tower operators are not included as a separate entity in this function analysis.

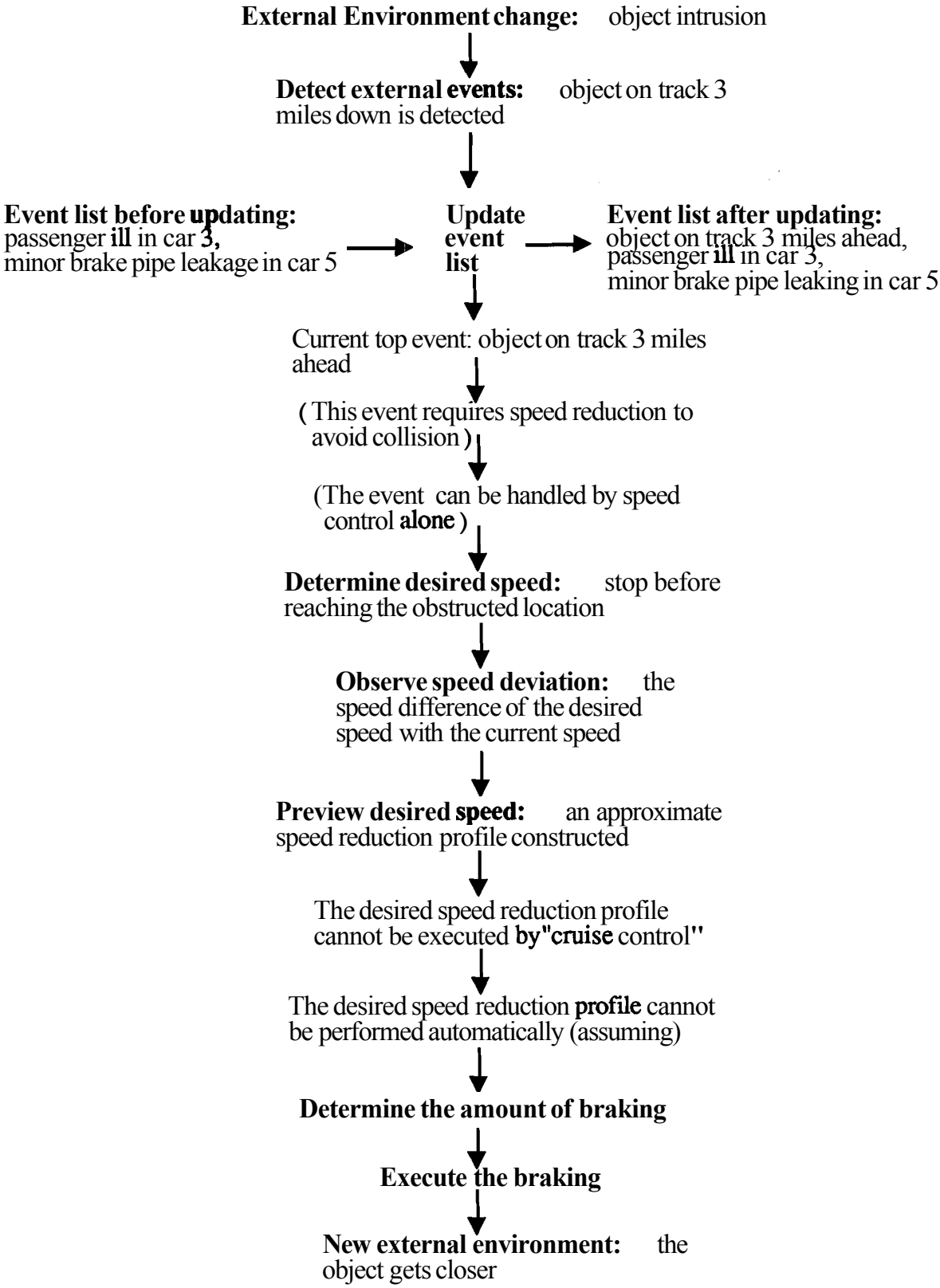


Figure 3-10. **Example of Chronological Event Flow (From Ex. of Section** 3.1.4)

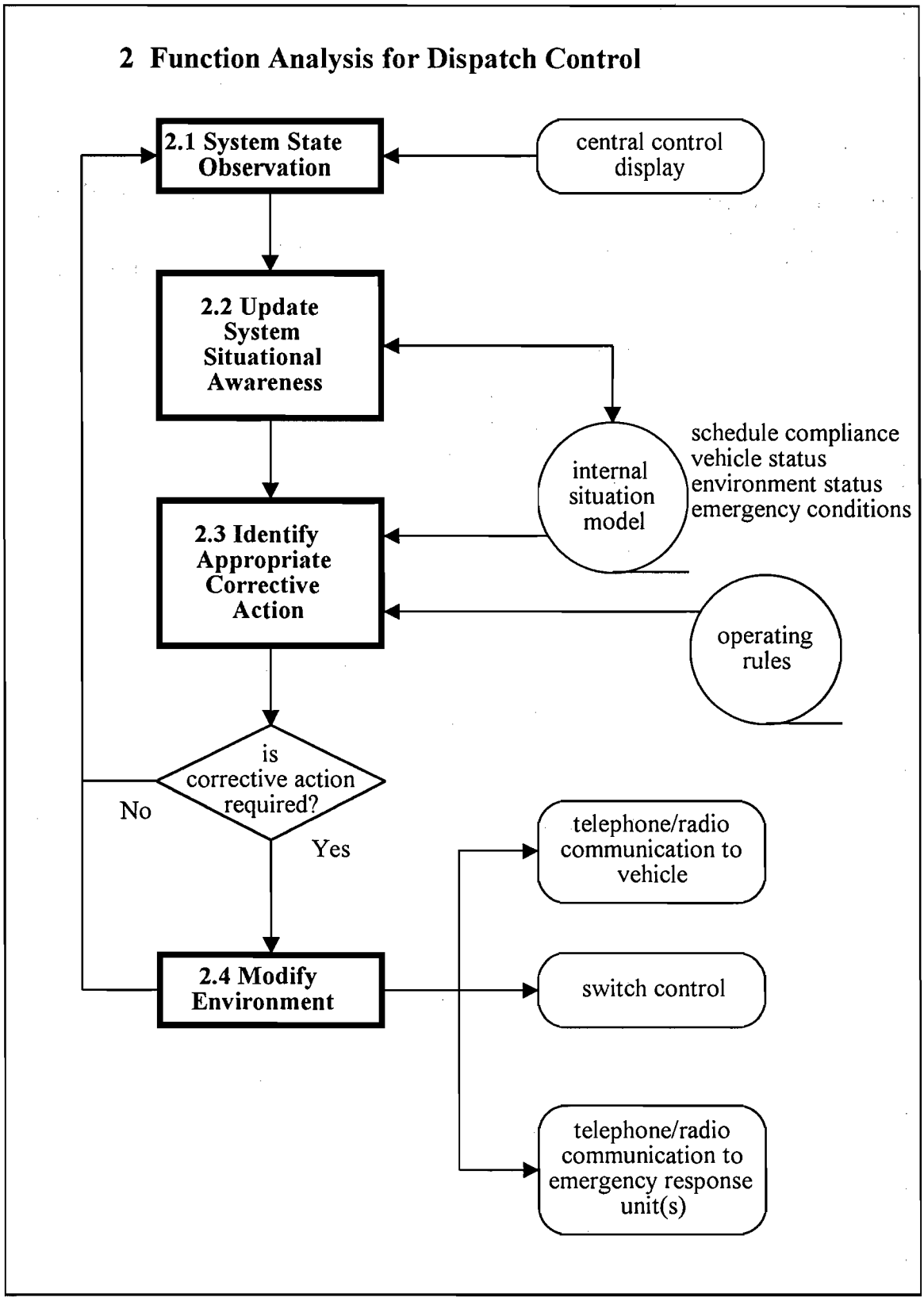


Figure 3-11. Functional Flow Diagram: Dispatch Control, Top Level

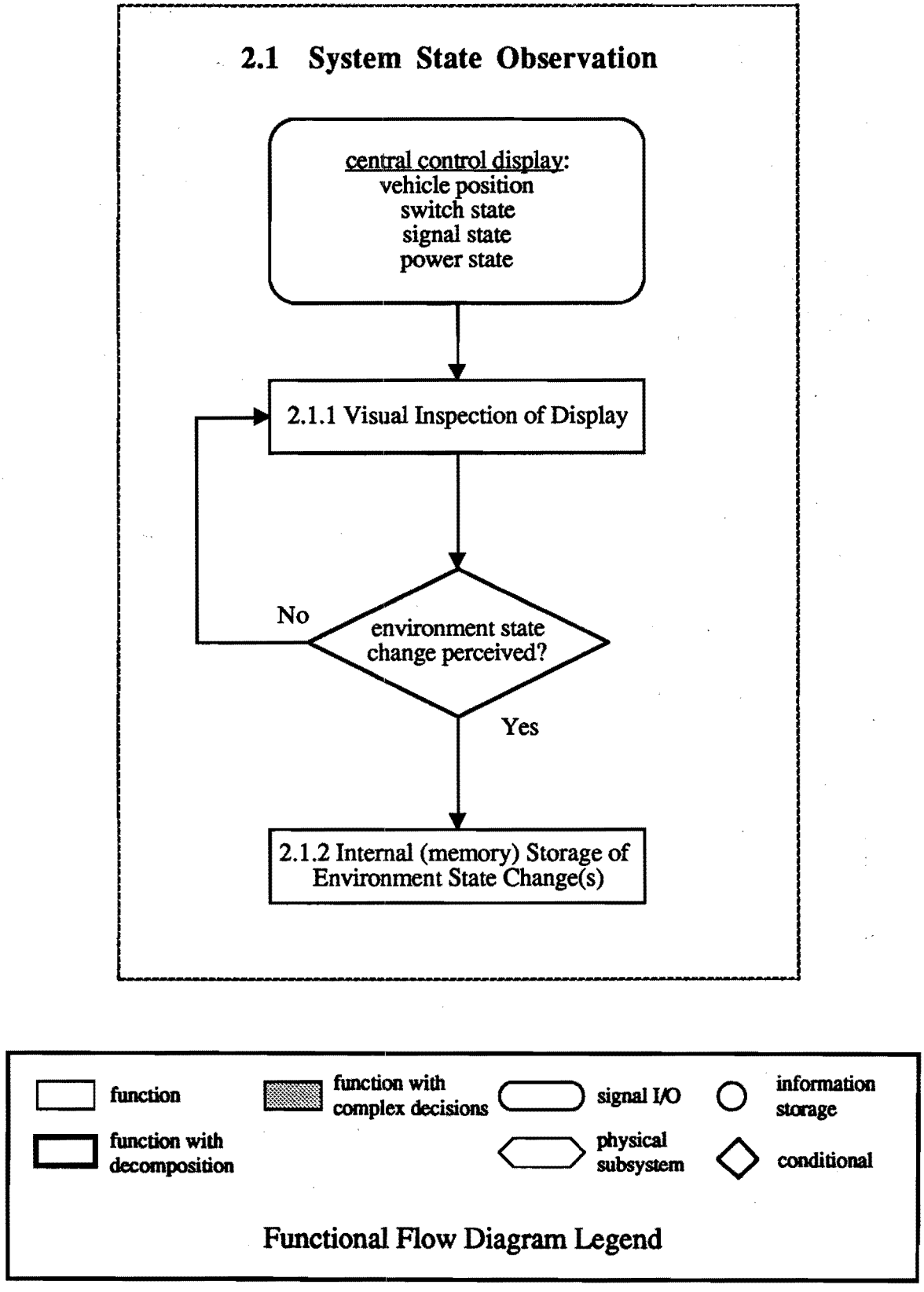


Figure 3-12. Functional Flow Diagram: System State Observation

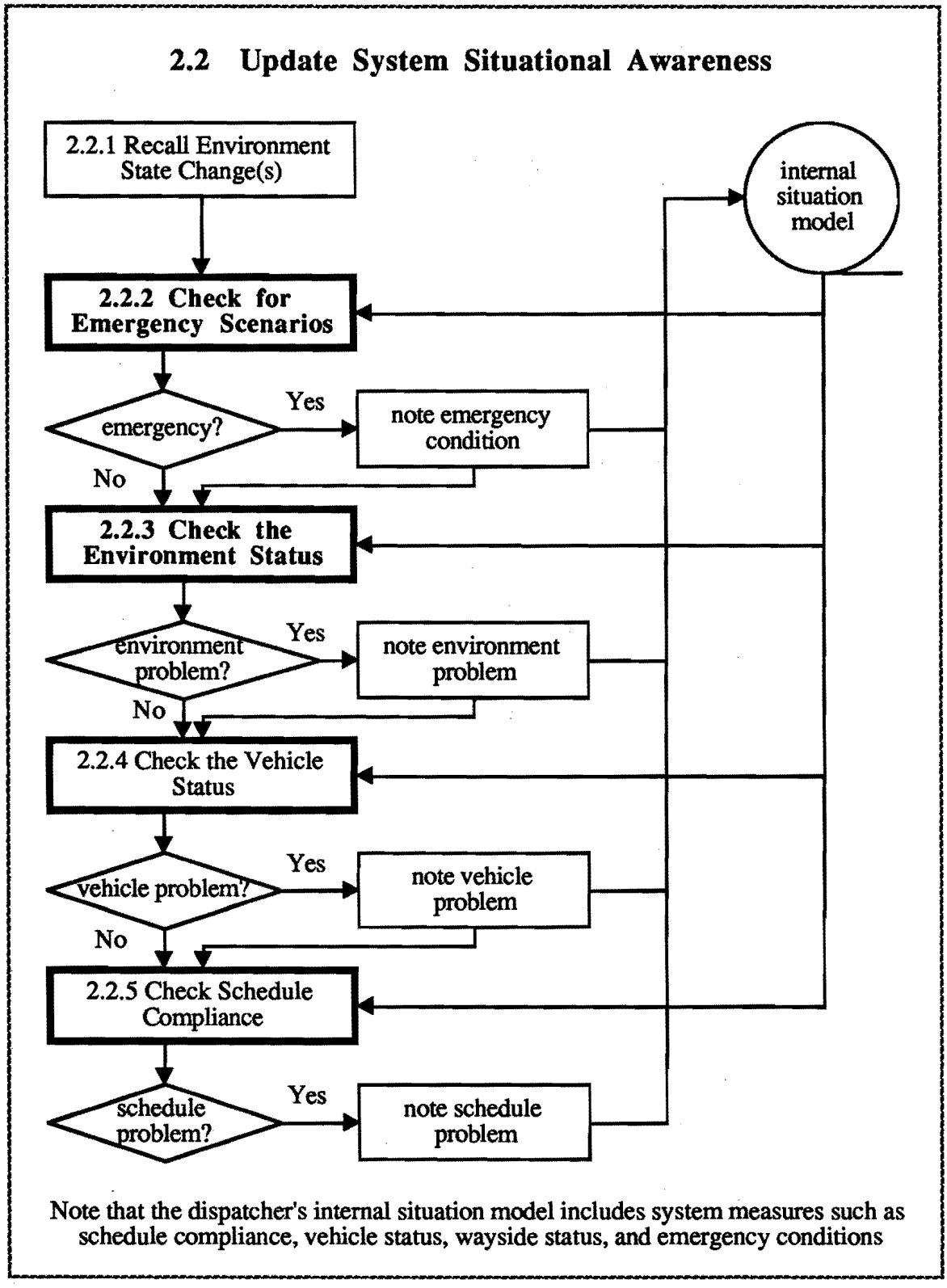


Figure 3-13. Functional Flow Diagram: Dispatch Situation Awareness

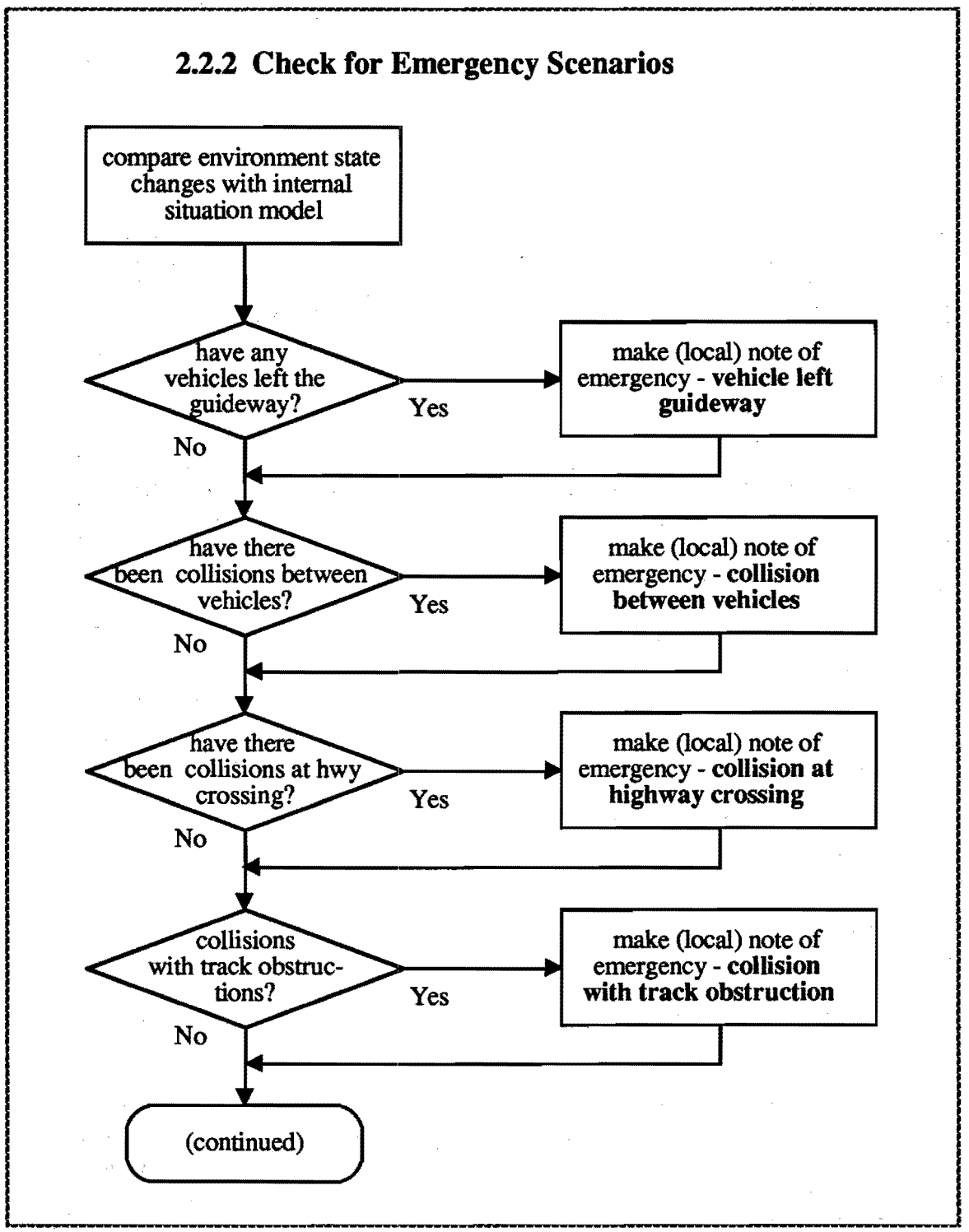
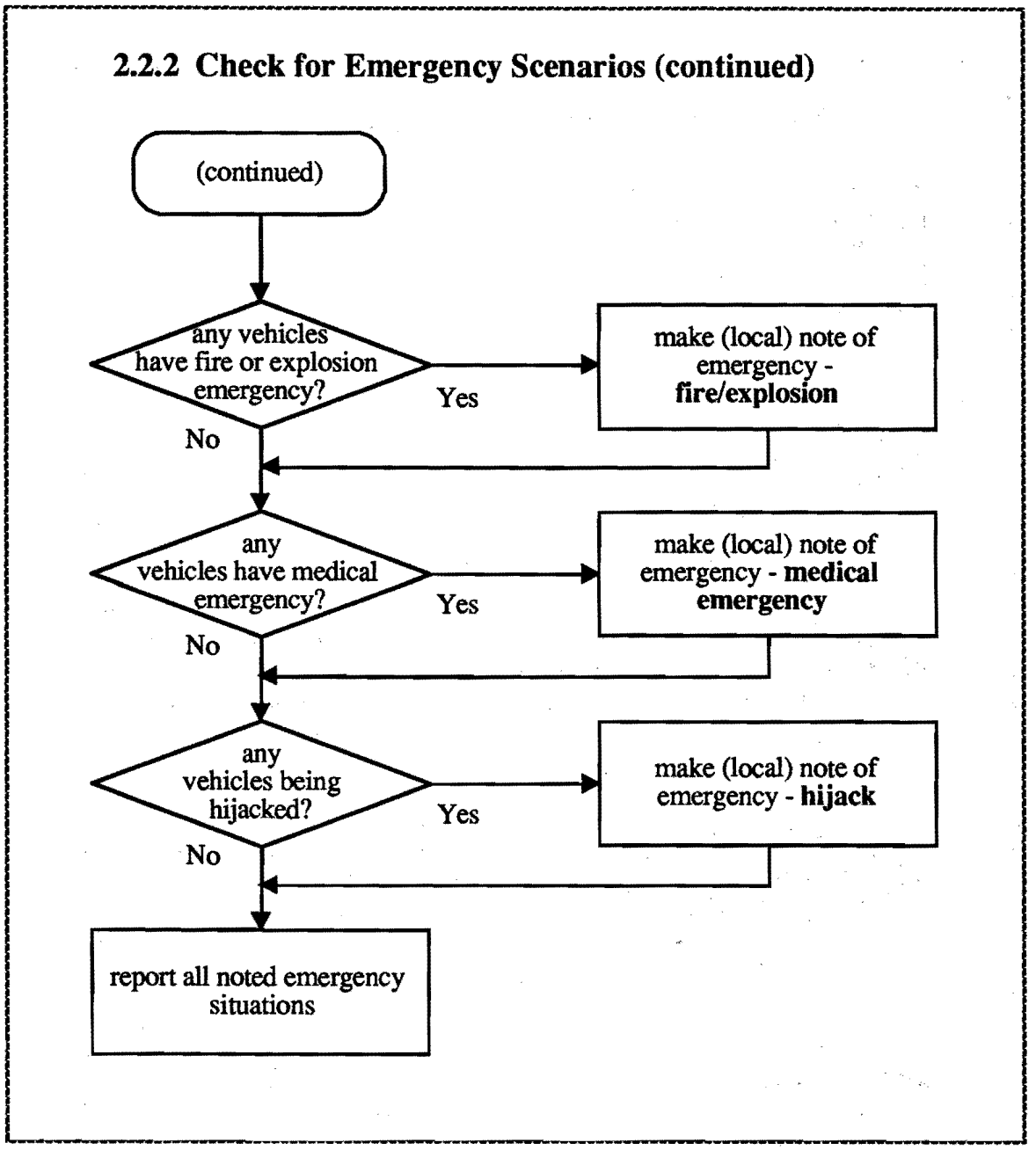


Figure 3-14. Functional Flow Diagram: Checking for Emergency Situations



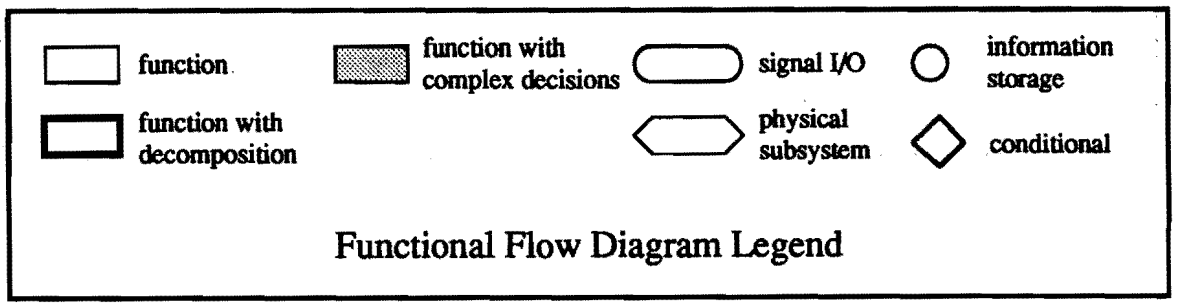


Figure 3-14. Functional Flow Diagram: Checking for Emergency Situations (continued)

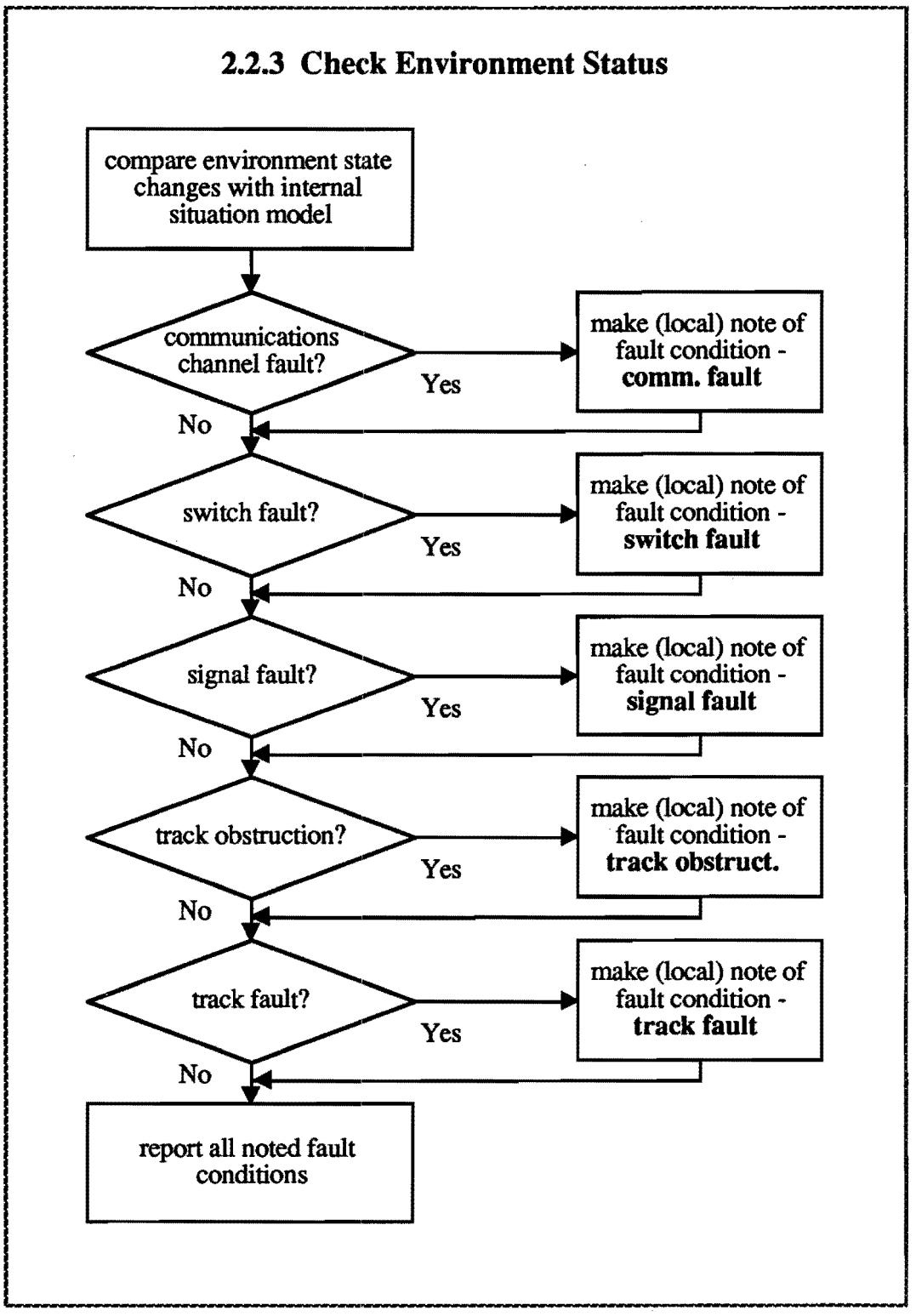


Figure 3-15. Functional Flow Diagram: Checking Environment Status

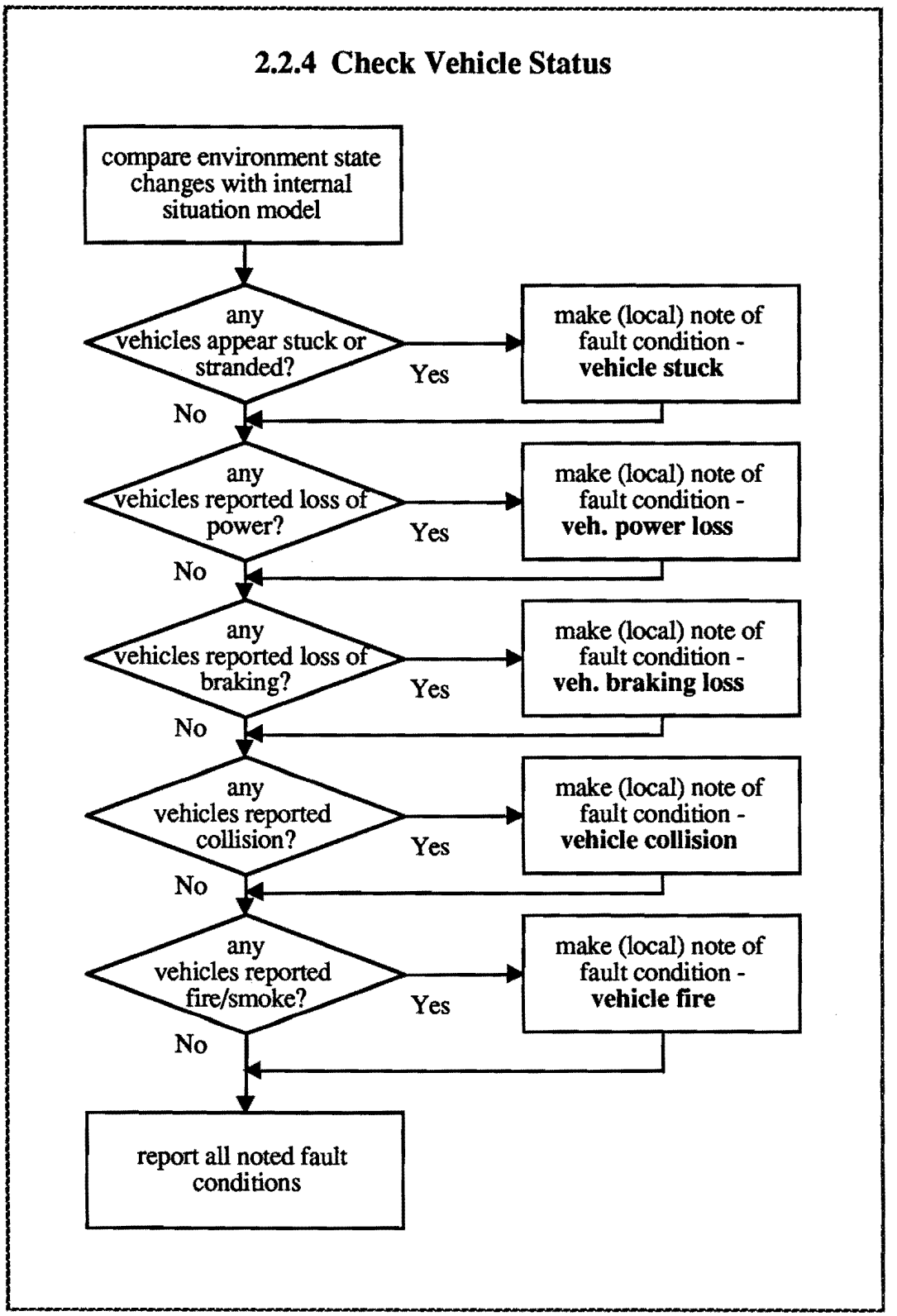
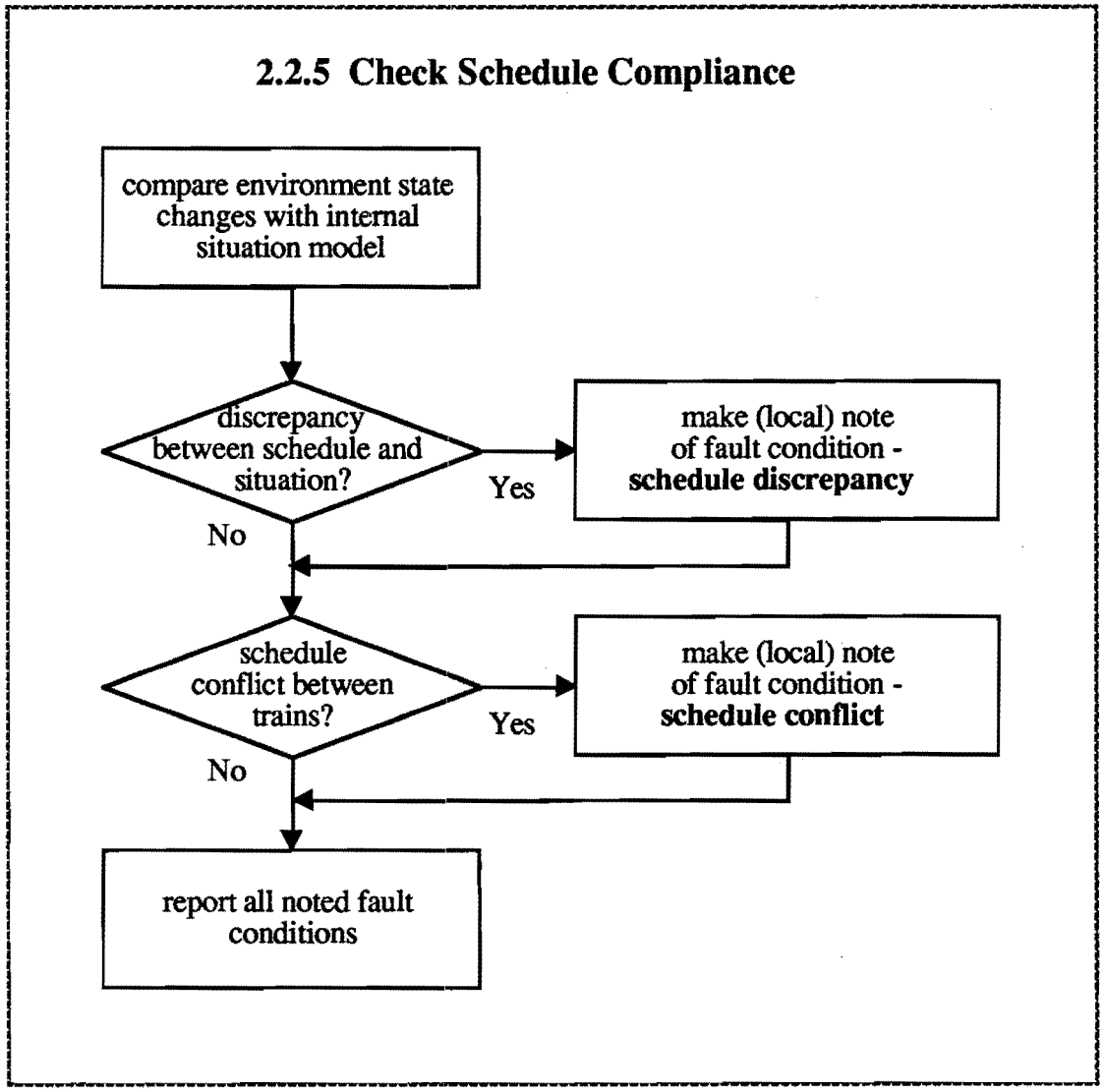


Figure 3-16. Functional Flow Diagram: Checking Vehicle Status



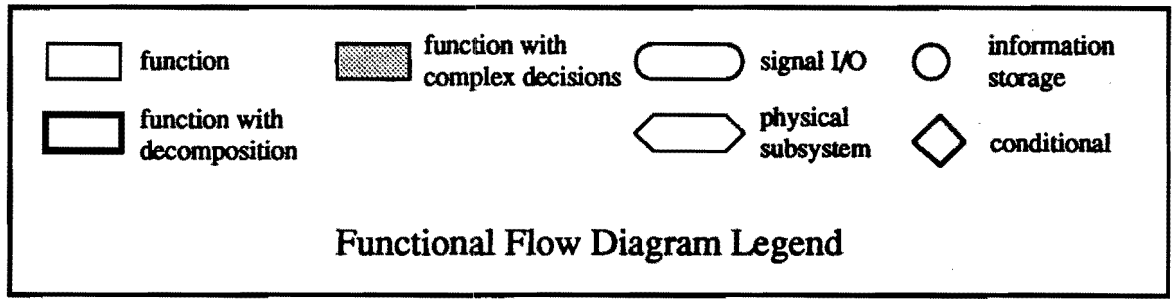
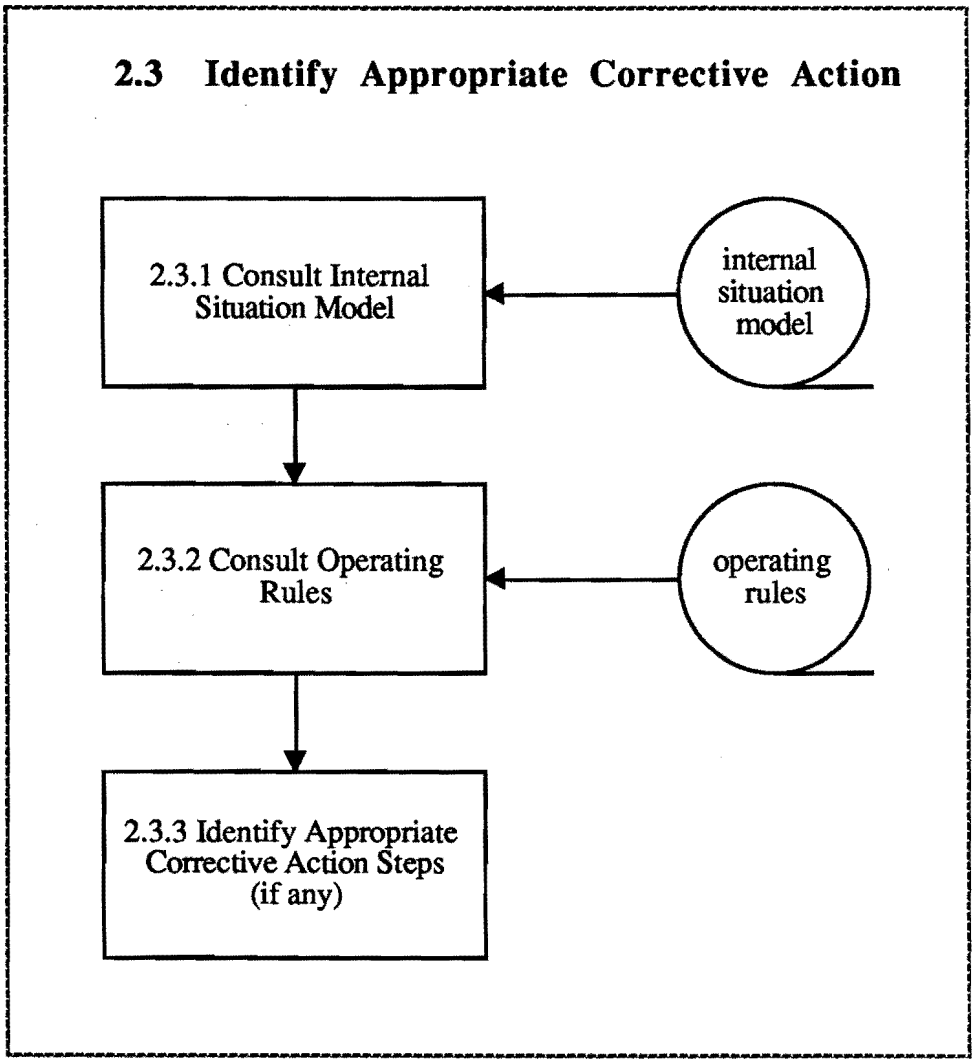


Figure 3-17. Functional Flow Diagram: Checking Schedule Compliance



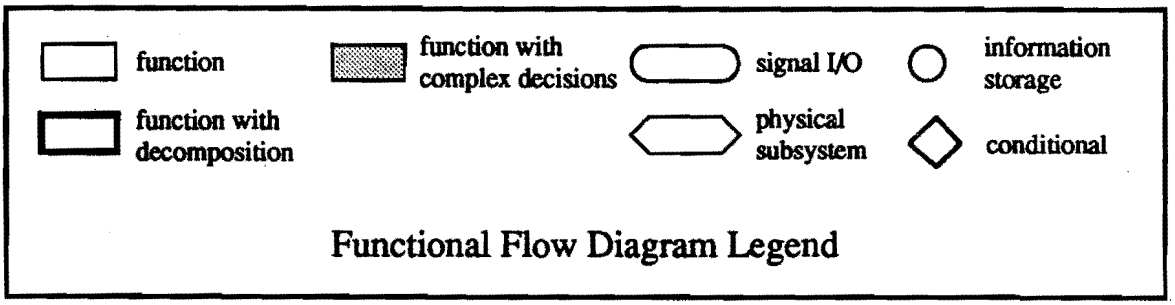


Figure 3-18. Functional Flow Diagram: Identifying Appropriate Corrective Action

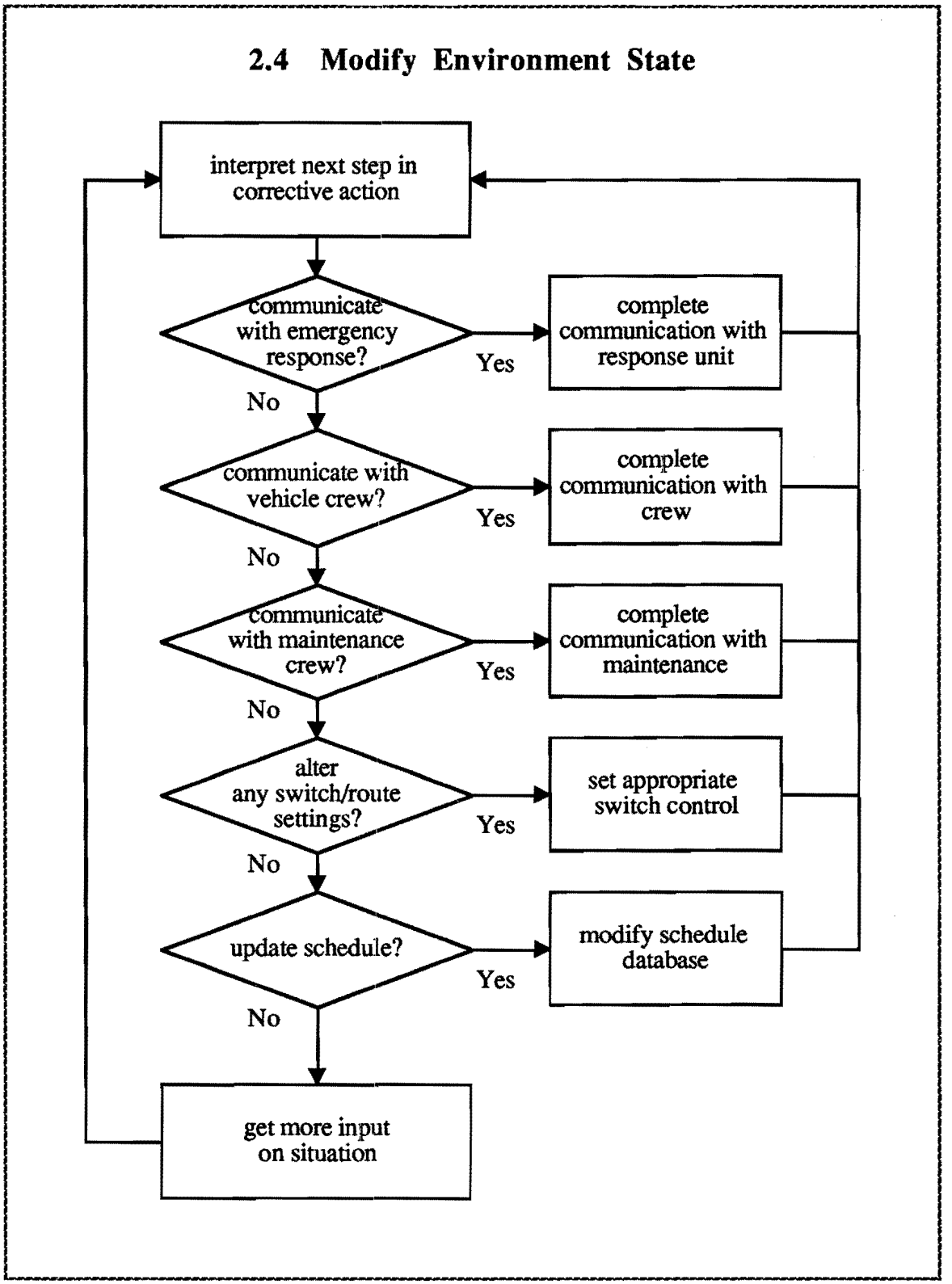


Figure 3-19. Functional Flow Diagram: Modifying Environment State

With centralized control facilities, the dispatchers sit in a control room and gather information regarding the status of the vehicles and the environment through a shared computer system. This system is also the mechanism used for actuating the available environment state parameters, such as switch settings. In effect, the command center acts as a centralized sensor and actuator interface for the collective group of dispatcher personnel, so that they can perform their operations from a common position. Some of the benefits of this approach are as follows:

1. ***Common input data.*** All of the dispatch personnel have access to the same input data from the system. Although each person is assigned to a specific portion of the system, there is generally access from any one controller station to the entire system.

2. ***Broader situation awareness.*** As a result of giving multiple personnel access to the same system input data, there can be multiple interpretations of that data, thus allowing broader situation awareness. This is enhanced in a central control station design which encourages verbal communication between the working dispatchers.

3. ***Distributed rules database.*** With all dispatchers in the same location, the responsibility for storing and accessing the stored rules database becomes a distributed task. The rules database is the collection of rules, regulations, and operating knowledge that is used in the decision process of the controllers. Especially when this database is stored in the combined memory of the personnel, the presence of several people can result in more rapid access to certain rules.

4. ***Enhanced system robustness via parallel operation.*** The presence of multiple dispatchers operating in the same location automatically provides a backup mechanism in the event of a failure of one of the controllers. For example, if a controller were to suddenly become ill and be unable to perform his or her job functions, there would be other personnel in the immediate vicinity that would be potentially capable of picking up some or all of that functionality. It is desirable that the design of a central control station provide the flexibility for dynamically reassigning duties of controller personnel in the event of such a failure.

Current practice in centralized command and control does not normally provide for computer automated environment control, although some automated decision aid tools are available. Each controller must typically maintain an internal situation awareness model throughout the shift. Some manual decision aids are used, such as schedule run sheets, but few, if any, are currently computerized. The set of operating rules, as referenced in the diagrams, consists of both the formal rules contained in the appropriate manual and the internalized rules learned through operating experience.

This analysis identifies two areas which may lead to problems in high-speed operation. The first has to do with communication delays in the sensor and actuation signal paths. Although these delays are most likely fixed and/or well characterized, they become more significant as the speed of the train rises. This is due to the fact that, for a fixed communication delay time, higher train speed results in more ground covered in the available control loop period. In effect, the communication delay may become a limiting factor in the bandwidth of the control loop, preventing the human from making control decisions in sufficient time, and leading to system

instability. This problem can be avoided by performing careful human-machine system analysis and reducing communication delays as necessary.

The second potential problem area is decision latency, which is related to the previous problem. By requiring the dispatchers to internalize the situation analysis model, as well as the operating rules and regulations, there may be a substantial period of time required by the dispatcher to sort out the necessary control issues. This, too, will be exacerbated by high-speed operation, as functional activity must occur in a shorter period of time due to higher speed. Either by itself or in conjunction with communication delay, this may lead to decision latency and instability, as described above. This problem can be minimized by judicious application of automated operator assistance tools.

3.2 SCENARIOS OF ABNORMAL SITUATIONS

This section identifies and describes selected scenarios to which a HSGGT system may be exposed. These scenarios (Tables 3-1 to 3-3) are devised to provide a framework for our study of safety and function allocation for high-speed train operation, and for developing the corresponding system-design guidelines associated with human factors issues. They will be used later for simulation and experiment.

Based on study of causes and consequences of accidents in (DOT/FRA 1993a) and in view of our objectives of studying safety and function allocation issues, each scenario is defined with certain train and/or environment conditions. Depending on the locomotive engineer's responses in the experiments, different unwanted consequences may result. All scenarios can be used to evaluate the ability of collision avoidance and other emergency handling of the system under a particular scheme of function allocation.

Table 3-1 lists some example scenarios that could be used for evaluating various function allocation and safety issues via human-in-the-loop experiments. Each scenario is characterized by three attributes: the ***cause*** of the abnormal situations, the ***scenario*** description, and the ***potential consequences.*** Note that the cause of an abnormal situation refers to the initial condition that leads to the abnormal situation. For example, "locomotive engineer fails to observe obstruction" is not the original cause of a potential abnormal situation, although it may lead to a collision. Instead, it is the "obstruction on track" that makes that driving environment abnormal. Whether the locomotive engineer succeeds or fails in observing the obstacle depends on the system function allocation design and the locomotive engineer's vigilance at the moment. The scenarios set a framework for evaluating the system function allocation design and related safety issues. Therefore, the authors believe that categorization in terms of the causes of the abnormal situations instead of the consequences (DOT/FRA 1993a) helps in development of human-in-the-loop simulation and evaluation of various function allocation schemes.

Table 3-1. Example Scenarios of Abnormal Situations with Trainset

SCENARIOS ASSOCIATED WITH A TRAINSET			
Num	**Cause**	**Scenario**	**Potential Consequences**
1	Locomotive engineer error	a) Operator fails to obey speed limit. Train is equipped with an ATP system.	Collision (with another train or maintenance equipment) and/or derailment at curve, which may be avoided if ATP activates in time.
		b) Operator fails to obey speed limit at low speed. Train is not equipped with an ATP system.	Collision (with another train or maintenance equipment), and/or derailment at curve.
		c) Alarm (cause unknown) sounds when approaching or passing a tunnel.	Locomotive engineer stops train in tunnel instead of beyond tunnel.
2	Dispatcher error	a) Under the failure of interlocking safe route system, dispatcher wrongly sets switch and diverts the train onto a wrong track.	Collision with another train or maintenance equipment on the same track.
3	Object intrusion	a) Debris, animals, people, or vehicles on track. Detected in advance by signal system.	Collision (with object) and/or derailment, which may be avoided if detection is early enough.
		b) Debris, animals, people, or vehicles on track. Cab has no advance indication.	Collision (with object) and/or derailment.

Table 3-1. Example Scenarios of Abnormal Situations with Trainset (continued)

SCENARIOS ASSOCIATED WITH A TRAINSET			
Num	**Cause**	**Scenario**	**Potential Consequences**
4	Highway vehicle crossing	a) Highway vehicle crosses the track due to failed crossing signal or human error on the part of the highway vehicle locomotive engineer. No advanced warning to locomotive engineer.	Collision with highway vehicle. May derail depending on the weight of the highway vehicle.
5	Brake system failure	a) Braking system failure en ***route*** as brakes are applied."	Collision with a similar high-speed train on same guideway, or with maintenance equipment, or object on track. Derail if at down-slope curve.
		b) Braking system failure as brakes are applied at guideway end or close to station.	Overrun at guideway end or at station.
		c) Braking system failure, caused by electronic or mechanical component failure, which is indicated before brakes are applied.	Collision with another vehicle on the same guideway.
6	Signal system failure	a) An undetected malfunction of the signal system resulting in a false proceed signal.	Collision with another vehicle on the same guideway.
7	Failure of a critical component	a) Failure of a wheel.	Possible derailment.

* The most common example of a braking fault is a train departing on a leg of a journey with inoperative brakes after a failure to perform proper pre-departure brake tests. Actually, mechanical or electrical failures in the braking system historically have been very rare (DOT/FRA 1993a).

Table 3-1. Example Scenarios of Abnormal Situations with **Trainset** (continued)

SCENARIOS ASSOCIATED WITH A **TRAINSET**			
Num	Cause	Scenario	Potential Consequences
8	Loss of power	a) Loss of electrical power from pantograph. Backup batteries are below useful level or not available. Could be caused by terrorism, transformer failure, or converter failure.	Inadvertent stopping in a tunnel. Passenger anxiety. Danger that passengers will try to escape, and inadvertently place themselves in a life-threatening situation.
9	Track fault	a) Broken rail or track buckling.	Derailment, or damage to track and trainset.
10	Passenger illness	a) Passenger cannot wait for next station stop, needs immediate hospital treatment.	Direct threat to passenger life if not treated in time.
		b) Passenger illness on an otherwise normal train. Needs first aid.	Direct threat to passenger life if not treated in time.
11	Fire on train	a) Electrical fire on power car.	Fire expansion, loss of power, injury to locomotive engineer.
		b) Passenger car on fire.	Direct threat to passenger lives.

Table 3-2. Example Scenarios of Abnormal Situations with Dispatching Center

SCENARIOS ASSOCIATED WITH DISPATCHING CENTER			
Num	**Cause**	**Scenario**	**Potential Consequences**
1	Power loss in dispatching center	a) Electrical power loss due to any (unknown) reason, and backup power fails. However, telephone communication is intact.	Loss of dispatching control for an extended time (e.g., 10 minutes). Commands to locomotive engineers via telephone.
		b) Electrical power loss and backup power fails. In addition, telephone communication is cut off.	Total loss of dispatching control. Locomotive engineers may make control decisions on their own, and inadvertently place the vehicle in danger.
2	Dispatching equipment failure	a) Computer terminal breaks down during dispatching activities.	Loss of contact with locomotive engineers. May use phone line to communicate.

Table 3-3. Example Scenarios Special to Maglev

SCENARIOS SPECIAL TO MAGLEV			
Num	**Cause**	**Scenario**	**Potential Consequences**
1	Magnet gap control loop malfunction	a) Loss of safe hover due to Maglev gap control loop malfunction, or guideway irregularities too large for speed.	Vehicle drops on skids, potentially resulting in damage to vehicle and/or passenger injury from impact.
2	Failure of a critical component	a) Malfunction in a Maglev support or guidance magnet.	Vehicle cannot move from a specific location. Vehicle drops to skids, potentially resulting in damage to vehicle and/or passenger injury from impact.
3	Crosswinds above safety limits	a) Inadequate warning of crosswinds above safety limits which leads to asymmetrical touchdown.	Vehicle contacts skids while in motion, potentially resulting in damage to vehicle and/or passenger injury from impact or sudden vehicle body motion.

4. CONSIDERATIONS OF SAFETY

The purpose of this section is to provide a background of the human factors perspective regarding safety of complex human-machine systems in general. The first section treats theoretical considerations, including definitions and costs of safety, theories and therapies for human error, safety in dynamic systems, and risk modeling. The second section comments on eighteen specific safety and human factors issues in high-speed rail.

4.1 THEORETICAL BACKGROUND OF SAFETY

Safety is a key issue in the public acceptance of high-speed rail systems. The average person has a perception of a greater risk and/or a lower tolerance for risk in circumstances that are beyond his or her control. This is evident when people ride in airplanes, elevators, and amusement park rides. As a result, it is expected that there will be a high level of safety validation required for a high-speed rail system before the public will accept it for everyday revenue use.

The term safety in everyday use means the absence of undesirable consequences, depending on context. The dictionary defines safety as "freedom from exposure to danger; exemption from hurt, injury or loss" (Webster's Third New International Dictionary 1965). Safety in economics refers to loss of money; safety in politics has to do with maintaining popularity and getting elected. Safety in transportation means getting from origin to destination without bodily harm (death or injury) or damage to property, or even (as in the first Webster definition) exposure to any of these. Another relevant term is risk, which in everyday usage means absence of safety (in Webster's Third, "the possibility of loss, injury, disadvantage or destruction").

Quantitative rigor requires more precise definitions of these terms. That, in turn, requires distinguishing two factors. The first is consequences, the actual occurrence of specific undesirable events (such as death or a specific type of injury to a specific person, or specific property damage). The second is probability, the number of times some specific consequence occurs in association with some event (a given origin-destination trip), divided by the total number of occurrences of that event (whether the event is actual or hypothetical). For us, risk means the product of consequences and their probability of occurence, or statistical expectation of consequences.

But what, then, of the idea of Lowrance (1976) cited earlier, that safety means both the assessment of risks and the assignment of value judgments to risk (or statistical consequences)? Where does the value judgment part come in?

The magnitude of the goodness or badness of consequences can sometimes be put as dollar equivalent (gained or lost). However, this is not always easy for property damage, and in the case of bodily harm it is quite difficult and controversial (insurance payoff, loss of future earnings are common measures). Some assert that it cannot be done — how does one put a dollar figure on pain and suffering?

Decision theorists, however, have a better way of scaling the goodness or badness of consequences, or their statistical expectation, by means of a well-defined experimental procedure. This approach also allows for equating different, seemingly incommensurate, consequences. It is a technique based on *utility theory* (Von Neumann and Morganstern 1944). This theory makes the fundamental assumption that if a person is indifferent to the definite occurrence of consequence A (100%, i.e., probability is 1.0) and the possible occurrence of consequence B with probability P, then the utility (the relative worth) of A is P times the utility of B. Thus, given the utility of any specific consequence B as a starting point, with a succession of experimental trials with different P values to determine the indifference judgment point for persons whose utility is being assessed, one can scale the utility or relative worth of any other consequence A.

The function relating utility or relative worth for any combination of variables of interest is called the *objectivefunction*. The simplest form is a linear weighting on the key variables. For example, for a rail passenger the utility might be

$$[K_1 \text{ times (train velocity)} + K_2 \text{ times (ride quality according to some scale of vibration)}]$$

where K values (or a nonlinear function of the salient variables) are determined by a utility elicitation from interested parties (using a more complex procedure than that described above, called *multi-attribute utility elicitation* (Keeney and Raiffa 1976)).

Obviously, while both train velocity and ride quality are desirable, reality imposes a tradeoff between the two criteria, so the traveler must decide which is most important and by how much. Usually, objective functions are non-linear, and the functions relating utility on the y axis to the physical amount of the consequences on the x axis are usually concave downward (e.g., ten ice cream cones have less than ten times the utility of one ice cream cone).

While this theory is simple and elegant and has been used in practice to model safety in many situations, critics claim that it is shortsighted for many reasons. Among these are:

1. Judges who do not have a sophisticated understanding of probability cannot make reliable judgments of the type prescribed (for example, experiments have shown that subjectively judged probabilities of mutually exclusive and collectively exhaustive events do not add to one, as mathematics would require (Edwards and Tversky 1967));

2. People cannot seem to make utility judgments for events with which they have not had personal experience (Tversky and Kahneman 1981). Asking American rail passengers about the desirability of a "tilt car" as in the Swedish X-2000 is an example;

3. Perceived negative utility for loss of life in catastrophic, low-probability events such as nuclear plant meltdown or a major train crash is significantly greater than negative utility for loss of life in more common, higher probability events such as automobile accidents. According to (Starr 1969), this has do with the fact that one is less inclined to choose exposure to dangerous low-probability events when one is not in control.

The third criterion, however, should not be confused with the fact that consequences with high dollar losses and low probability (e.g., death, extreme property damage) are perceived as much

higher risks than consequences with low dollar losses and high probability (fender-bender minor accidents) – even though the expected dollar losses are the same. This is called ***risk aversion.*** Utility theory accounts for this simply by means of a negative utility function which is increasing at a rate greater than dollar loss. This also accounts for why people tend to buy insurance for high loss/low probability events, which, of course, reduces their expected gain (gives profit to insurance companies).

Questions of how much risk is acceptable (how safe is safe enough) are matters of public interest in spending dollars to avoid risk (achieve safety). Obviously, safety costs money, and we all exercise our own utility functions for taking risks, as do the larger state and national communities through the political process. That 100% safety can never be achieved does not mean it is not a goal to strive for while considering economic and other constraints.

Currently, however, in the authors' opinion, Von Neumann's utility theory, which incorporates a notion of relative worth, for all its imperfections in practice, is the "best game in town" for assessing safety and risk quantitatively. Risk, then, is taken as probability times negative utility, and, assuming utility is normalized to a range from 0 to 1, safety could be considered to be one minus risk.

Other approaches may have promise and we suggest one below, namely that of control theory. However, first let us examine more deeply the questions of classification, causation, analysis, and therapy for human error in relation to machine failure.

4.1.2 Theories of Human Error

Human error and its role in accidents is especially salient to this report. Some people assert that accidents "just happen" and no person or thing is to blame. However, this is usually regarded as an unacceptable position. More acceptable to most people is the notion that accidents result from equipment failures (from either hardware or software) or from human error. Hardware and software failures are not the subject of this report, except with respect to operators erring by not detecting, diagnosing and properly responding to compensate for them. (Of course, at the design stage, hardware and software failures themselves can be called human designer error.) In any case, a major means to improve safety is the reduction of human error.

There has always been great interest in human error from a political, legal, and practical viewpoint. Recent interest has been concentrated in the nuclear power industry following the accident at Three Mile Island, as well as in the commercial aviation sector, because of the massive overhaul of the air traffic control network. Excellent books on human error include (Reason 1990, Norman 1988, and Senders and Moray 1991). This discussion is adapted from a chapter on human error in (Sheridan 1992).

It is easy and common to blame operators for accidents, but investigation often suggests that the operator "erred" because the system was poorly designed. Testimony of an operator of the Three Mile Island nuclear power plant in a 1979 congressional hearing makes the point: "Let me make a statement about the indications. All one can say about them is that they are designed to provide

for whatever anticipated casualties you might have. If you go beyond what the designers think might happen, then the indications are insufficient, and they may lead you to make the wrong inferences. In other words, what you are seeing on the gage, like what I saw on the pressurizer level — I thought it was due to excess inventory — I was interpreting the gage based on the emergency procedure — hardly any of the measurements that we have are direct indications of what is going on in the system." Clearly, we should design our train driving and dispatching control rooms so that they are more "transparent" to the actual working system, so that the operator can more easily "see through" the displays to "what is going on." ***Situation awareness*** is a useful term used in the aviation sector for the pilot's ability to perceive consciously the overall flight situation.

Often the operator is locked into the dilemma of selecting and slavishly following one or another written procedure, each based on an ***a priori*** anticipated causality. The operator may not be sure what procedure, if any, fits the current not-yet-understood situation. This makes his or her response quite unpredictable. In this regard (Rasmussen 1978) commented: "In the analysis of accidents, the human element is the imp of the system... The variability and flexibility of human performance together with human inventiveness make it practically impossible to predict the effects of an operator's actions when he makes errors, and it is impossible to predict his reaction in a sequence of accidental events, as he very probably misinterprets an unfamiliar situation."

Theoretically, anything that can be specified in an algorithm can be given over to the computer, so the reason the human supervisor is present is to add novelty, creativity, and adaptability in response to unexpected situations — precisely the ingredients that cannot be prespecified. This means, in effect, that the best or most correct human behavior cannot always be prespecified.

An usually acceptable definition of a human error is, "an action that fails to meet some implicit or explicit standard of the actor or of an observer (Senders and Moray 1991). "Error–no error" is the simplest possible (binary) categorization of complex human behavior, and it depends on an arbitrary standard. Behavior can be relegated to "error" or not by a modification of the standard. "Operator error" may be more a function of the measurement criterion of the analyst than of the behavior of the operator. ***Accidents*** are not the same. A definition of an accident is an "unwanted and unwonted exchange of energy" (Senders and Moray 1991).

One sometimes speaks of "good errors." The engineer would assert that there can be no feedback control without an error signal — a measured deviation, however small, from a desired reference. Many learning psychologists would assert that error is part of learning and skill development. The artist would claim that error is essential to creativity. Darwin claimed that error (he called it "requisite variety") is an integral part of evolutionary improvement of plants and animals.

Common distinctions among types of errors are:

- errors of omission vs. errors of commission (forget to do something necessary vs. do something wrong);
- errors in sensing, memory, decision, response (misunderstand situation);

- errors in intention (mistakes) vs. errors in implementing those intentions (slips);
- forced errors (in which task demands exceed physical capabilities) vs. random errors (which can be slips or mistakes).

That errors have causes seems obvious. Yet investigations of errors or accidents seldom come up with neat explanations of causality (unless they expediently truncate their investigation with simplistic explanations like "locomotive engineer drunk" or "inattention"). Most behavioral scientists would assert there is no one absolute cause, but something closer to a causal chain leading to the error. The following are some of the popularly attributed causes of human error:

1. Invalid internal model of the prevailing cause-effect relations;
2. Lack of feedback about whether results of an action were as intended;
3. Capture, where in a non-routine sequence of actions, as soon as one encounters a step common to a different but routine sequence, the latter is followed inadvertently;
4. Hypothesis verification, where subjects work to verify hypotheses they hold, searching for and retaining confirming evidence and ignoring or forgetting contradictory evidence (Rouse and Hunt 1984);
5. Inference from too-small samples of data, reliance on anecdotes and isolated cases, possibly because such anecdotes provide good mnemonics;
6. Stress and perceptual narrowing, also called tunnel vision or cognitive lockup, meaning the tendency to limit one's physical or mental attention and action to what is most immediate and familiar, being unable or unwilling to avail oneself of a broader set of options;
7. Risk (error) homeostasis, the notion that people inherently tend toward some constant level of risk (for whatever genetic or psychological or sociological reason), e.g., when safety features or increased steering or braking capability are added to automobiles, locomotive engineers tend to drive faster or otherwise take increased risks to the point where the risk level remains as before.

One can examine such human error in conjunction with machine error in the sequence:

Exposure –> attention –> decision –> action –>feedback –> correction *(if necessary)*

Each of these steps has its characteristic types of error. Errors can occur at different steps in the sequence, and can be either independent of one another or interact. Discrete failure combinatorial modeling, which incorporates previously tabled Human Error Probabilities (HEPs) for selected events, is best described by THERP, the Technique for Human Error Rate Prediction (Swain and Guttman 1983). HEP sensitivity analysis (Hall et al. 1981) starts with a nominal HEP and uses conventional combinatorics to determine what happens to some combined human-machine system as the HEP increases or decreases. Time-continuum failure models determine Mean Time Between Failure (MTBF). Assuming the operator is good at recovery or repairing, one can

incorporate data on Mean Time To Repair (MTTR) and generate statistics for the fraction of time a given system is available. Markov network models (where any change from one state to another state is a given constant probability) are also used to predict failure modes and likelihoods.

4.1.3 Recommendations for Reducing Human Error

Senders and Moray (1991) suggest the following categories of therapy:

1. ***Design to prevent error.*** Provide immediate and clear feedback of consequences resulting from upstream actions (those earlier in the consequence chain). Downstream consequences should also be used to clarify and confirm earlier actions. Provide special computer aids and integrative displays showing which parts of the system are in what state of health. Give attention to cultural stereotypes of the target population — e.g., in Europe the expectation is that flipping a wall switch down will turn a light on, so, if designing for Europeans, don't use the American stereotype. Use redundancy in information coding, and sometimes have two or more actors operate in parallel to guarantee that proper action is taken. Design the system to forgive, and to be "fail-safe" (i.e., so that a single human error or machine component failure does not lead to system failure), or at least "fail-soft" (i.e., system failure may occur, but with modest consequences).

2. ***Train operators (locomotive engineers, conductors, and dispatchers).*** Get operators to admit to and think about error possibilities and error-causative factors, since although people tend to catch their own errors of action, they tend less to catch their own errors of cognition. Train operators to cope with emergencies they haven't seen before, using simulators where available.

3. ***Restrict exposure to risky situations.*** Reduce exposure by careful design. Be conscious that this limits operator opportunity.

4. ***Warn and alarm only for most critical situations.*** Keep in mind that too many warnings or alarms overload and distract the observer; or, condition him or her to ignore them.

5. ***Make any automation more understandable.*** If automation is indicated, try to keep the operator knowledgeable about what the automation is doing, and whether it is performing as it should. Provide opportunity for operator takeover from the automation if it fails, and in training engender some operator sense of responsibility to do this.

6. ***Accept and try to recover from errors.*** It is best to strike a balance by allowing operators some tolerance of variability, and not expecting people to be error-free zombie automatons.

There are several further considerations about human error in relation to system context. It is undesirable consequences of error, not error itself, that we seek to reduce. In this regard, according to Senders and Moray (1991), "The less often errors occur, the less likely we are to expect them, and the more we come to believe that they cannot happen...It is something of a paradox that the more errors we make the better we will be able to deal with them."

It is commonly appreciated that humans and machines are rather different, and that thus a combination of both has greater potential for reliability than either alone. It is not commonly understood how best to make this synthesis. Humans are erratic. They err in surprising and unexpected ways. Yet they are also resourceful and inventive, and they can recover from both their own and the equipment's errors in creative ways. Once programmed, machines are more dependable, which means they are dependably stupid, not flexible and adaptable under changing system conditions.

Reliability analysts of nuclear power plants, aircraft and air traffic control systems, and other large systems struggle to include not only human-operator errors but also human-operator-initiated recovery factors in their analyses. This is laudable but unfortunately still insufficient. This is because human error occurrence and recovery pervade the performance of these large systems in many locations and at many stages — not just in the control room. There are many other aspects of planning and design, plant construction and fabrication of equipment by vendors, installation, calibration, maintenance, administration, and management to which operator error and recovery can be traced.

Some observers believe that often what is alleged to be operator error is in reality management's way of disguising its inability to administer effectively and to negotiate fairly with union workers, plus everyone's inability to cope with interpersonal problems — sometimes the real provocation for human error (Egan 1982). Intentional malevolence, whether from within an organization or outside, is not normally considered human error, but it is human-related and it is a source of system error. While overt attacks and sabotage are properly the domain of guards and professional security investigators and analysts, there probably exists a large "gray area" of carelessness and neglect by operators and maintenance and administrative personnel that is provoked by malevolent feelings or apathy.

4.1.4 Safety in Dynamic Systems: Temporal Dependencies

The above discussions of safety and human error characterize independent events occurring within a static (unchanging over time) or quasi-static system. In this case, causality is probabilistic and temporal dependencies are ignored. A contrasting perspective is that of dynamics and control systems, wherein differential equations are derived relating system outputs or ***states*** at each point in time to system inputs at current and all previous points in time. In the case of rail systems, state variables might commonly be considered train position and velocity, perhaps also power used. Inputs might be throttle or brake control position, track grade or curvature, and signals. Locomotive and train-consist characteristics, type and quality of track and roadbed, weather conditions, etc. would be parameters of the equations. An important characteristic of dynamic systems is the sense of history — the system retains the effects of an input event for some period of time after that event has occurred.

Associated with each state, possibly in combination with inputs and parameters, is an ***objective function,*** a function which specifies how good or bad any system state is, as described earlier in this section. In most applications of control theory, objective functions are extremely simple, such as "badness" (of some combination of train location, time, and power being used) equals the sum

of squares of the deviations of those state components from some ideal location, time, and power, each of the three terms of the sum having its own weighting coefficient. The idea is to minimize the "badness" objective function, which in this case is the equivalent of a negative utility function in static decision theory.

Our tentative belief is that rail safety should be thought of in terms of a dynamic system model, which characterizes the relative probability of different failure modes and hence indicates risk (safety). Avoidance of risk exposure then is a matter of the system state trajectory staying far from the state categories which lead to unsafe conditions, farther from those with the greatest risk. This is not unlike the problem of collision avoidance as commonly formulated in robotics (i.e., how to have the robot hand do useful work, yet not have unintended collisions with its environment). Such a formulation, in contrast to a static-state and discrete-error formulation of failure, is that the temporal determinism inherent in a dynamic system can be captured to minimize risk and maximize the assumed objective function. An example in high-speed rail is the danger of a series of small thrust actions which cause build-up of speed and momentum to a point where a reasonable braking profile cannot slow a train for an upcoming curve or stop at a designated station. With the dynamic systems approach, the "bad" effects of the sum of small accelerations would have a failure predictability built in that is absent in the traditional, more static, approaches that, for example, might treat the "badness" of each small acceleration as independent of the others. (At this point in our project we have not progressed very far in developing such models and testing such predictability for system safety. However, a more specific example is described in the next section.)

4.1.5 Network Modeling of System Risk

Consider the fault network shown in Figure 4-1. The network models the risk of certain system failures using discrete Markov state theory. This example studies safety with respect to eight "safety states" (rectangular boxes) which comprise all combinations of three component variables: degree of overspeed; track curvature; and wheel (or whole bogey) breakage. In this simple example, each component variable has only two categories: true or false. These eight safety states lead to either of two possible system failure modes: derailment of the train or the train getting stuck on the tracks (round-comered boxes). Other state component variables and failure modes are not considered in this example. Note that failure of a wheel (or that of a bogey), a subsystem, is considered a state component. The "bottom line" (lower blocks in this example) are considered system failures, not component failures.

Transition paths between the safety states are shown as solid lines. A transition path from a safety state to a system failure mode is shown as a shaded line. Arrows are included on the lines to show the possible directions of causality, and labels on the lines indicate what determines the transition. Transitions between safety states occur based on some probabilistic event.

Some of these transitions from safety states to failure modes would occur with near-certainty, while others may have lower probability. For example, if the train is traveling at an illegally high speed, is on a curve, and experiences wheel failure, it may be fairly certain that it will derail.

However, if the wheel fails while it is at a speed less than the speed limit, it might derail or it might just stop on the tracks, with some probabilistic expectation of each.

Certain state transitions are at the control of the operator, and that is why we feel an approach such as this is important to consider in a study emphasizing the viewpoint of the human in the system. In this example, the speed of the train is under the control of the locomotive engineer, and all of the state transitions due to speed come at his or her command. Other state transitions come as an expected result of some static configuration, such as the curvature of the track. Still other state transitions will come as a result of "random" physical failure of a subsystem, such as wheel or bogey failure. The safety state analysis should help us understand the cumulative (over time) effects of both human errors and subsystem failures independently, as well as the interactions between these.

Note that while some safety states in this example lead unavoidably to a failure mode, other safety states, even ones which pose a higher risk if no corrective action is taken, can be modified by the locomotive engineer's control. It is precisely these situations that we must analyze in order to determine the safety of various human roles and control architectures. By modeling the risk states within a network, we provide the opportunity to consider the options available to the operator to recover from a state which is at an unacceptably high risk. This is a significant departure from other forms of risk assessment and estimation (such as fault tree analysis or event tree analysis).

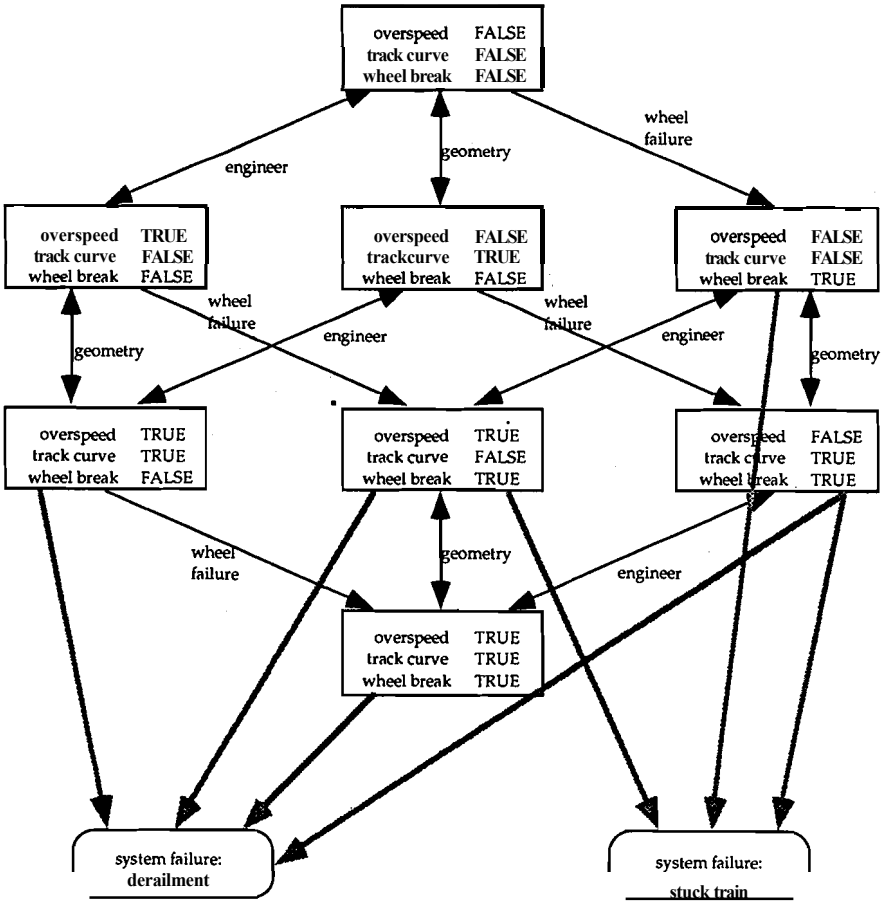


Figure 4-1. Example of a Safety State Network

To expand this methodology to safety analysis of a full high-speed train set, it is expected that the following state variables must be included for each vehicle, and could perhaps be categorized into more than two levels:

- speed,
- train position,
- brake system status,
- power system status,
- electronic systems status,
- fire/explosion,
- medical emergency, and
- hijack/terrorism.

For each segment of track (length prespecified):

- signal status,
- speed limit,
- track curvature,
- track condition,
- track obstruction status, and
- weather.

For each controlled track element (i.e., switches):

- switch state,
- actuator status, and
- sensor status.

Ideally, there would be a continually updated failure mode analysis for each vehicle within the rail system. This on-line failure analysis would be used to provide a running estimate of the safety of that vehicle, and this information would be continuously available to both the locomotive engineer and appropriate dispatchers. Perhaps such a safety analysis could also be used as a validation tool for both human and automatic control elements by providing a means for measuring and evaluating the control actions of any control element which has an impact on safety.

Such a failure mode analysis could be extended to analyze the operation of the entire rail system, focusing on the interaction between trains, between trains and switches, trains and track work crews, trains and station facilities, etc. Then the system state variables might include:

- pending collision between trains (for each pair of trains),
- train approaching failed switch (for each switch),
- train approaching failed signal (for each signal),
- train approaching obstruction (for each train), and
- central control sensor failure (for each available sensor).

This approach to system risk analysis allows simultaneous estimation of various potential paths of system failure. It recognizes that system failures are often the result of several causal factors, and identifies the risk paths from a given system state to a system failure. It can help the system designer realize the ideal of "fail-safe" or "fail-soft" by identifying when there are no "back-ups" or means to "buy time," and test in theory how system safety would be enhanced if there were.

4.2 SPECIFIC RAIL SAFETY ISSUES EXACERBATED BY HIGH SPEED: RELEVANT TECHNOLOGY TRANSFER

High speeds in passenger train operation appear to increase the importance of a number of specific safety issues. Below we cite eighteen such issues. Some have been mentioned earlier in the report. Their order of discussion is not intended to indicate priority.

4.2.1 Delay and Instability of Command and Control Loop

The faster the response of any dynamic system (e.g., a train), the greater the effect of any given delay in control (e.g., braking). If a delay reaches one-half cycle of some closed loop adjustment, what is meant to be negative feedback becomes positive feedback, and can lead to making matters worse instead of correcting them (i.e., instability). (Such tendencies are recalled by past users of intercontinental telephone circuits, which had sufficient time delay so that one tended to repeat oneself just as the other person was heard to reply.) Time delays are exacerbated when two or more persons (e.g., locomotive engineer and dispatcher) are involved in making repeated control decisions because of the delay in their communication and joint decision. For these reasons, it is important to identify all delays, whether caused by electronics, machines, procedures, or operator reaction times (or a combination), in all closed control loops. This includes, for example, delays in any manual or automatic speed control system, signal setting system, interlocking system, switch operation system, schedule control, emergency response, etc. These systems should be characterized sufficiently so that parameters such as source of possible delay, expectation (probability density) of delay, control bandwidth, communication noise, possibility of instability, and failure modes are reasonably well understood.

4.2.2 Preview and Braking Distances

At the high speeds considered (above, say, 200 km/h), the locomotive engineer's available visual preview distance for objects smaller than a car or truck becomes shorter than the distance required to stop the train, even under good daylight viewing conditions. At night it is evident to anyone riding in the cab that preview distances are even worse. Thus, the operator will be unable to halt the train before such an object on the track is struck by the train. This problem suggests grade separation, an obvious but expensive solution. (Current practice in all countries employing high-speed rail systems appears to exempt locomotive engineers from responsibility for injuring persons on the track between stations.)

4.2.3 Accommodation of Low-Speed Passenger or Freight Trains

High speeds also make it much more difficult to accommodate low-speed passenger and freight trains on the same track. Long headways will have to be enforced to keep a safe distance and to allow the same time separation required for meets and passes.

4.2.4 Danger to and Warning of Maintenance Crews

Higher speeds and resulting greater surprise factor may require additional measures to warn track maintenance crews of oncoming high-speed trains.

4.2.5 In-Cab Signaling

In our discussions with SNCF, DB and EJK, we were told repeatedly that locomotive engineers of high-speed trains cannot reliably read wayside signals of conventional size. The seemingly obvious solution is in-cab signaling (see Gruire 1992).

4.2.6 Locomotive Engineer View Ahead

Traditional locomotives have ample forward and side-looking windows to provide a wide view (about 200 degrees). New designs of the TGV cab reduce the forward-looking view to a small window in the center of the cab, presumably because there is nothing the locomotive engineer can do about obstacles in the forward view and also because objects dropped from bridges and other overhead structures can break the windows, especially at high speed, and injure the locomotive engineer. We feel that such a reduction in window area is appropriate, but that some view ahead is necessary and gives the locomotive engineer a better sense of where he or she is along the route. Side windows are essential to confirmation of the correct stopping point in stations and to communication with station personnel.

4.2.7 Headway Control, Interlocking and Signaling

Current rail-safety practice is based on blocks which are fixed to the track and have fixed location wayside signals. Safety interlocking is predicated on the block system. With continuous train location (GPS or other), and continuous communication and updating of in-cab displays, the traditional block system loses its necessity. Separation rules can be put into effect which are continuous in time and space (sometimes called "moving blocks" or "bubbles"), including electronic interlocking which is a function of speed and other factors. These would allow the same margin of safety without the "noise" factor introduced by the discretization of position and time, and could allow shorter headways on the average. Some advanced system planners in Germany and Japan have similar developments underway.

4.2.8 Locomotive Engineer Alertness Measures

More extensive and sophisticated automation, by definition, removes the operator from the control loop. Operators may even become so confident in the automation that they feel themselves to be less responsible for control than without automation. Experience in commercial aviation and nuclear power station operation has shown that automation makes it easier for the operator to become unalert and even fall asleep. If automation fails, the onset of the demand for human attention may be sudden, and the resulting transition from very low to very high workload may be overwhelming. For these reasons, some artificial means may be necessary to monitor locomotive engineer alertness, perhaps some means more sophisticated than alerter systems now commonly used in the US. Section 2.4.1.10 discusses alerter systems being used in the ICE and TGV systems. Some such device is deemed to be a good idea for American high-speed rail systems, but the choice of the precise technique needs significant further investigation.

4.2.9 Speed Control Aids — Predictor Displays, Speed Command Display, Cruise Control, and Automatic Speed Control

We believe that higher speeds pose a need for speed control aiding to the locomotive engineer, in the form of either information displays or automatic controls, or both. Four specific categories of locomotive engineer aids are as follows:

1. A "predictor display" such as that proposed by (Kuehn 1992) which presents a prediction of the position of the train over the next several minutes based on past and current control activity. Perhaps this display could show directly the relative risk of the predicted trajectory, or even indicate possible logical paths (contingencies) to system failure, as discussed in Section 4.1.5.

2. A display which tells the locomotive engineer exactly what throttle and brake actions are necessary to arrive at the next station as close to on-time as possible while minimizing traction energy. This proposal is described in (Yin and Sheridan 1994).

3. A "cruise control" system similar to that of an automobile, where the locomotive engineer can set the reference speed and the system will automatically control to that speed.

4. A fully automatic speed system which continuously adjusts throttle and brake actions to arrive at the next station as close to on-time as possible while minimizing traction energy (see Section 5). The locomotive engineer could override this system, if necessary.

4.2.10 In-Cab Display of Traffic Information

Currently, aircraft flying on instruments depend on the air traffic controller to be aware of other aircraft or weather hazards in the vicinity. A system called TCAS (Traffic Alert and Collision Avoidance System), which gives the pilot the same type of information, is being evaluated for use in air-control systems. The same could be done for trains, where the locomotive engineer sees a display of all trains and the relevant track configuration within, for example, 100 km.

4.2.11 Integrated "System Health" Displays for Locomotive Engineers or Dispatchers

Following the nuclear power plant accident at Three Mile Island (TMI), in which control room operators did not comprehend the developing situation in time to avoid the catastrophe, the U.S. government mandated that all nuclear plants have a retrofit "safety parameter display system." This included logic to process signals from the myriad of existing alarms and to indicate to the operator very simply whether the plant was in "good health," and, if not, what major system was abnormal. In an ***ab*** *initio* design of high-speed train cabs and dispatch control rooms it is probably best to include this function at the highest level, and then to have all other alarms, warnings, and cautions flow logically from this point (as in a fault tree). Such a design should maximize the diagnosticity of any system failure. This prevents the situation where a myriad of warnings and alarms occur simultaneously, leaving the observer confused about the root cause.

4.2.12 Computer-Based Emergency Procedures: Tying into Alarms

Another potential technology transfer, from recent developments for nuclear plant control rooms and commercial aircraft cockpits, concerns the storage and display of procedures and associated system information. In emergencies, both the locomotive engineer and the dispatcher observe alarm or warning signals, and, quite naturally, search for the cause of the alarm. Thus, they may want to refresh their knowledge of the physical structure or logical architecture of the alarmed subsystem. They may also want to be reminded of the procedural steps to consider in responding to the alarm (though the precise best steps depend upon other circumstances and must be left to the operator's judgment – that is why a human is there). Further, the issuance of any rule and procedure change could be a potential cause of human error, since the locomotive engineer, especially when under stress, might revert to the old regulations or rules. The proposed diagrams, specifications, and procedures could be brought up automatically on a graphical computer screen (or be available with a minimum of page selection). As with the predictor display mentioned above, perhaps this display could also show the relative risk of the predicted trajectory or indicate possible logical paths to system failure. In addition, reasons and assumed conditions could be stated explicitly (always a good idea with expert systems where a user, particularly one under stress, may tend to feel that he or she knows better and the recommended procedure does not

apply in this case). To a modest extent, such computer-based assistance for response to alarms already exists in the ICE and TGV systems (see Section 2.4.1.4.).

4.2.13 Event-Based vs. Symptom-Based Procedures

The accident at Three Mile Island taught an important lesson about operating procedures, namely that "event-based procedures" ("if failure A occurs, then do B") may be useless in a crisis where it is very unclear what has failed. Typically all that is known at the outset in such situations is that some indications the operator receives are not normal and suggest trouble. The first impulse is to seek more information and commence a diagnosis before taking action. However, if some serious consequence is one of many possible outcomes of the situation, one cannot keep searching out data without taking some precautions, some responses to allay the most serious concerns and "buy time." Before the TMI accident, the nuclear power industry was well equipped with finely honed "event-based" procedures, but it became evident that what was needed in addition were sufficient "symptom-based" procedures, i.e., procedures that are followed in immediate response to (a pattern of) indications when no clear understanding of their cause is evident. We believe that as U.S. rail systems operate at higher speeds and become more complex, there will be a need for addition of "symptom-based" procedures.

4.2.14 Required Pre-Trip Testing of Brakes

It was pointed out in Chapter 2 that braking failure is usually caused by the locomotive engineer's failure in pretrip testing. Such human error can be prevented by programming the pretrip tests into the computer and using the computer to monitor the locomotive engineer's pretrip testing procedure. In other words, the system could be designed such that if the pretrip tests are not performed, the train will not start or at least the infraction will be logged automatically. Generalizing this notion, a computer could have a check list of items that had to be tested at certain times and could demand at least some verification (e.g., a switch on and off), otherwise it would sound an alarm.

4.2.15 Computer-Graphic Schedule Maps for Dispatchers

A key piece of information used in dispatching control centers is the paper chart showing time on the horizontal axis, location along the track on the vertical axis, and representing each train's schedule as a diagonal trajectory with horizontal pauses at the stations. Currently, these charts are prepared along with the schedule, but are modified from day to day based on track conditions, maintenance, trainset changes, etc. This information can be put on a computer screen and modified in real time, so that when any train is inadvertently slowed it could easily be seen how other trains would be affected, how far the effect would go, and under what circumstances serious dispatching difficulties would result. We believe current DB experiments with this type of display and associated computer-based decision aiding are very promising as a means of avoiding collisions, and the design of such aids deserves further study.

4.2.16 Enhanced Large Screen Displays for Dispatching Center

Currently, large common screens at dispatching centers provide personnel with a shared space for monitoring and discussing traffic situations. Current computer technology and panel displays (LED and LCD) would permit operators to use individual displays to scroll horizontally or vertically to visually selected areas on the large screen and bring up much greater detail, possibly using other controls to "page down," add or suppress data, etc. Such flexibility could be a means to enhance "situation awareness" of dispatchers. Therefore, we believe this is also a fruitful area for further study of alternatives provided by today's technology.

4.2.17 Telepresence Inspection of Remote Locations on Train or Track

Telepresence refers to the ability, provided by currently evolving display technology, to feel "present" visually at any remote location and visually inspect over a wide solid angle by moving one's head as one would if one were actually present at that location. This is done by donning a "head-mounted video display" (or positioning a miniature video monitor mounted on a multi-axis boom) and simultaneously having the remote camera orientation servoed to the head or boom orientation. By this technique the achievable sense of presence and ease of scanning is remarkably easy and natural. A single radio or coaxial video or optical fiber communication channel could be tied to a large number of miniature video cameras to inspect key locations on various train cars, etc. This technique may be especially useful in high-speed rail systems to allow train set inspection (e.g., underneath or in otherwise inaccessible places) during runs and/or to minimize inspection at stations.

4.2.18 Design and Training to Enhance Cognitive Consistency

Cognitive consistency refers to the consistency of environmental reality with what the operator thinks about the environment. Three caveats are:

1. It is important in supervisory control of complex systems that cognitive consistency be designed into the operator displays and controls, the architecture and any internalized model of the controlled system, and finally the mental models taught to the operators (or implied in training). These system and task elements must be consistent both with one another and with the actual controlled process (the traction system, the braking system, or whatever). This applies to display-control directional compatibility, size, layout, and other features.

2. In training, the difference between "rules of thumb," which may not apply in some cases, and absolute truths should be made clear to operators. In the Three Mile Island nuclear plant accident, operators became obsessed with a rule-of-thumb — "never let the pressurizer go solid" — which completely dominated and even distracted the operators from the reality that the pressurizer (which is a coolant reservoir in the primary reactor cooling loop) had filled to the top with water because a pressure relief valve at its top had opened, not because of high water pressure. Thus, rules of thumb must be taught and designed around only after close examination of the extent of their robustness and generality.

3. It should be clarified under what circumstances operators are expected to follow established policies, procedures, and practices, and under what circumstances they should be resourceful and creative (or how they get permission to do so) in order to cope with reality, especially under stress. Otherwise, there will be a dilemma and inaction at just the worst time. Such a dilemma might occur, for example, when a train is stuck in snow.

5. HUMAN-MACHINE ALLOCATION IN FUTURE HIGH-SPEED TRAINS

5.1 INTRODUCTION

As is evident from the function analysis, the primary task in train driving is speed control. To perform this task well, the locomotive engineer or machine must know the track properties (grades, curvatures, etc.), the train properties (length, weight, propulsive power, characteristics of resistance and tractive forces, etc.), and the operating rules (speed limits, emergency handling procedures, etc.). As measurement technology develops and computer capability improves, fully automatic speed control becomes technically possible.

The question is then: how should the available information and control capability be used? At one end of the utilization spectrum is manual control, which presently dominates most locomotive operations. At the other end is completely automatic control. The former is very demanding on the locomotive engineer and is likely to result in less than ideal performance. The latter may not be easily accepted by the public for various reasons, even if technology permits, and will surely fail when the input information is incorrect.

Assuming full automation, keeping the operator in the cab without an opportunity to participate in the control during normal operations can be problematic. The operator may develop complacency, low job satisfaction and/or other human factors problems, and therefore may not be able to cope with emergencies the way he or she is expected to. Further, machines lack the flexibility that humans have in handling abnormal or emergency situations. Dorer (1994) cites the following problem areas under full automation (results of either locomotive engineer or dispatcher actions, though more critical aspects revolve around the locomotive engineer):

Under normal operating conditions:

- improper baseline information entered by locomotive engineer for brake system;
- improper use of override features of automatic control;
- manual backing up into station after overrrun under automatic control;
- station overrun by locomotive engineer;
- lack of attention or slow awareness to failures of automation.

Under emergency conditions:

- improper action — e.g., fire in tunnel, operator stops train in what proves to be an undesirable location;
- delayed action — undetected (by automation) obstacle not immediately noticed;
- slow or improper response to emergency situation;
- lack of attention or slow awareness to failures of automation.

What we seek then, is some kind of human-machine cooperation that combines the strength of the two agents in the cab and overcomes their weaknesses.

Studies have been made on automatic dispatching that involve pacing trains over a territory by a train dispatcher to ensure travel according to an optimal velocity profile so as to save fuel (Harker 1990, Kraay et al. 1991). However, the issue of how the locomotive engineer uses the

velocity profile (a combination of throttle and brake settings) and how it might be used for automated speed control has been addressed insufficiently.

This section addresses the issue of human-machine allocation of train control tasks by considering alternative uses of optimal speed and thrust-braking profiles which can either be displayed to the operator as a manual control aid, or be used for automatic speed control. A particular approach to this is presented in detail in (Yin and Sheridan 1994).

5.2 COMPUTING OPTIMAL THRUST AND BRAKING PROFILES

Technically, it is now quite feasible to automate train speed control to keep the train within speed limits, adhere to the schedule, and, under these constraints, simultaneously minimize energy consumption. Automatic measurement of train position, velocity, thrust, braking, and other variables has steadily improved, and advanced cab-signaling systems are becoming available. Modeling of train dynamic characteristics is more precise with the advent of new techniques. Computers are becoming faster, cheaper, and more reliable, which allows us to implement some computationally demanding algorithms that were not possible earlier. Therefore, once the current location, time, and scheduled next stop location of a train are known, it is possible to obtain an optimal solution of the speed control for its whole trip — optimal in terms of energy consumption.

An example of a particular approach to optimization of speed and thrust-braking profiles is described in (Yin and Sheridan 1994). Such an approach could be used for automatic speed control. Yin and Sheridan (1994) also suggest an integrated display which might be used by the locomotive engineer as a driving aid, much as a flight director display is used by an aircraft pilot (see also p. 4-13). The following section presents options for such a display to be used in view of human-machine allocation issues in cab design.

5.3 TO KEEP OR NOT TO KEEP THE LOCOMOTIVE ENGINEER?

Yin and Sheridan (1994) describe two contrasting ways of applying an optimal time-energy solution in train speed control. It is argued that, under the assumption of sufficiently accurate models of track geometry and train dynamics, and sufficiently accurate train state measurements, optimal automatic control of train speed is quite feasible. One design of such an automatic control would be the direct implementation of the optimal thrust-braking profile described above. Alternatively, the optimal profile can be used, not for automatic control, but for a display to a locomotive engineer. If the human, in manual control, followed precisely such a profile, it is claimed that better speed-control performance would be achieved than if that person had to perform various mental calculations during continuous decision-making and control. This decision-making process can be quite demanding for a new locomotive engineer. Thus there are four rather different options:

1. **Manual control, with traditional displays only.** Keep the locomotive engineer in charge and do not give him or her the integrated display, for fear that otherwise there would be a tendency to slavishly follow its recommendations and lose the ability to "think for oneself."

2. **Manual control, with the integrated display as an aid.** Keep the locomotive engineer in charge, give him or her the display described above, and expect the display to be used properly as a decision aid for controlling the train.

3. **Manual control, with the integrated display as an aid, plus the automatic control option.** Keep the locomotive engineer in charge, give him or her the display described above, and, in addition, make some form of optimal automatic control available. Leave the use of either mode of control at any time up to the operator (much as "cruise control" is now used in trains and automobiles).

4. **Fully automatic control with emergency-override options.** Use automatic optimal speed control under normal conditions, but allow emergency override by:

   a. an operator in the cab who is there to perform other duties, or

   b. staff personnel elsewhere on the train who might take over control from where they are, or come forward to the cab as time allows. or

   c. a dispatcher from the dispatching center, if the system allows.

In the fully automatic control mode, the display serves as a means for the computer to communicate with the locomotive engineer about the current states and future intentions of the automatic control system.

Note that all the above options should include the ATP capabilities with which a train is normally equipped.

Several considerations bear upon the choice among the speed control alternatives:

1. **Basic system features.** As discussed in Section 2.4, system features, especially signal system capability and types of braking systems, strongly influence the appropriate level of cab automation and thus the role of the locomotive engineer.

2. **Experimental results.** There is no substitute for experimental tests and demonstrations to verify the usefulness of the proposed locomotive engineer aid and modes of automation. The authors expect to perform preliminary laboratory demonstrations as a future part of this research.

3. **Proper view of human's role in automation.** A prevalent position taken by some system designers is that automatic control is essential for modern high-speed trains, and there is simply nothing to debate. A high degree of automation is now widely accepted in aviation by pilots, airlines, and regulators, although human pilots remain in cockpits. However, accidents continue to occur, accidents for which the pilots often blame the automation.

   With regard to automation, history has shown that we are not always as smart as we think we are. For example, Charles Stark Draper, the "father" of inertial guidance (used to take the astronauts to the moon), proclaimed at the outset of the Apollo Program that the astronauts

were to be passive passengers and that all the essential control activities were to be performed by automation. It turned out that he was wrong. On that mission and many since, many routine sensing, pattern recognition, and control functions had to be performed by the astronauts, and certainly some critical emergency decisions as well.

4. **Introduction of new tasks for the locomotive engineer accompanying the automation.** Since some tasks (such as planning ahead, replanning in case of emergency, voice communication with the dispatcher, etc.) may not be automated, it may require that a trained operator remain in the cab, but without much to do during normal operations. This may result in loss of vigilance and development of complacency. A natural remedy is to give the operator something more to do. More activity than now practiced in diagnosing various subsystems on the train (such as air conditioning , engine operating status, etc.) is one possibility. How such additional tasks interact with the speed control task is an issue to be investigated.

5. **Public anxiety.** It is expected that there will be great public anxiety with driverless control in full-size high-speed trains. However, it is clear that some small-scale trains which operate within airports (e.g., Dallas-Fort Worth, Atlanta, Orlando, and Chicago) or from airport to city center (e.g., the French VAL) are driverless. Therefore, reflex anxiety about driverless trains may be waning.

6. **Liability in case of an accident.** The threat of litigation in case of any accident in an automated system gives developers pause.

We believe that development of speed control should progress in stages, from the current situation of fully manual control (item 1 from the list of control options at the beginning of this section), to manual control with an integrated display as an aid (item 2), then to manual control with an automatic control option (item 3), and perhaps finally to fully automatic control (item 4). We think this would be the safest and most acceptable way for development and evaluation to go.

6. SUMMARY, CONCLUSIONS AND RECOMMENDATIONS

6.1 SUMMARY

Section 1 of this report assumes that future U.S. passenger rail systems will operate at significantly higher speeds and closer headways than are found at present. It also assumes that much more sophisticated technology for measurement, communication, computation, control, and display will be available for such future high-speed passenger rail systems than there is now. These factors pose important questions regarding the best use of both this new technology and the available capability of operators. Does it require full automation without human involvement? Or does it mean continuing to depend primarily on human judgment and decision-making without depending upon automatic sensing and control. Alternatively, is there some other, more intelligent integration of both human and machine resources?

In Section 2 we consider these central questions in the context of examining a range of human factors issues associated with high-speed rail technology as evidenced in Europe (primarily Germany and France) and Japan, as well as current practices in the U.S. In the process we also examine "human-centered automation" approaches already taken in aviation, space, nuclear power, and other large scale systems where public safety is critical, and which have in some sense led the rail industry in technology implementation.

We further consider various methods of safety analysis (Section 3) including function analysis and consideration of potential accident scenarios.

Section 4 presents our current thinking on safety and risk, primarily from the viewpoint of human factors. It also discusses briefly a number of specific safety issues pertaining to rail systems, many of them already well known, and what technology can be transferred from other sectors. We point here to a number of specific opportunities for computer-based decision aids to both the locomotive engineer and the dispatcher for planning, previewing conditions as they develop, responding to alarms, using correct procedures, etc.

Section 5 considers the specific problem of speed control, perhaps the most obvious area for reconsidering the human role in high-speed trains. In this regard, we offer a specific example of how, assuming new train location and dynamic modeling technology, optimal control becomes feasible to both keep trains on time and minimize energy usage (see (Yin and Sheridan 1994) for more detail). Finally, we consider a rational progression for development of automation in speed control.

6.2 CONCLUSIONS AND RECOMMENDATIONS

1. It is evident that the German philosophy of rail development emphasizes automated control with use of the human as a system monitor, while the French and Japanese depend more on the human for control decisions. However, the similarities in development are more striking than the differences.

a. All three countries have faced the fact that high speeds tend to preclude dependence on the locomotive engineer's out-the-window preview to avoid collision, and pose more stringent requirements on automatic braking.

b. All three countries have adopted in-cab signaling, and technology for monitoring the alertness of the operator (with automatic braking if he or she fails certain tests).

From a human factors viewpoint, we endorse all of the above for adaptation in the U.S.

2. With regard to technology transfer from other technological sectors, such as aviation, space, and nuclear power, it is evident to us that neither overnight nor wholesale adoption of existing systems from other sectors is practical or sensible. Yet there are many ideas which seem to have great relevance for future high-speed rail systems in the U.S., including Global Positioning System location technology, digital data communications, computer graphics display, symptom-based procedures, hierarchical alarms to aid diagnosis, telepresence remote inspection, and others.

3. We see many "static" approaches to safety as being limited in the high-speed rail application. We recommend further development of certain techniques, described here in initial form, for considering safety with respect to alternative operator actions in dynamically evolving situations ("safety states" having different probabilities of leading to "failure modes").

4. We believe the trend toward what is commonly called "supervisory control" or "human centered automation" — humans aided by computers for information and planning, and implementing control decisions through computer intermediaries — is highly applicable to high-speed rail systems. Yet certain realities, including lack of perfect measurement and modeling, as well as unanticipated events, continue to call for active participation by an operator. We fully endorse the use of computer and control aids provided that they are sufficiently well "human engineered," and their use ***per*** se does not become too much of a distraction to human monitoring and retention of responsibility for safety. We envision an evolutionary approach that begins with full control by a locomotive engineer who observes "optimal" control advice, progresses to discretionary use of automatic control, and perhaps eventually evolves to full automatic control with the engineer monitoring systems and with the potential of override capabilities.

5. The new close collaboration between locomotive engineer and computer does not mean the locomotive engineer must be a computer programmer, but it does mean he or she must have sufficient training and understanding of what computers are, how they work, and what can be expected in particular rail system applications. Not only because of new computer controls, sensors, and communications, but also because of the increasing speeds and momentum levels, locomotive engineers of high-speed trains must be more literate and better trained in computers and salient forms of electromechanical technology than at present.

REFERENCES

Amtrak (1992). *Manual of Instruction For Transportation Department Employees.* National Railroad Passenger Corporation.

Bing, A., A. Boghani, and T. Rasmussen (1990). "Maglev Signal/Control Assessment." Unpublished letter report to VNTSC, April.

Chapanis, A. (1965). "On the Allocation of Functions between Men and Machines." *Occupational Psychology,* 39: 1-11.

Dorer, R.M. (1994). Personal communication.

Dorer, R. M. and W. T. Hathaway (1991). *Safety of High Speed Magnetic Levitation Transportation Systems, Preliminary Safety Review of the Transrapid Maglev System.* DOTIFRA Interim Report DOT-VNTSC-FRA-90-3, November 1990, Reprint May 1991.

Dorer, R. M., S. H. Markos, et al. (1992). *Safety of High Speed Magnetic Levitation Transportation Systems: German High Speed Maglev Train Safety Requirements - Potential for Application in the United States.* Final Report DOT-VNTSC-FRA-92-3.

DOTIFRA (1991a). *Safety Relevant Observations on the ICE High Speed Train.* July.

DOTIFRA (1991b). *Safety Relevant Observations on the TGV High Speed Train.* July.

DOTIFRA (1993a). *Safety of High Speed Guided Ground Transportation Systems, Collision Avoidance and Accident Survivability,* Volume 1: Collision Threat. Final Report DOT-VNTSC-FRA-93-2.I, March.

DOTIFRA (1993b). *Safety of High Speed Guided Ground Transportation Systems, Collision Avoidance and Accident Survivability,* Volume 2: Collision Avoidance. Final Report DOT-VNTSC-FRA-93-2.11, March.

DOT/FRA (1993c). *Safety of High Speed Guided Ground Transportation Systems, Collision Avoidance and Accident Survivability,* Volume 3: Accident Survivability. Final Report DOT-VNTSC-FRA-93-2.111, March.

DOTIFRA (1993d). *Safety of High Speed Guided Ground Transportation Systems, Collision Avoidance and Accident Survivability,* Volume 4:Proposed Specifications. Final Report DOT-VNTSC-FRA-93-2.IV, March.

Edwards, W. A., and A. Tversky (1967). *Decision Making.* Penguin Books, Baltimore.

Egan, J. (1982). "To Err is Human Factors." *Technology Review* 85.

Fayada, Catherine (1992). "Methods and Strategies for Confirming the Reliability of Train Driver's Aptitudes." *The First European Congress of Railway Psychology.* Lyon, France, September 23-25.

Federici, Francois (1992). "New SNCF Computer Tests for Selection of Train Drivers." *The First European Congress of Railway Psychology.* Lyon, France, September 23-25.

Fitts, P. M. (ed.) (1951). *Human Engineering for an Effective Air-Navigation and Traffic-Control Systems.* Washington: National Research Council.

Forbes, T. W. (ed.) (1972). *Human Factors in Highway Traffic Safety Research.* Wiley-Interscience.

Friedland, Bernard (1986). *Control System Design: An Introduction to State-Space Methods.* McGraw-Hill.

Gelb, Arthur (ed.) (1974). *Applied Optimal Estimation.* MIT Press.

GRS (1979). *Elements of Railway Signaling.* General Railway Signal.

Goedken, Charles (ed.) (1985). *Highway Safety Forum.* ASCE.

Greenstein, Joel S. and Siu-Tong Lam (1985). "An Experimental Study of Dialogue-Based Communication for Dynamic Human-Computer Task Allocation." *Intl. Journal of Man-Machine Studies* 23: 605-621.

Gruire, Y. (1992). *Signalling: a High Performance Component of Railway Systems from the TVM* 300 *to the TVM* 430, Report of CSEE Transport, France.

Guilleux, Bernard (1992). "Signaling on New Lines, The Transition to the TVM 430 System." *Revue Generale Des Chemins de Fer.* Gauthier-Villars, pp. 59-65.

Guilloux, Jean-Paul (1992). "TVM430 Enhances Train Control Capacity." *Railway Gazette International,* August, pp. 515-518.

Hall, R. E., P. K. Samanta and A. L. Swoboda (1981). *Sensitivity of Risk Parameters to Human Errors in Reactor Safety Study for a PWR.* Brookhaven Natl. Lab. Rep. 51322, NUREG-CR-1879, January.

Harker, Patrick T. (1990). "Use of Advanced Train Control Systems in Scheduling and Operating Railroads: Models, Algorithms, and Applications." *Transportation Research Record* 1263:101-110.

Jordan, Nehemiah (1963). "Allocation of Function Between Man and Machines in Automated Systems." *Journal of Applied Psychology,* 47: 161-165.

Karnopp, D. and R. Rosenberg (1975). *System Dynamics: A Unified Approach.* Wiley-Interscience.

Keeney, R. L., and N. Raiffa (1976). *Decisions with Multiple Objectives: Preferences and Value Tradeoffs*. Wiley.

Kraay, David, Patrick T. Harker and Bintong Chen (1991). "Optimal Pacing of Trains in Freight Railroads: Model Formulation and Solution." *Operations Research,* Vol. 39, No. 1, January-February, pp. 82-99.

Kuehn, George (1992). *Advanced Train Control System Evaluation.* Final Report FRA-ORD-92/32, IIT Research Institute (Prepared for FRA). October.

Lowrance, William W. (1976). *Of Acceptable Risk.* Los Altos, CA: William Kaufmann, Inc.

Luedeke, Jonathan F. (1992). *Glossary of Terms,* for the Program Analytical Methodology for Safety Validation of Computer Controlled Subsystems Used in Guided Ground Transportation Systems to Volpe National Transportation Systems Center, December 18, Interim Report.

Macaire, Jean-Pierre (1991). "Selection and Monitoring of Safety Staff Aptitudes and Human Reliability" *Proc. of the International Seminar on Railway Safety at Chalfont and Latimer.* Great Britain, October 31 - November 1.

Macaire, Jean-Pierre (1992a). "The Implementation and Maintenance of Human Reliability Within the Company." *Preliminary note for the First European Congress of Railway Psychology,* Lyon, France, September 23-25.

Macaire, Jean-Pierre (1992b). "The Role of the Psychologist in a Transport Company." *The First European Congress of Railway Psychology,* Lyon, France, September 23-25.

Marshall, Gilbert (1982). *Safety Engineering.* Brooks/Cole Engineering Division.

McRuer, D., I. Ashkenas and D. Graham (1973). *Aircraft Dynamics and Automatic Control.* Princeton University Press.

Meister, D. (1971). *Human Factors: Theory and Practice.* New York: Wiley.

Norman, D.A. (1988). *The Design of Everyday Things.* Basic Books.

Ogata, Katsuhiko (1990). *Modern Control Engineering.* 2nd edition, Prentice-Hall.

Pourdieu (1992). "The Supporting and Advisory Role of the Psychology Department in Preventive and Projective Human Resource Management." *The First European Congress of Railway Psychology.* Lyon, France, September 23-25.

Price, Harold E. (1985). "The Allocation of Functions in Systems." *Human Factors,* 27(1). pp. 33-45.

Price, Harold E. and R. Pulliam (1983). "Control Room Function Allocation – A Need for Man-Computer Symbiosis." *Proceedings of the 1982 IEEE Computer Forum.* Denver, CO: Institute of Electrical and Electronics Engineers.

Rasmussen, Jens (1978). *Notes on Diagnostic Strategies in the Process Plant Environment.* Riso Natl. Lab., Rep. M-1983, Riso, Denmark.

Reason, James (1990). *Human Error.* Cambridge.

Rieger, Christine A., Joel S. Greenstein (1982). "The Allocation of Tasks Between the Human and Computer in Automated Systems." *Proc. of IEEE 1982 Intl. Conf. On Cybernetics and Society,* New York.

Rodgers, William P. (1971). *Introduction to System Safety Engineering.* New York: John Wiley and Sons, Inc.

Rouse, W. B., and R. M. Hunt (1984). "Human Problem Solving in Fault Diagnosis Tasks." in Rouse, W. B., *Advances in Man-Machine Systems Research,* Vol. 1:195-222, Greenwich, CT:JAI Press.

Salvendy, Gavriel (ed.) (1987). *Handbook of Human Factors.* Wiley-Interscience.

Sanders, Mark S. and Ernest J. McCormick (1987). *Human Factors in Engineering and Design.* 6th Edition, McGraw-Hill Publishing Company.

Senders, J.W. and N.P. Moray (1991). *Human Error: Cause, Prediction and Reduction.* Erlbaum.

Sheridan, Thomas, and W. Ferrell (1974). *Man-Machine Systems.* MIT Press.

Sheridan, Thomas (1992). *Telerobotics, Automation, and Supervisory Control.* MIT Press.

Stammer, Robert (ed.) (1988). *Highway Safety: At the Crossroads.* ASCE.

Starr, C. (1969). "Societal Benefits vs. Technological Risk." *Science,* 165:1232-1238.

Sussman, E. Donald (1993). "Human Roles in Automated High Speed Passenger Systems." Internal memo, Volpe National Transportation Systems Center.

Swain, A. D. and H. E. Guttman (1983). *Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications.* Sandia Natl. Labs., NUREG CR-1278, Washington, D.C.: U.S. Nuclear Regulatory Commission.

The French Railway Review (1992). "In the Driver's Cab With a TGV Driver." *Revue Generale Des Chemins de Fer, A Decade of TGV Operation.* Gauthier-Villars, pp. 79-81.

Tversky, A., and D. Kahneman (1981). "The Framing of Decisions and the Psychology of Choice." *Science,* 211: 453-458.

Von Neumann, J. and O. Morganstern (1944). *Theory of Games and Economic Behavior.* Princeton University Press.

Wiener, E., and D. Nagel (ed.) (1988). ***Human Factors in Aviation.*** Academic Press.

Yin, Shumei and Thomas B. Sheridan (1994). **"An** Optimal Driving Aid for High-Speed Train Speed Control." ***Proc.*** 1994 ***Transportation Research Board Annual Conference.*** Washington D.C.