

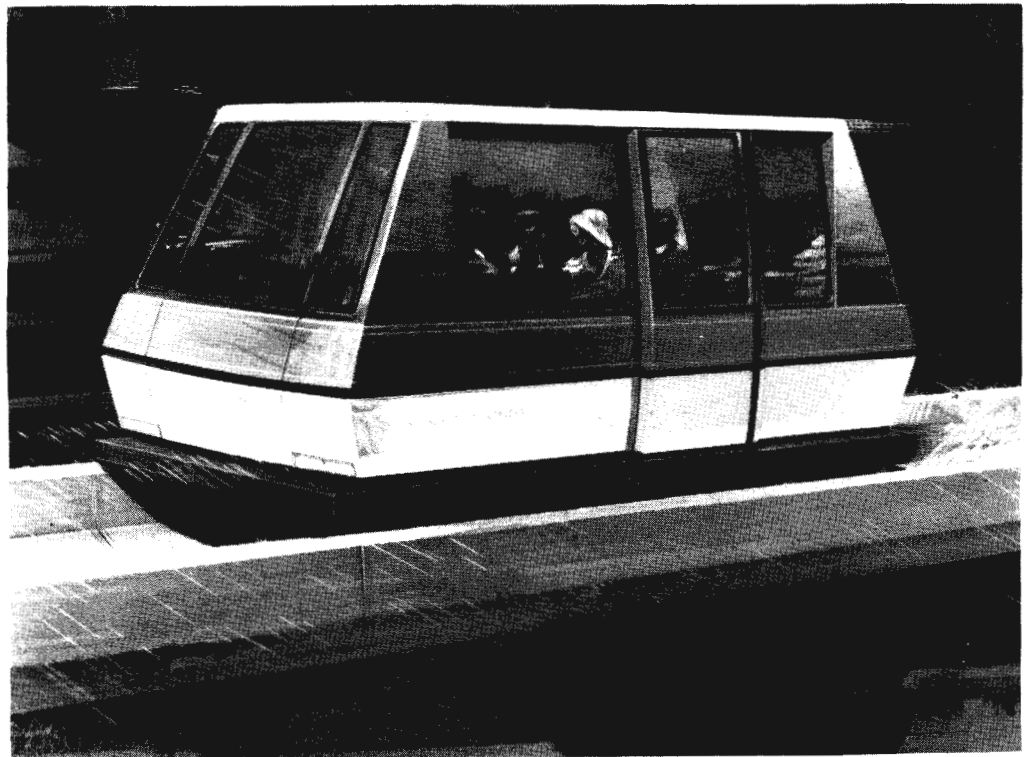
UMTA-WA-06-0011-86-1

Advanced Group Rapid Transit Phase IIB Executive Summary & Final Report

Don D. Lyttle
Dave B. Freitag
Doug H. Christenson

SCIENCE LIBRARY

FINAL REPORT
MARCH, 1986



U.S. Department
of Transportation

**Urban Mass
Transportation
Administration**

TA
1207
.L97
1986

NOTICE

The United States Government does not endorse products or manufacturers. Trade or manufacturer's names appear herein solely because they are considered essential to the object of this report.

NOTICE

This document is disseminated under the sponsorship of the Department of Transportation in the interest of information exchange. The United States Government assumes no liability for the contents or use thereof.

1. Report No. UMTA-WA-06-0011-86-1		2. Government Accession No.		3. Recipient's Catalog No.	
4. Title and Subtitle AGRT PHASE IIB EXECUTIVE SUMMARY AND FINAL REPORT				5. Report Date FEBRUARY 1986	
				6. Performing Organization Code	
7. Author(s) D. D. Lyttle, D.B. Freitag, D.H. Christenson				8. Performing Organization Report No.	
9. Performing Organization Name and Address BOEING AEROSPACE COMPANY Automated Transportation Systems P.O. Box 3999 Seattle, Washington 98124				10. Work Unit No. (TRAIS)	
				11. Contract or Grant No. DOT-UT-80041	
12. Sponsoring Agency Name and Address U.S. Department of Transportation Urban Mass Transportation Administration 400 Seventh Street, S.W. Washington, D. C. 20590				13. Type of Report and Period Covered FINAL REPORT 1978 - 1986	
				14. Sponsoring Agency Code URT-12	
15. Supplementary Notes					
16. Abstract This report summarizes the work performed during the AGRT Phase IIB Program, Contract DOT-UT-80041. Attainment of a three second headway control system which meets "Brickwall" stop safety requirements is noted. Derivation of critical technology through the application of System Engineering and System Management Methodology is described. Derived technology for partial automation of existing transit functions is noted. A technology base for the potential development of more fully automated systems to further enhance surface transportation productivity is documented.					
17. Key Words Automated Transit, Command and Control, Collision Avoidance System, Vehicle Longitudinal Control, Fail-Safe, Checked-Redundant, Safe-Life			18. Distribution Statement Available to the public through the National Technical Information Service Springfield, Virginia 22161		
19. Security Classif. (of this report) Unclassified		20. Security Classif. (of this page) Unclassified		21. No. of Pages 205	22. Price

FOREWORD

TA
1207
.L97
1986

This report summarizes the work completed by Boeing Aerospace Company under the Advanced Group Rapid Response (AGRT) Contract, DOT-UT-80041. The results of this research are being made available to the transit community in the interest of information exchange without charge. We direct this writing to those professionals engaged in the managerial, operations, and maintenance activities of the transit community.

We have two goals in presenting this work. One, to provide an insight into this developing technology, and to describe our method of managing the technology and resources in the context of reaching for Automated Guideway Transit goals established by the AGRT contract.

Two, to identify resulting critical technologies that may be adaptable to existing transit operational, maintenance, and management functions to lower operational costs, improve reliability, and enhance productivity.

We regard this report as a starting point rather than an ending. The methods and technology we describe here are mature, available, and have been proven in many diverse applications. Given closer ties between the research and transit communities, the work accomplished and the lessons learned on the AGRT Contract will bear fruit.

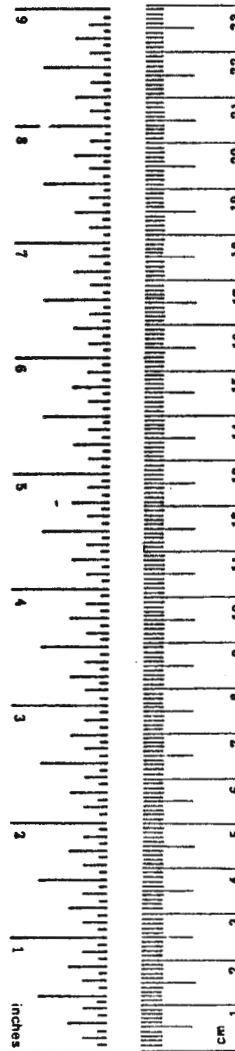
METRIC CONVERSION FACTORS

Approximate Conversions to Metric Measures

Symbol	When You Know	Multiply by	To Find	Symbol
LENGTH				
in	inches	*2.5	centimeters	cm
ft	feet	30	centimeters	cm
yd	yards	0.9	meters	m
mi	miles	1.6	kilometers	km
AREA				
in ²	square inches	6.5	square centimeters	cm ²
ft ²	square feet	0.09	square meters	m ²
yd ²	square yards	0.8	square meters	m ²
mi ²	square miles	2.6	square kilometers	km ²
	acres	0.4	hectares	ha
MASS (weight)				
oz	ounces	28	grams	g
lb	pounds	0.45	kilograms	kg
	short tons (2000 lb)	0.9	tonnes	t
VOLUME				
tsp	teaspoons	5	milliliters	ml
Tbsp	tablespoons	15	milliliters	ml
fl oz	fluid ounces	30	milliliters	ml
c	cups	0.24	liters	l
pt	pints	0.47	liters	l
qt	quarts	0.95	liters	l
gal	gallons	3.8	liters	l
ft ³	cubic feet	0.03	cubic meters	m ³
yd ³	cubic yards	0.76	cubic meters	m ³
TEMPERATURE (exact)				
°F	Fahrenheit temperature	5/9 (after subtracting 32)	Celsius temperature	°C

Approximate Conversions from Metric Measures

Symbol	When You Know	Multiply by	To Find	Symbol
LENGTH				
mm	millimeters	0.04	inches	in
cm	centimeters	0.4	inches	in
m	meters	3.3	feet	ft
m	meters	1.1	yards	yd
km	kilometers	0.6	miles	mi
AREA				
cm ²	square centimeters	0.16	square inches	in ²
m ²	square meters	1.2	square yards	yd ²
km ²	square kilometers	0.4	square miles	mi ²
ha	hectares (10,000 m ²)	2.5	acres	
MASS (weight)				
g	grams	0.035	ounces	oz
kg	kilograms	2.2	pounds	lb
t	tonnes (1000 kg)	1.1	short tons	
VOLUME				
ml	milliliters	0.03	fluid ounces	fl oz
l	liters	2.1	pints	pt
l	liters	1.06	quarts	qt
l	liters	0.26	gallons	gal
m ³	cubic meters	35	cubic feet	ft ³
m ³	cubic meters	1.3	cubic yards	yd ³
TEMPERATURE (exact)				
°C	Celsius temperature	9/5 (then add 32)	Fahrenheit temperature	°F



*1 in = 2.54 (exactly). For other exact conversions and more detailed tables, see NBS Misc. Publ. 286, Units of Weights and Measures, Price \$2.25, SD Catalog No. C13.10-286.

AGRT EXECUTIVE SUMMARY REPORT

TABLE OF CONTENTS

<u>SECTION</u>		<u>PAGE</u>
	FOREWORD	ii
1.0	EXECUTIVE SUMMARY	1
2.0	INTRODUCTION	3
3.0	PROGRAM SUMMARY AND RESULTS	11
3.1	VEHICLE CONTROL UNIT (VCU) DESIGN SUMMARY AND RESULTS	21
3.2	GUIDEWAY COMMUNICATION UNIT (GCU) DESIGN SUMMARY AND RESULTS	33
3.3	ODOMETER DATA DOWNLINK COLLISION AVOIDANCE SYSTEM (ODDCAS) DESIGN SUMMARY AND RESULTS	41
4.0	SYSTEM AND SUBSYSTEM OVERVIEW	45
4.1	SYSTEM MANAGEMENT-SYSTEM ENGINEERING-METHODOLOGY	46
4.2	SYSTEM DESIGN OVERVIEW	70
4.3	SUBSYSTEM DESIGN OVERVIEW	79
5.0	PROGRAM AND SAFETY REVIEWS AND TECHNICAL INTERCHANGES	103
5.1	PROGRAM REVIEWS	105
5.2	SAFETY REVIEWS	118
5.3	TECHNICAL INTERCHANGES	124
6.0	SYSTEM AND DESIGN REVIEWS	130
6.1	SYSTEM DESIGN REVIEW	131
6.2	PRELIMINARY DESIGN REVIEWS	136
6.3	CRITICAL DESIGN REVIEWS	149
7.0	BRASSBOARD FABRICATION, DEVELOPMENT TESTING AND VCU VERIFICATION TESTING	161
8.0	SIGNIFICANCE OF TECHNICAL ACHIEVEMENTS	192
8.1	SIGNIFICANCE TO EXISTING TRANSIT SYSTEMS	193
8.2	SIGNIFICANCE TO NEW SYSTEMS	196
9.0	CONCLUSIONS	198
10.0	REFERENCES	200

**AGRT EXECUTIVE SUMMARY REPORT
LIST OF FIGURES**

<u>SECTION</u>	<u>PAGE</u>	
2.0-1	HISTORY OF GOVERNMENT EXPENDITURES FOR PUBLIC TRANSIT	6
2.0-2	AGRT SYSTEM OVERVIEW	7
2.0-3	MPM PHASE I EXPERIENCE, PHASE II GUARANTEED PERFORMANCE	9
2.0-4	MORGANTOWN SYSTEM AVAILABILITY HISTORY PHASE II	9
3.0-1	AGRT-EDS-C ³ SCHEDULE	13
3.0-2	AGRT-EDS COMMAND AND CONTROL (C&CS) HIERARCHY	14
3.0-3	AGRT ENGINEERING DEVELOPMENT SPECIFICATION	18
3.0-4	AGRT-EDS COMMAND & CONTROL HIERARCHY (STATUS)	19
3.1-1	AGRT-FINAL SYSTEM SAFETY REVIEW - SCOPE	22
3.1-2	AGRT-FINAL SYSTEM SAFETY REVIEW - (VCU DESIGN VERIFICATION PROCESS)	23
3.1-3	AGRT-FINAL SYSTEM SAFETY REVIEW - (BACKGROUND)	24
3.1-4	AGRT-FINAL SYSTEM SAFETY REVIEW - (INITIAL SYSTEM SAFETY REVIEW)	24
3.1-5	AGRT-FINAL SYSTEM SAFETY REVIEW - SAFETY DESIGN PRINCIPLES	26
3.1-6	AGRT-FINAL SYSTEM SAFETY REVIEW - DEFINITION OF SAFETY TERMINOLOGY	27
3.1-7	AGRT-FINAL SYSTEM SAFETY REVIEW - CATEGORIZATION OF FAILURE RELATING TO HIGH TECHNOLOGY	27
3.1-8	VCU SAFETY HIERARCHY	29
3.2-1	GCU CHECKED REDUNDANT CONFIGURATION	35
3.2-2	ODDCAS CHECKED REDUNDANT CONFIGURATION FOR CAS	35
3.2-3	GCU CHECKED REDUNDANT SPEED LIMIT CHECKER CONFIGURATION	35
3.2-4	SPEED LIMIT CHECKER SOFTWARE STRUCTURE	39
3.2-5	SPEED LIMIT CHECKER PROCESSING TIMING	39
3.3-1	ODDCAS SAFETY CONCEPT	43
4.1-1	AGRT-WORK BREAKDOWN STRUCTURE	47
4.1.2	AGRT-DEVELOPMENTAL PROGRAM METHODOLOGY-ROADMAP	49

AGRT EXECUTIVE SUMMARY REPORT
LIST OF FIGURES (continued)

<u>SECTION</u>	<u>PAGE</u>	
4.1-3	RELATIONSHIP BASELINE PROGRESSION TO MAJOR REVIEWS	52
4.1-4	SIMULATION ENSEMBLE SUMMARY	55
4.1-5	ANALYSIS TOOLS	57
4.1-6	BOEING AEROSPACE Co. (BAC) SYSTEMS APPROACH	59
4.1-7	BAC SYSTEM APPROACH - ULTIMATE GOALS	59
4.1-8	BOEING AGRT DESIGN PROCESS	62
4.1-9	DEVELOPMENT OF SYSTEM SAFETY	63
4.1-10	AGRT FUNCTION TREE	63
4.1-11	CHANNEL-MTBUF RELATION TO CHECK TIME	66
4.1-12	VCU CHECKED REDUNDANT DESIGN - TIME BETWEEN CHECKS	66
4.2-1	OPERATIONAL COMMAND AND CONTROL SYSTEM STRUCTURE	72
4.2-2	FLEET MANAGEMENT (QUASI SYNCHRONOUS)	75
4.3-1	EDS BASELINE SOFTWARE	81
4.3-2	EDS C&CS HARDWARE BASELINE	82
4.3-3	ODDCAS AT NON-INTERSECTION AREA	85
4.3-4	ODDCAS AT MERGE AREA	85
4.3-5	ODDCAS AT DIVERGE AREA	85
4.3-6	VEHICLE COMMAND AND CONTROL BLOCK DIAGRAM	87
4.3-7	VEHICLE CONTROL ELECTRONIC INTERFACES	89
4.3-8	VEHICLE LOAD AND DISPATCH	91
4.3-9	VEHICLE CONTROL THROUGH A MERGE	93
4.3-10	VEHICLE STATION ARRIVAL	95
4.3-11	EDS BASELINE COMMAND AND CONTROL SYSTEM - SYSTEM TRANSACTION	99
5.1-1	FIRST QUARTERLY REVIEW - TASK 6A SYSTEM SPECIFICATION	106
5.1-2	FIRST QUARTERLY REVIEW - AGRT UPLINK DRIVER	107
5.1-3	AGRT QUARTERLY REVIEW - FEBRUARY 14, 1980 AGENDA	109
5.1-4	AGRT QUARTERLY REVIEW - JULY 2, 1980 - HALL EFFECT	111

AGRT EXECUTIVE SUMMARY REPORT
LIST OF FIGURES (continued)

<u>SECTION</u>	<u>PAGE</u>	
5.1-5	AGRT QUARTERLY REVIEW - SEPTEMBER 22, 1980 - CC&S TRADES	113
5.1-6	AGRT PROGRAM OVERVIEW - MAY 20, 1983 - LCS ANALYSIS	115
5.1-7	AGRT/MAG-LEV PROGRAM REVIEW - OVERVIEW OF VLCS HYBRID SIMULATION	116
5.2-1	VEHICLE SEPARATION ASSURANCE SYSTEM REVIEW - DECEMBER 2, 1981 SAFETY REQUIREMENTS - SENSOR SIGNAL SELECTION	121
5.2-2	SYSTEM SAFETY REVIEW - OCTOBER 5, 1982 - SAFETY SYSTEM REQUIREMENT	122
5.2-3	FINAL SAFETY REVIEW - SEPTEMBER 16, 1984 - DATA PACKAGE	123
5.3-1	TECHNICAL INTERCHANGE - SAFETY PHILOSOPHY OF DESIGN	126
5.3-2	TECHNICAL INTERCHANGE MINUTES - OCTOBER 30 & 31, 1980	128
5.3-3	TECHNICAL INTERCHANGE - CAS ALTERNATIVE CONCEPT EVALUATION TABLES	129
6.1-1	AGRT - SDR/QUARTERLY REVIEW DATA PACKAGE AND AGENDA	133
6.1-2	SECOND SDR - MAJOR AGRT/EDS REQUIREMENTS - SAFETY	134
6.1-3	DESIGN VERIFICATION TEST MATRIX MAJOR CATEGORIES - AS PRESENTED IN VCU DESIGN VERIFICATION TEST PLAN	134
6.2-1	TEST TRACK SOFTWARE AND VCU PDR DATA PACKAGE AND AGENDA	137
6.2-2	TEST TRACK SOFTWARE AND VCU PDR ACTION ITEM CLOSURES	139
6.2-3	VEHICLE/PROPULSION/BRAKE AMP/MODU PDR AGENDA - TESTS TRADE STUDIES	142
6.2-4	GCCS PDR - REQUIREMENTS FLOW DOWN	144
6.2-5	GCCS PDR OUTLINE	144
6.2-6	GCCS ACTION ITEM CLOSURE	146
6.2-7	ODDCAS PDR DATA PACKAGE	148

AGRT EXECUTIVE SUMMARY REPORT
LIST OF FIGURES (continued)

<u>SECTION</u>	<u>PAGE</u>	
6.3-1	TEST TRACK S/W CDR - EDS DEVELOPMENT SUMMARY	150
6.3-2	TEST TRACK S/W CDR - EXAMPLE OF ALLOCATION PROCESS	151
6.3-3	VCU - CDR - DATA PACKAGE	153
6.3-4	GCU CDR - DATA PACKAGE	156
6.3-5	ODDCAS CDR AGENDA	159
7.0-1	ODDCAS TESTING CATEGORIES	163
7.0-2	ODDCAS GCU SINGLE-THREAD TEST	163
7.0-3	ODDCAS VEHICLE EQUIPMENT	166
7.0-4	ODDCAS WAYSIDE EQUIPMENT	168
7.0-5	ODDCAS WAYSIDE TEST CONFIGURATION	169
7.0-6	CHECKED DUAL REDUNDANT VCU	171
7.0-7	SIMPLIFIED BLOCK DIAGRAM OF VCU ELECTRONICS	172
7.0-8	VCU ASSEMBLY DRAWING	174
7.0-9	SYMMETRICAL DUAL-DISSIMILAR SOFTWARE WITH REDUNDANT SOFTWARE DISPARITY CHECK LOGIC	175
7.0-10	DESIGN VERIFICATION TEST CONFIGURATION	180
7.0-11	TEST ARTICLE & TSG	181
7.0-12	TEST VEHICLE SIMULATOR	181
7.0-13	VCU TEST RACK ASSEMBLY DRAWING	183
7.0-14	VCU TEST SET DRAWING TREE	184

LIST OF TABLES

<u>NO.</u>		
1	VEHICLE POSITION REGULATION REQUIREMENTS	78
2	FAILURE MANAGEMENT FUNCTIONS AT TEST TRACK	97
3	TEST TRACK MAJOR FEATURES	102
4	VCU TEST PROGRAM OVERVIEW	186

1.0 EXECUTIVE SUMMARY

This summary and the detailed reports noted below document a developing technology supporting advanced Automated Guideway Transit. The Advanced Group Rapid Transit program summarized in this report focuses on the identification and implementation of the critical technologies required to safely command and control the movement of unmanned vehicles along a guideway.

The AGRT's Command and Control System, which incorporates the critical technologies, safely controls the movement of vehicles within extremely short three-second headways. This capability to control the movement of vehicles within short headways met initial program goals and was substantiated utilizing an elaborate test set that exercised the final program hardware and software.

Numerous innovative design features have evolved during the development of this system that could be utilized in many areas of the existing transportation industry. Transfer of the technology, through cooperative efforts of the research and transit communities, into existing and new transit systems will enhance system efficiency and mitigate the transit subsidy trendline.

This report is organized to provide the reader an insight into the management and development of this technology. A history of the program and its dependency on earlier developed and implemented technology is provided. The identification and description of the critical technologies incorporated into the Command and Control System follows. Key issues and goals are documented as defined by the Urban Mass Transportation Administration for the introduction of microprocessor-based control systems.

The attainment of these goals is summarized. Emphasis is given to safety of the checked redundant microprocessor-based Command and Control

System. Possible applications of specific derivatives of this technology to existing and potential transit systems are noted. A more definitive explanation of these subsystems incorporating the critical technologies is provided in the following sections. The detailed reports noted below, provide comprehensive design, development, and test data:

Vehicle Control Unit (VCU) - Final Report (reference 43)

Guideway Communication Unit (GCU) - Final report (reference 41)

Odometer Data Downlink Collision Avoidance System - Final Report (reference 42)

The analytical phase of the program that established the AGRT system and safety requirements is described in the context of applying (and explaining) system management and system engineering methods. Specific tools are described that could conceivably be used in existing transit applications. These include Failure Modes and Effects Analysis (FMEA), Fault Tree/Probability Analysis (circuit, timing, and error analysis), and quantitative safety analysis.

Summary conclusions detailed in Section 9.0 are noted as follows:

- 1) The technology developed supports the partial automation of existing systems and more complete automation of new systems.
- 2) Long range research and development directed to implementation of the technology to enhance transit efficiency and productivity should be continued.
- 3) Safety and evaluation standards for implementation of microprocessor based control systems are required.
- 4) A steering action group directed to monitor the implementation of automation to enhance transit system productivity is recommended.

2.0 INTRODUCTION

This report Summarizes the Advanced Group Rapid Transit (AGRT) Phase II-B Program including an overview of the system and its components, results of the program, significance of the technical achievements, and the safety, economic, and dependability features of the system.

A list of related reference material is contained in section 10.0. The reader is encouraged to obtain the referenced material that may be of interest. All the documented studies listed are available to the U.S. public through the National Technical Information Service, Springfield, Virginia, 22161. Papers can be found in the documentation of the various professional conferences as noted in the references.

EARLY HISTORY AND GOALS

Boeing began independent studies of AGT Systems as early as 1962 but the main effort was initiated in May 1971 when we were placed under contract to UMTA for design, fabrication, and test of the Morgantown People Mover (MPM) Vehicle subsystem. Subsequently, in August 1971 we became system manager for the Morgantown System. Extensive studies and analyses of Automated Guideway Technology being developed by Western Germany, France, England, and Japan were undertaken. A strong organizational team was in place to support the AGRT program.

The AGRT program historical roots date back to the Department of Transportation (DOT) sponsored Transpo 72, a transportation exposition at Dulles Airport in Washington, D.C. The AGRT program (initially called High Performance Personal Rapid Transit) goals as stated by DOT-UMTA were twofold:

One, to develop the technology of automated command and control, safety protection, and communication systems that could provide a significant increase in the flexibility, efficiency, and productivity of transit operation as compared to conventional bus and rail operations.

Two, to integrate these advances into a prototype system so that the technology could be demonstrated to the industry in an operational setting.

Performance goals were to provide dispersed origin-destination service for medium density urban areas. To achieve this, the system would operate a large fleet of vehicles over an extensive guideway network, with peak line capacity in excess of 14,000 seated passengers per lane per hour in 12 passenger vehicles. The combination of vehicle size and line capacity dictated operating at headways as low as three seconds. (In contrast, we had designed Morgantown to operate at 15 second headways.)

AGRT - PHASE I - PHASE IIA

Initially, AGRT was a two-phase development program with three prime contractors: the Boeing Company, the Otis Elevator Company, and Rohr Industries. Phase II was originally intended as a full scale prototype development by one contractor selected from the original three. After the completion of Phase I however, a decision was made to split Phase II into two parts. All three contractors continued work on their separate design approaches in Phase II-A, but this phase was constrained to design refinements and laboratory testing of selected key hardware and software elements. At the completion of Phase II-A Rohr Industries Inc. withdrew from the program. Rohr then signed a licensing agreement with the Boeing Company granting rights to their integrated magnetic propulsion and suspension technology (subsequently designated Mag-Lev).

PHASE IIB

The thrust for the AGRT Phase II-B follow-on program was noted in the proceedings of the conference on Automated Guideway Transit Technology, February 28-March 2, 1978 (1). The conference chairman, at that time the Associate Administrator for Technology Development and Deployment, Urban Mass Transportation Administration, stated: "We are in the AGT business because these systems do hold out the promise of being able to pay for their operating and maintenance costs out of the fare box.

Because of that, I believe it is worthwhile for the Government and Industry to pursue this kind of alternative, not as a cure-all, not as a substitute, but as a complement to existing transportation systems."

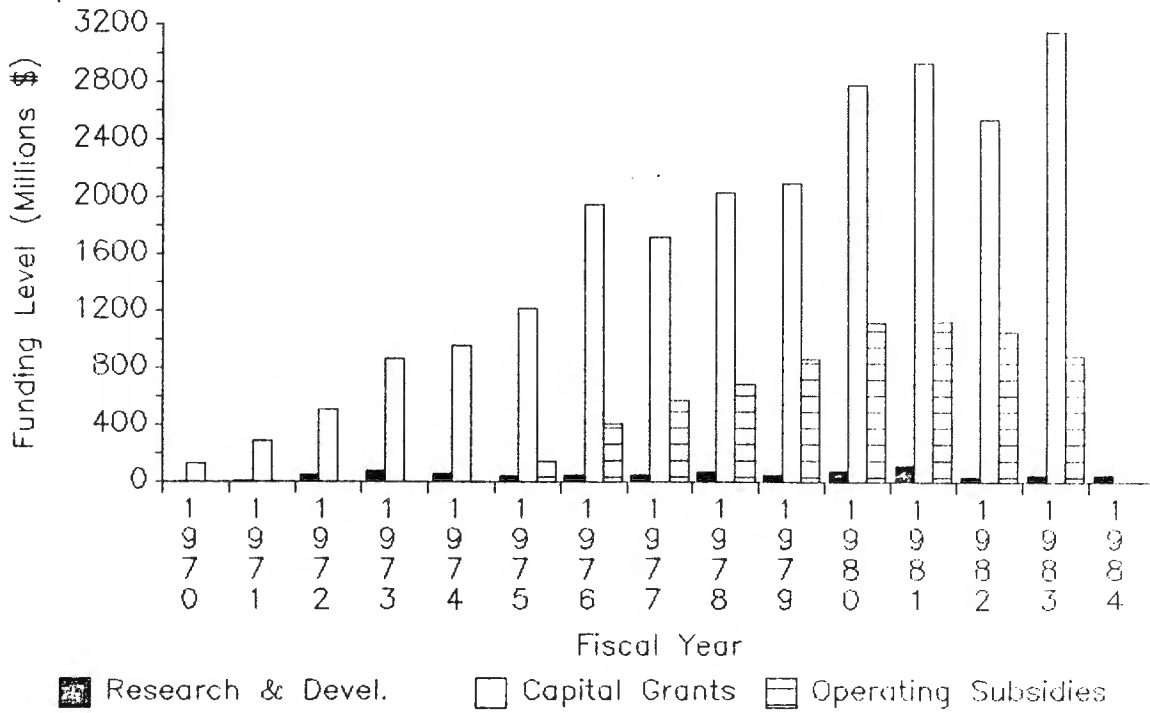
AGT research and development was further supported by studies and reports undertaken by the Office of Technology Assessment (OTA). One extensive study on Automated Guideway Transit was documented May 1975 at the request of the Senate Committee on Appropriations Transportation (2). Another extensive assessment report on AGRT (including Mag-Lev) was documented January 1980 at the request of the House Committee on Appropriations (3).

Figure 2.0-1 summarizes spending for Capital Grants, Operations and Maintenance (O&M), and Research and Development (R&D). This data emphasized the need for R&D, such as AGRT, to reduce and eventually eliminate operating and maintenance subsidies (4).

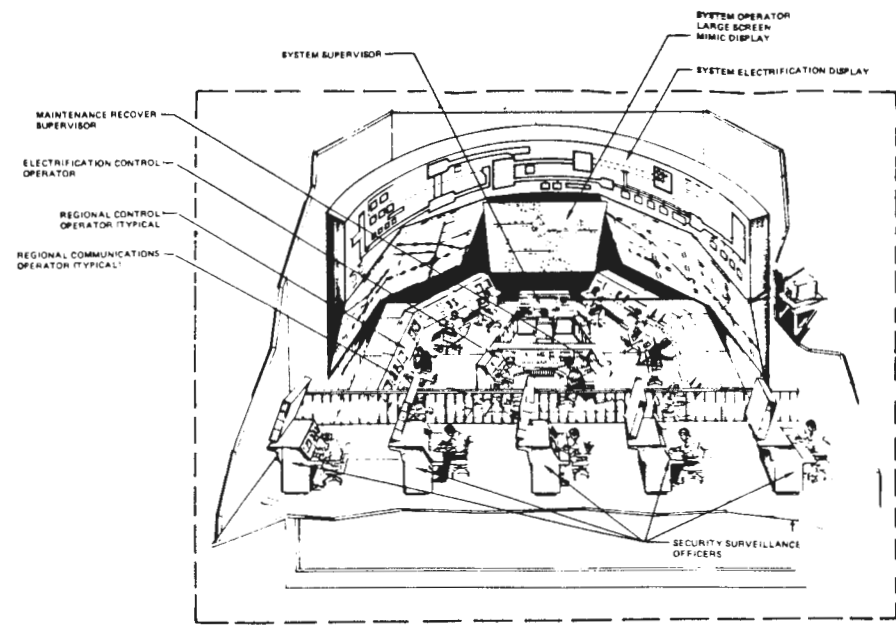
AGRT - TECHNOLOGY BASE

The AGRT Phase II-A studies and the Phase II-B proposal extended the technology developed and implemented on the Morgantown People Mover (MPM). Our use of the MPM system as a viable research and development test bed is well illustrated in the design of the AGRT Command and Control System (C&CS). The MPM vehicle management sub-system is centrally synchronous--that is, the position of all vehicles is known at all times at central control and they move in synchronism determined by central control. This system established a practical limit on the number of vehicles that can be so controlled. The AGRT C&CS decentralizes control so that vehicle control is delegated to the local control level; central performs only the supervisory functions that do not interact with the vehicle in real time. The local control system is thus a logical system module which can be replicated as needed in expanding the system incrementally. Our proposed AGRT/EDS System is shown in Figure 2.0-2.

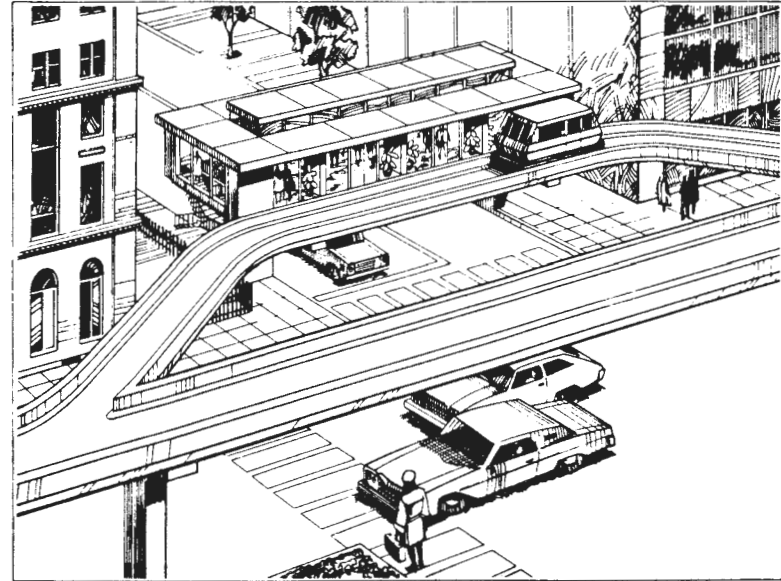
History of Government Expenditures
for Public Transit
Figure 2.0-1



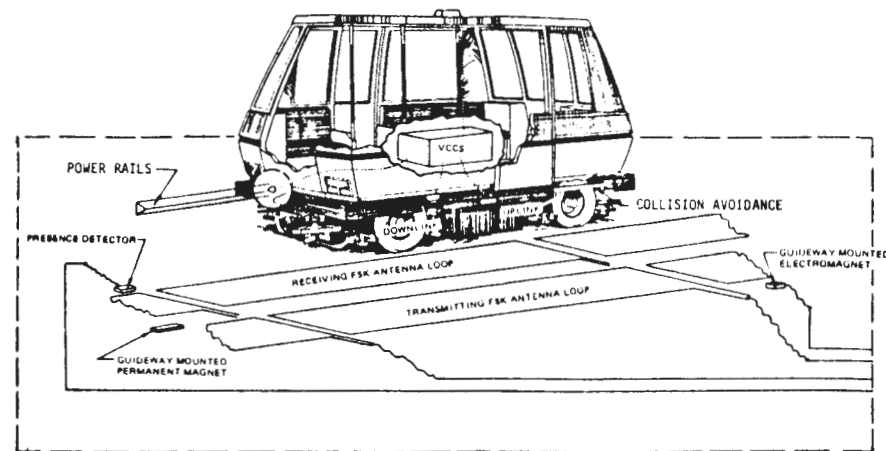
Data from APTA Transit Fact Book 1985
and DOT Appropriation Data



URBAN CENTRAL CONTROL



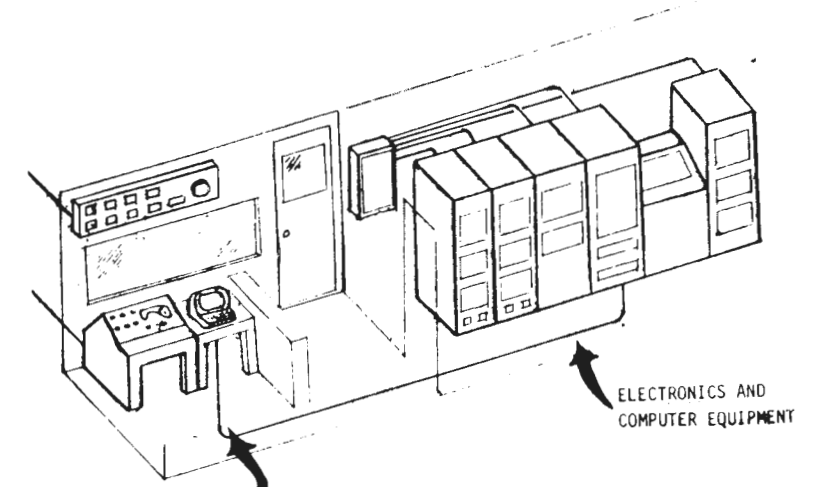
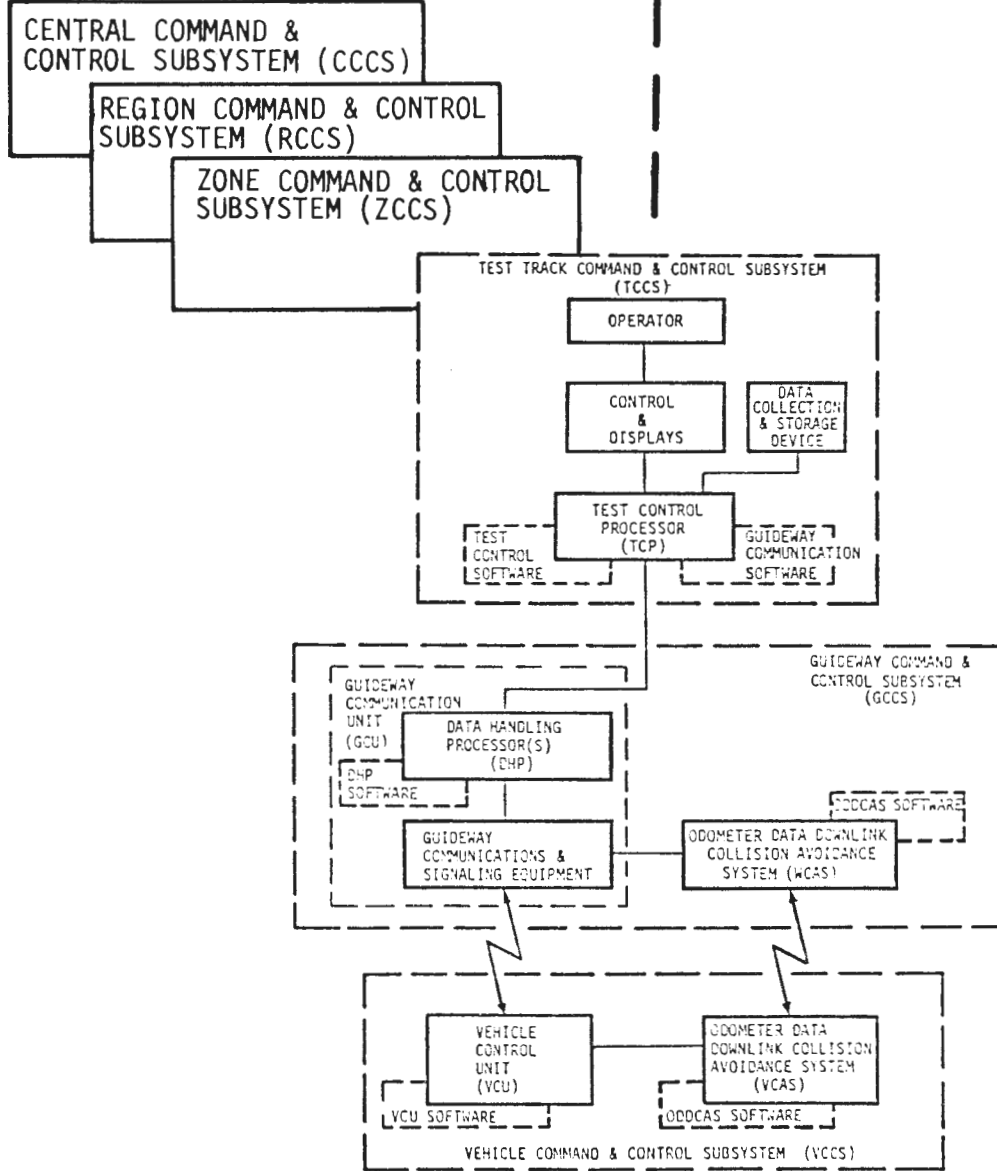
URBAN STATION



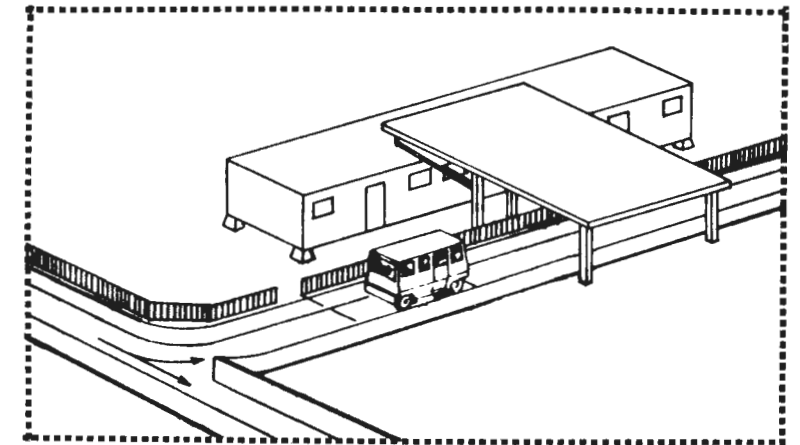
GUIDEWAY CONTROL ELEMENTS

URBAN DEPLOYED SYSTEM

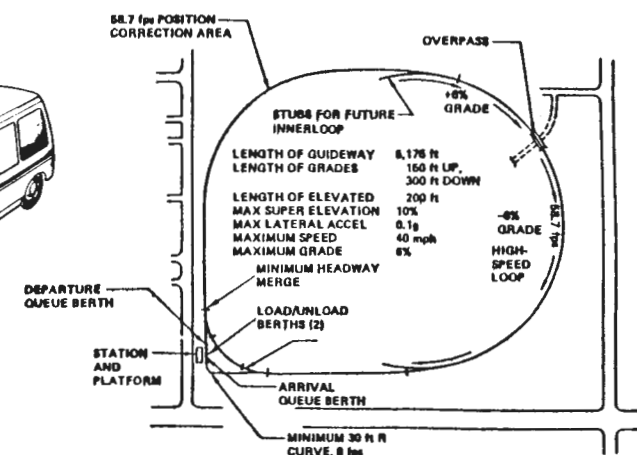
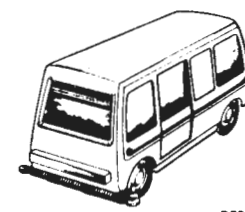
ENGINEERING DEVELOPMENT SYSTEM (EDS)



EDS CENTRAL CONTROL



EDS STATION



EDS TEST TRACK

THIS PAGE INTENTIONALLY LEFT BLANK.

FIGURE 2.0-3

MPM PHASE I EXPERIENCE, PHASE II GUARANTEED PERFORMANCE

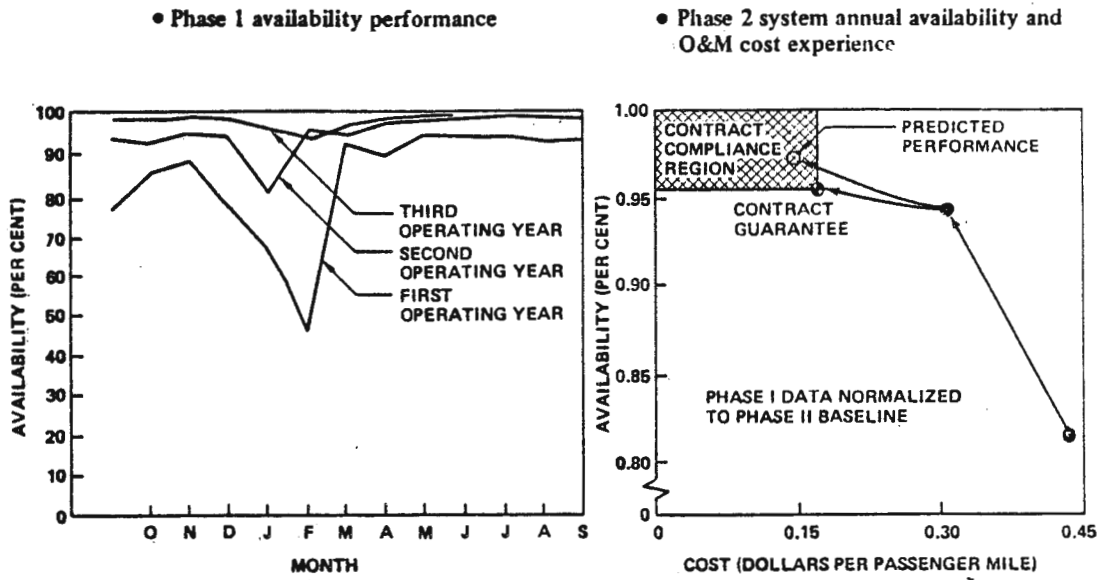
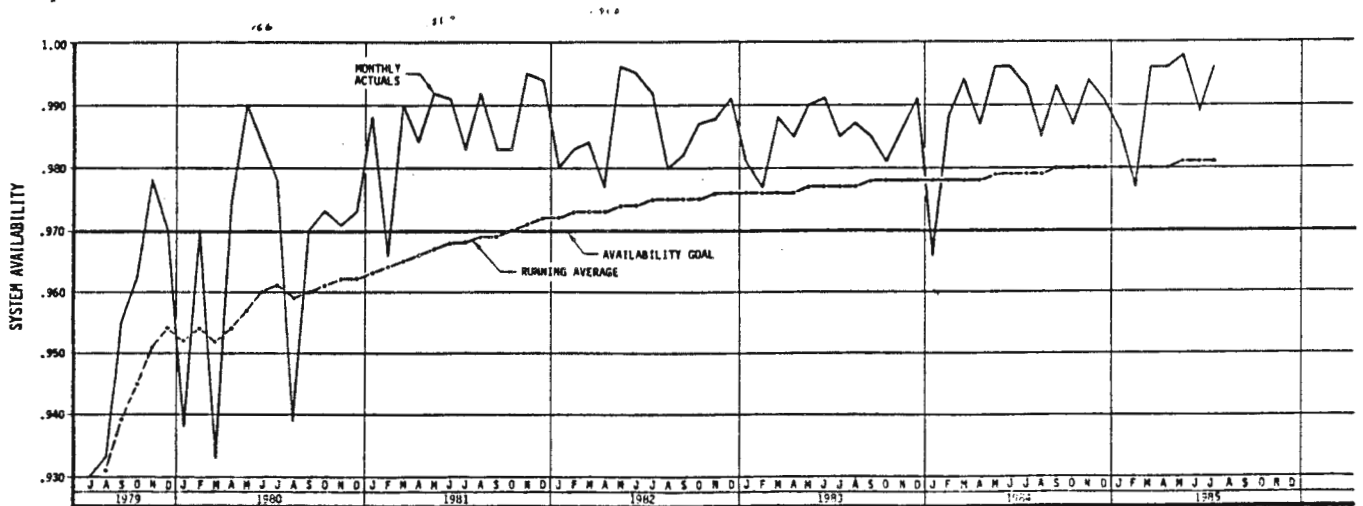


FIGURE 2.0-4

MORGANTOWN SYSTEM AVAILABILITY HISTORY PHASE II



PASSENGERS CARRIED..... 22 MILLION
 FLEET MILEAGE..... 6 MILLION

(DATA PROVIDED BY WEST VIRGINIA UNIVERSITY)

3.0 PROGRAM SUMMARY AND RESULTS

This section provides a summary and results of the technology derived from the AGRT-EDS program. This program established the feasibility of microprocessor-based control systems for general application to urban mass transit. This control system was incorporated in the AGRT-EDS subsystem identified as the Command and Control System (C&CS).

To assist the reader in understanding the material, we provide a brief introduction to the nomenclature abbreviations and acronyms used to identify functional elements of the AGRT-EDS system. This is followed by an outline of the major AGRT-EDS subsystems encompassing the critical technologies. The outline is intended to provide the reader with an insight into the critical technologies in the context of their development in the AGRT-EDS system.

ABBREVIATIONS and ACRONYMS

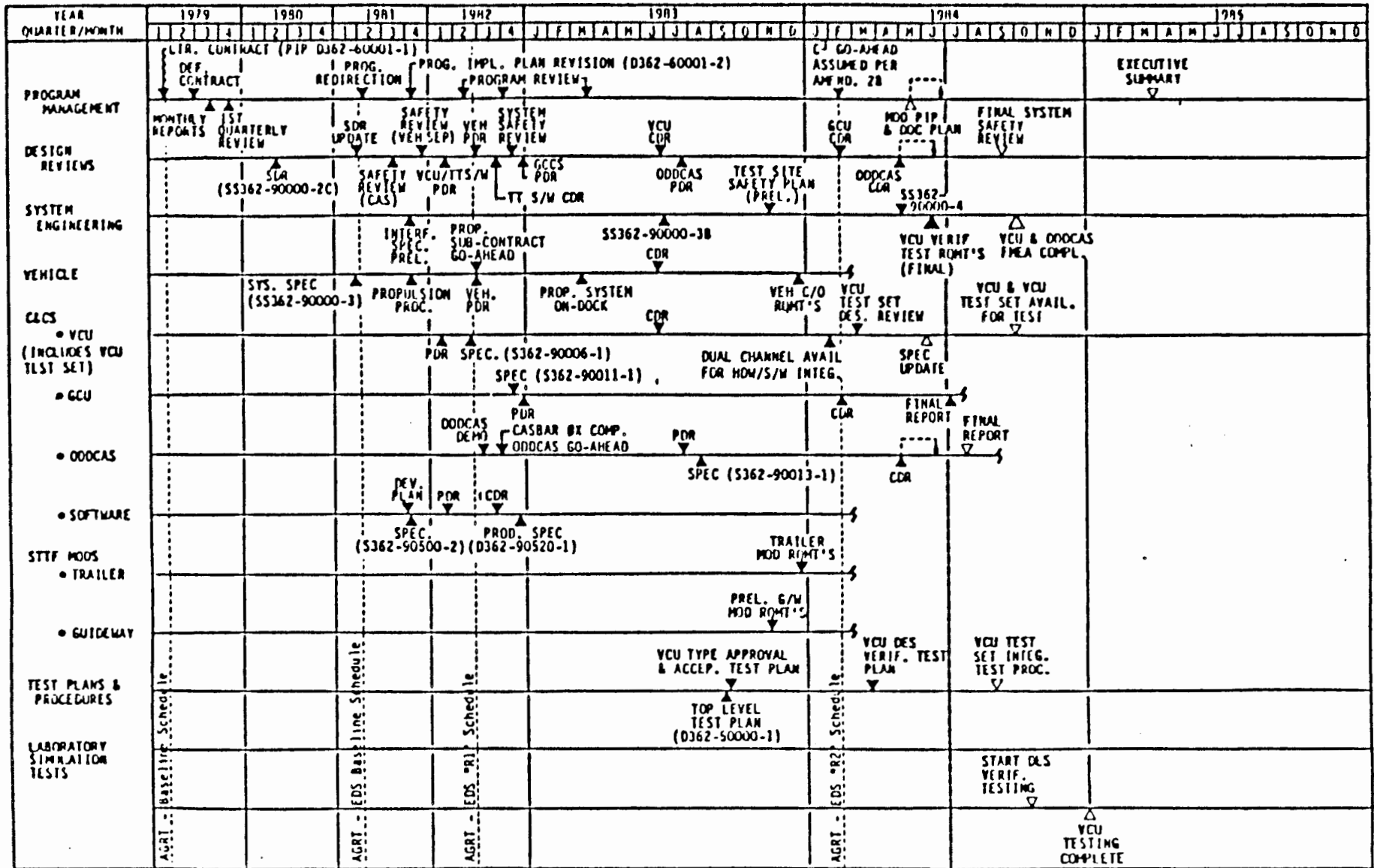
The critical technology is incorporated into two critical elements of the AGRT-EDS identified as the Longitudinal Control System (LCS) and the Collision Avoidance System (CAS). The LCS and CAS are functionally incorporated into the AGRT-EDS Command and Control System (C&CS). The AGRT-EDS C&CS is composed of a Test Track Command & Control Subsystem (TCCS), a Guideway Command & Control Subsystem (GCCS), and a Vehicle Command & Control Subsystem (VCCS).

In turn, the GCCS is composed of the Guideway Communication Unit (GCU) and the Odometer Data Downlink Collision Avoidance System (ODDCAS) - Wayside Collision Avoidance System (WCAS). The VCCS encompasses the Vehicle Control Unit (VCU) and the ODDCAS-Vehicle Collision Avoidance System (VCAS).

System Design Reviews (SDR) are formal technical reviews, providing approval of the system specification and establishment of the functional baseline. Preliminary Design Reviews (PDR) are technical reviews on contract configuration items, i.e., VCCS, which approve subsystem specifications establishing the allocated baseline and authorize start of

FIGURE 3.0-1

AGRT-ENGINEERING DEVELOPMENT SYSTEM-COMMAND, CONTROL, AND COMMUNICATIONS - C³-TIER I SCHEDULE "R2"



VEHICLE COMMAND & CONTROL SUBSYSTEM (VCCS)

The VCCS, at the lowest level of control, serves as the eyes, ears, and brains of the unmanned vehicle. It is responsible for the control and safety of the vehicle. The VCCS is an electronics package consisting of the vehicle's portion of the Collision Avoidance System (VCAS) and the microprocessor based Vehicle Control Unit (VCU). Following the PDR the VCU specification was approved and detailed design was initiated. This detailed design was presented at CDR and fabrication was authorized. The VCU was completed and verified to drawing; verification testing is covered in Section 7.

COLLISION AVOIDANCE SYSTEM (CAS)

The Collision Avoidance System is intended to prevent vehicle collision. Collision Avoidance equipment includes Vehicle CAS (VCAS) which uses vehicle-borne ODDCAS elements to format and send speed and position reports to wayside equipment; these reports are used to determine if safe separation exists between vehicles. This wayside equipment is referred to as Wayside CAS (WCAS). It uses ODDCAS elements which were to be installed on ramps, in channels, at merges, diverges, and on the main guideway. The WCAS removes a safe-to-proceed signal from the guideway to prevent an unsafe condition. The ODDCAS specification was approved following PDR. Following CDR, selected ODDCAS hardware was fabricated and checked out in support of VCU verification testing.

PROGRAM TESTING OVERVIEW

Thorough testing using a comprehensive computer simulation program confirmed the capability of the C&CS system to meet its specification requirements. In turn, the design approach provides "Traceability" to an Urban deployed system. The computer simulation, which is a very cost effective tool, is more fully covered in Section 7.

ADDITIONAL PROGRAM SUBSYSTEM DEVELOPMENT

Interfacing with the C&CS are the Vehicle and test track. Extensive preliminary design work, including design trades, and tests on vehicle subsystems were accomplished (prior to termination of the AGRT vehicle). Extensive design work was also done on the modified "MPM" vehicles. The

SYSTEM SPECIFICATION / METHODOLOGY OVERVIEW

The Phase IIB letter contract signed September 19, 1978 directed initial effort in contract tasks such as "Design Analysis and Trade Studies", "System Characteristic Studies", "Critical Item Development Plan", "Stopping Distance Report", and "Program Implementation Plan".

These activities, described more fully in Section 4, constitute system engineering and system management functions which provided Mission/Functional analyses. These analyses, in turn, led into Critical Technology definition permitting formulation of objectives. This period involved very close and frequent technical coordination with DOT-UMTA, DOT-TSC, The MITRE Corp., and Battelle. The thrusts were to develop the AGRT System Specification (SS362-90000-2) with emphasis on the incorporation of safety criteria and to determine exactly how detailed specification requirements would be verified at the test track to be "Traceable" to a deployed urban system. (See Figure 3.0-3)

The AGRT-EDS System Specification was superseded by the AGRT-EDS Command, Control, and Communications Specification (SS362-90000-4), July 1984. This program modification focused on the critical technologies with verification testing in the development lab. At the same time, we changed the program designation from AGRT-EDS to AGRT-EDS-C³ (Command, Control, and Communication). A VCU Test Set design review held March 14, 1984 detailed how the simulation testing program (to be conducted in our development lab) would fulfill the functional requirements of the vehicle and wayside communication with the vehicle and would provide traceability to an urban deployed system.

UMTA DEFINED KEY ISSUES / PROGRAM GOALS

With final program effort directed to the VCU, GCU and ODDCAS development were curtailed following their respective CDR's (see Figure 3.0-4). UMTA defined "Key Issues" and "Program Goals" at that time as follows:

EDS COMMAND AND CONTROL HIERARCHY (STATUS)

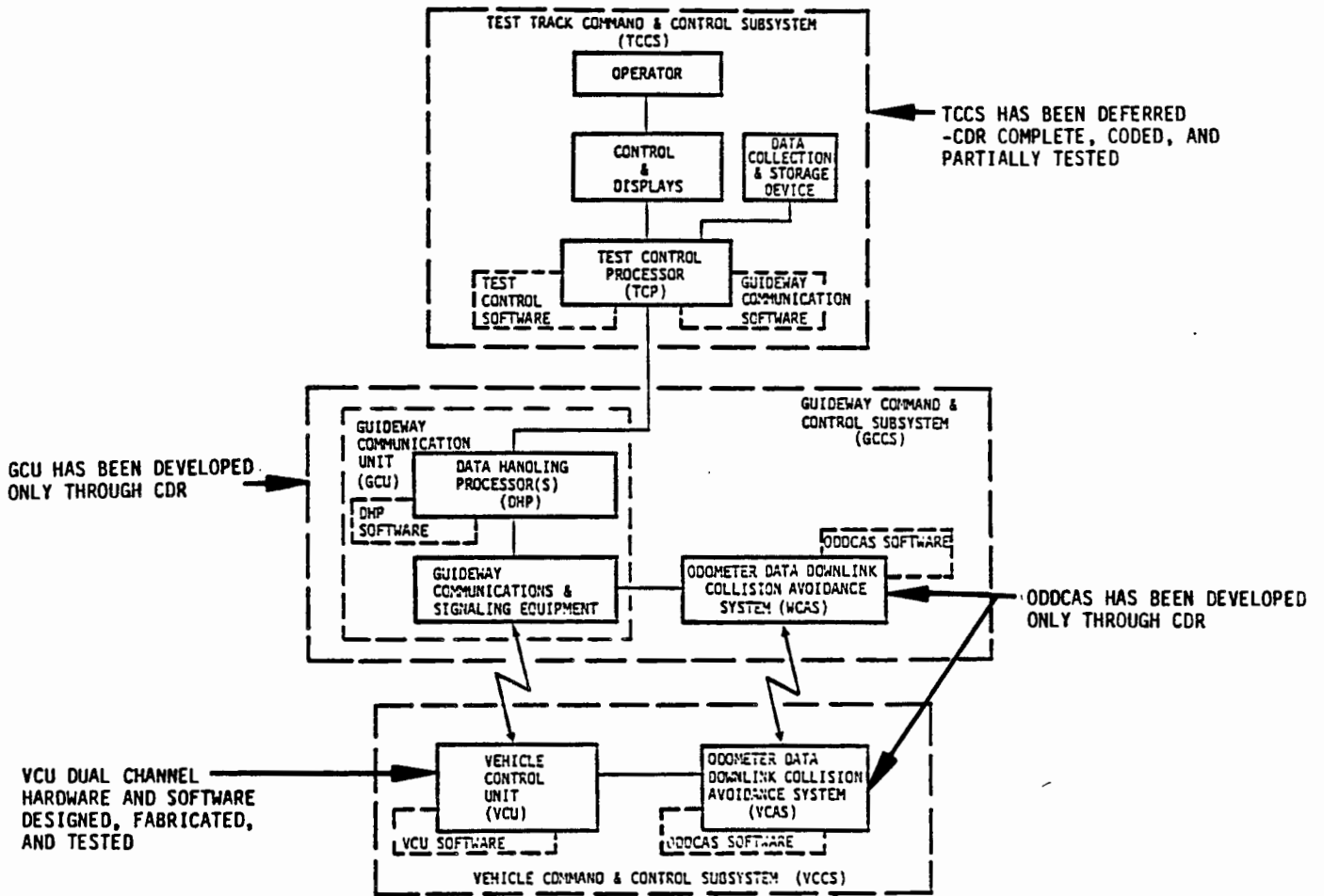


FIGURE 3.0-4

3.1 VEHICLE CONTROL UNIT (VCU) DESIGN SUMMARY AND RESULTS

This section provides a summary and results of the microprocessor-based VCU design. The focus is directed to UMTA's key issues and program goals as noted in Section 3.0.

SPECIFICATION CONTROL

The final AGRT-EDS safety review held September 26-27, 1984 comprehensively covered the safety concerns noted by UMTA. Figure 3.0-3 (from this safety review) reflects the incorporation of safety criteria into the initial System Specification and into subsequent iterations. Figure 3.1-1 depicts the allocation of safety requirements from the specification. The specifications incorporating the safety requirements were approved following System Design Reviews held April 7, 1980 and July 15-16, 1981.

Not shown in Figure 3.1-1 is the allocation of specific safety requirements to the "Prime Item Development Specification for Engineering Development System-Vehicle Control Unit" (S362-90006-1C). The VCU Specification, like the System Specification, is organized with Section 3.0 defining design requirements and Section 4.0 defining Quality Assurance requirements. Figure 3.1-2, "VCU Design Verification Process", depicts a page of the VCU specification showing how requirements in Section 3.0 are to be verified.

Figures 3.1-3 and 3.1-4 from the final system safety review are presented to provide the background of earlier System Engineering Safety activities.

- The third item on Figure 3.1-3, "Boeing formulated an accepted safety design approach through fail-safe, checked redundant, and safe life criteria for design", is the heart of the VCU design.

These safety criteria drove the VCU (as well as GCU and ODDCAS) design. During the AGRT-EDS development, factors necessary for application of microprocessors to safety critical designs were identified; techniques

TABLE 4.2-1: QUALITY ASSURANCE REQUIREMENTS VERIFICATION (Cont.)

SPECIFICATION PARAGRAPH	TITLE	SUCCESS CRITERIA	METHOD			
			I	A	T	D
3.5.2.7	Longitudinal Control	Per Requirements: Calculation of Command Profiles; Propulsion Contactor Control; Position Correction; Performance Level; Start-Up Timer; Jerk and Acceleration Limits; Closed Loop Emergency Stop; Forced Brakes; Station Stop Profiles; Speed and Position Error; Overspeed and Underspeed; Torque Command; Motor Command; Brake Command	X	X		

173
S362-90006-1C

I = Inspection A = Analysis T = Test D = Demonstration

3.5.2.7 Longitudinal Control Major Function

This major function controls vehicle longitudinal movement along the guideway by generating motor and brake torque commands based upon data received. This major function shall be performed during the first and second Minor Frames. It shall be composed of the Command Module, Speed and Position Controller, and the Signal Conditioning Functions (see Figure 3.5.2.7)

85
S362-90006-1C

FIGURE 3.1-2: VCU DESIGN VERIFICATION PROCESS

were developed to address these factors. This report can only provide an overview of these factors and techniques. We recommend an in-depth study be made by all concerned with safety in the application of microprocessor-based control systems in transit applications.

VCU DESCRIPTION

The AGRT control hierarchy (Figure 3.0-2) allocates control functions to the lowest possible level; hence, the Vehicle Control Unit (VCU) performs most of the control and safety processing. Because the VCU is carried on the vehicle, this approach permits use of a low speed data link between the vehicle and the wayside, and it reduces the need for safety critical processing at higher levels of the control hierarchy. However, this approach increases the complexity of the VCU and requires that virtually all VCU processing be done in a safe manner. Much of this processing is associated with longitudinal speed and position control, speed limit enforcement, door control and interlocks, fault monitoring and reactions, etc. It was judged that these complex processing requirements could not be met using traditional "failsafe" electro-mechanical vital elements due to inherent limitations of such devices. Instead the VCU design solution relies heavily on microelectronics to achieve safe, reliable performance within reasonable volume, weight, and power limitations.

Figure 3.1-5 provides the basic definition of three safety principles, "Fail-Safe", "Checked Redundant", and "Safe Life", that were available to the VCU hardware and software designer. Figure 3.1-6 provides further definition of safety terminology. Figure 3.1-7 identifies categorization of failsafe implementations relating to high technology.

Since design and safety engineering analyses concluded that micro-electronic devices are neither "Fail-Safe" nor "Safe Life", the final VCU design is "checked redundant" in both the hardware and the software.

The VCU accordingly meets UMTA's defined goals through application of checked redundant design. This concept employs independent dual redundant microprocessors and system status sensors, and independent, redun-

DEFINITIONS OF SAFETY TERMINOLOGY

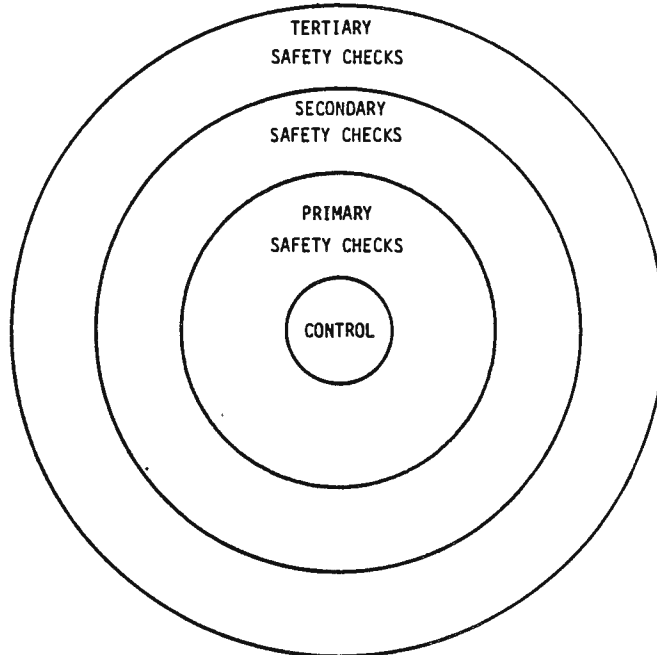
- o SAFETY CRITICAL FUNCTION -
 - o A FUNCTION THAT MUST BE PERFORMED WITH A SPECIFIED DEGREE OF CONFIDENCE TO GUARANTEE THAT THE SAFETY GOALS OF THE OVERALL SYSTEM ARE MET.
 - o MAY BE IDENTIFIED AT THE LOWEST LEVEL DISCERNIBLE.
 - o REQUIRES USE OF A SAFETY-CRITICAL ELEMENT.
 - o SAFETY-CRITICAL ELEMENT -
 - o A PIECE OF EQUIPMENT, OR COLLECTION OF EQUIPMENT, THAT IS PERFORMING A SAFETY-CRITICAL FUNCTION.
 - o IS FAILSAFE BY USE OF CHECKED REDUNDANT OR FAIL-SAFE PRINCIPLES.
 - o VITAL ELEMENT -
 - o A PIECE OF EQUIPMENT, OR COLLECTION OF EQUIPMENT, THAT HAS (AT LEAST) ONE FAILURE MODE, OR FAULT CONFIGURATION, THAT IS SO IMPLAUSIBLE THAT IT IS CONSIDERED IT WILL NOT OCCUR.
- AND
- o THIS CHARACTERISTIC IS PUT TO ADVANTAGE IN PERFORMANCE OF A SAFETY-CRITICAL FUNCTION.

FIGURE 3.1.6

CATEGORIZATION OF FAILSAFE IMPLEMENTATIONS RELATING TO HIGH TECHNOLOGY

- o CHECKED REDUNDANT
AN IMPLEMENTATION EMPLOYING THE PRINCIPLE OF CHECKED REDUNDANCY. A SAFETY CRITICAL FUNCTION IS PERFORMED IN TWO INDEPENDENT CHANNELS AND THE RESULTS ARE CHECKED AGAINST EACH OTHER TO DETECT (POTENTIALLY) UNSAFE FAILURES. A SAFE REACTION IS TAKEN BEFORE THE CONSEQUENCES OF A FAILURE CAN RESULT IN A HAZARDOUS CONDITION, OR BEFORE A SECOND SIMILAR FAILURE IN THE OTHER CHANNEL CAN OCCUR, DEFEATING FAILURE DETECTION.
- o FAIL-SAFE
ALL OTHER IMPLEMENTATIONS WHICH CAN BE SHOWN TO BE SAFE.
(i.e., DOES NOT EMPLOY CHECKED REDUNDANCY FOR SAFETY AND HAS NO PLAUSIBLE UNSAFE FAILURE MODES OR FAULT CONFIGURATIONS.)
- o SAFE LIFE
TRADITIONALLY ASSOCIATED WITH STRUCTURAL COMPONENTS BUT APPLICABLE TO ANY RELEVANT IMPLEMENTATION IF REGARDED AS A SPECIAL CASE OF A FAIL-SAFE IMPLEMENTATION.
(i.e., DOES NOT EMPLOY CHECKED REDUNDANCY FOR SAFETY AND HAS NO PLAUSIBLE UNSAFE FAILURE MODES OR FAULT CONFIGURATIONS WHEN INSPECTED AND SERVICED AT PREDETERMINED MAINTENANCE INTERVALS.)

FIGURE 3.1.7



THE "ONION SKIN" APPROACH

- o CONTROL:
 (vehicle control logic)
 speed and position command processing
 steering and door management
 communication management

- o PRIMARY SAFETY CHECKS:
 (S/W: data format anomaly control) (H/W: vehicle status anomaly checks)
 invalid data control brake pressure checks
 register overflow checks motor torque checks
 truncation error control hydraulic pressure checks
 range checks voltage checks
 X-channel sensor disparity control

- o SECONDARY SAFETY CHECKS:
 (S/W: data consistency checks) (H/W: microprocessor checks)
 odometer cross checks control flags check
 data rate of change checks CPU registers check
 motion profile control RAM and Rom checks
 cumulative error control dynamic exercising of emergency code

- o TERTIARY SAFETY CHECKS:
 (S/W: redundant software) (H/W: redundant hardware)
 A-B algorithm checks A-A algorithm checks "punch-in" key

FIGURE 3.1-8 SAFETY HIERARCHY

For example, consider a failure of a memory cell in only one channel of the dual control system. If that cell were used continually in the generation of vehicle control commands, its failure would be detected by the cross channel disparity check of the control commands. This primary check is done every forty milliseconds. This frequency of check assures detection and reaction in ample time to be safe. The failure of a memory cell used only under emergency conditions could remain undetected in both channels over a long period of time. This could result in an unsafe failure unless, independent of the normal disparity check cross channel, that cell is checked to prevent undetected common failures. The check of the seldom used cell is done often enough to make the probability of that element failing undetected in both channels negligibly small. The requirement set by the designers was to make the check on all RAM (Random Access Memory) cells every 9 (nine) minutes. The implementation does it once every two seconds.

Every element of the safety critical software path must be checked for failure. Software by its nature does not have a decay rate; it is either correct to start with or it contains errors that will result in erroneous commands under given conditions. Assuring that the software is error free isn't now technically feasible. To assure that such errors (which would result in common mode failures) are detected two check schemes were introduced.

The first involves the exercising of the code under dynamic conditions with false data that is deliberately skewed to result in simulated failure conditions. The resulting output of the code must be one of commanding a safe reaction; otherwise, a real emergency reaction is initiated. If the response is as expected, the true data is restored and normal control continues.

The second involves dissimilar software. Certain algorithms that are critical to the safe operation of the vehicle are designed redundantly within each of the two redundant channels (Symmetrical and Dual Dissimilar Software). Vital vehicle data or commands are first generated in a primary algorithm ("A" algorithm). A secondary algorithm ("B"

3.2 GUIDEWAY COMMUNICATION UNIT (GCU) DESIGN SUMMARY AND RESULTS

This section provides a summary and results of the microprocessor-based GCU design. The focus is directed to UMTA's defined issues and program goals as noted in Section 3.0.

SPECIFICATION CONTROL

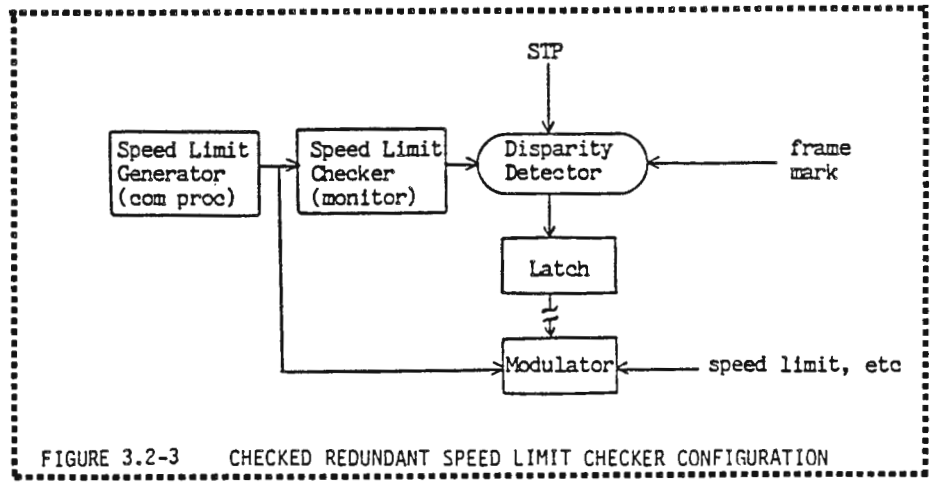
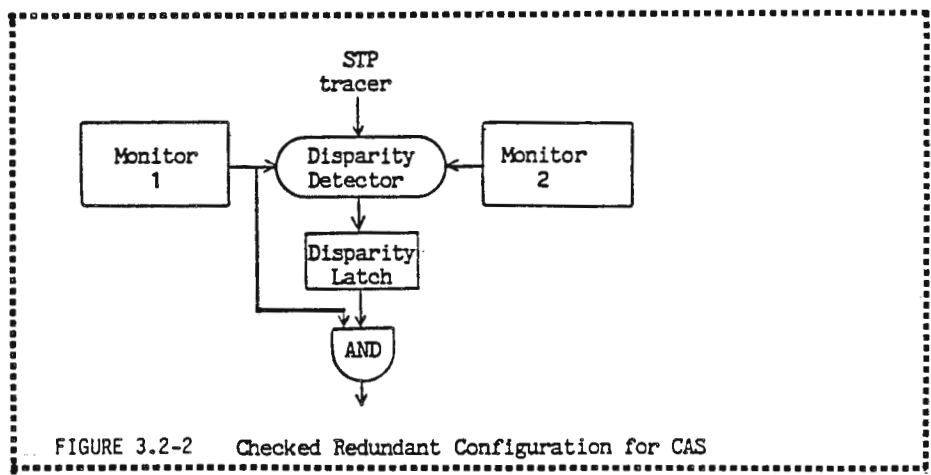
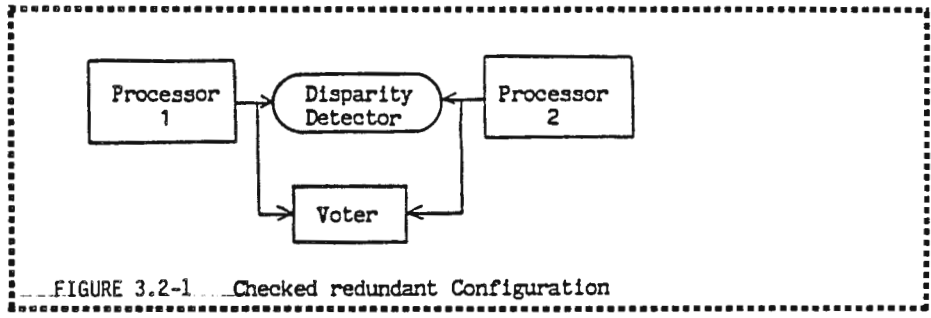
Like Section 3.1 on the VCU, the emphasis of this section is directed to the incorporation of the safety criteria in the hardware and software design of the GCU. Section 4.3 provides further GCU subsystem description. Reference 41 provides a detailed documentation of the GCU hardware and software design.

The final AGRT-EDS System Safety Review, as discussed in Section 3.1 on the VCU, applies also to the GCU. Safety criteria from the AGRT-EDS-C³ System Specification were also allocated to the AGRT-EDS Guideway Command and Control Development Specification. The GCU specification, like the VCU specification, sets forth Quality Assurance requirements to provide "traceability" to an Urban Deployed System.

GCU DESCRIPTION

As noted in Section 3.0 and Figures 3.0-2 and 3.0-4, the GCU is a subsystem of the GCCS which is the mid level of the C&CS control hierarchy. As previously described, the GCU serves as a communication link between the station (TCCS) and the vehicles (VCCS) on the guideway. The GCU consists of communication circuits in the station and communication equipment installed on the guideway.

The primary safety requirement of the GCU is to generate a speed limit in a failsafe manner and react to erroneous speed limit transmission by removal of the "Safe-To-Proceed" (STP) signal. As noted in Section 4.2, and detailed in reference 41, the STP signal is encoded in the "uplink" message being continually transmitted (every 40 ms) from the wayside to the vehicle over the Inductive Communication System (ICS).



simultaneous failure is small, the fixed reference does provide a slight improvement.

Use of a fixed standard (reference pattern) instead of the output from a redundant monitor is feasible for the Speed Limit Checker because a speed limit error can only be caused by equipment failure. This approach is not applicable to the CAS because CAS STP removal will usually be initiated by a vehicle conflict (minimum safe separation violation). The latched STP removal initiated by the disparity detector would be inappropriate for an ordinary conflict since the STP must be restored as soon as the conflict is resolved.

In summary, the functional requirements of the Speed Limit Checker are unique in several aspects which make a redundant checker unnecessary:

1. The redundancy between the Speed Limit Generator and the Speed Limit Checker.
2. The lack of latent speed limit failure modes in the communication monitor.
3. The high level of self exercising confidence possible in the Speed Limit Checker.
4. The applicability of a fixed standard.

SOFTWARE SAFETY DESIGN

The following provides a discussion of safety implementation from the perspective of the GCU software designer (41):

The central point in the design of the SLC software is safety; the SLC must be failsafe since the uplink speed limit must be generated and transmitted in a failsafe manner. For the SLC, this means that all hardware and software failures must result in an output which is detectable. Failure of the microcomputer to correctly execute instructions, or failure of instructions (or one instruction) in program memory, or

FIGURE 3.2-4
SPEED LIMIT CHECKER
SOFTWARE STRUCTURE

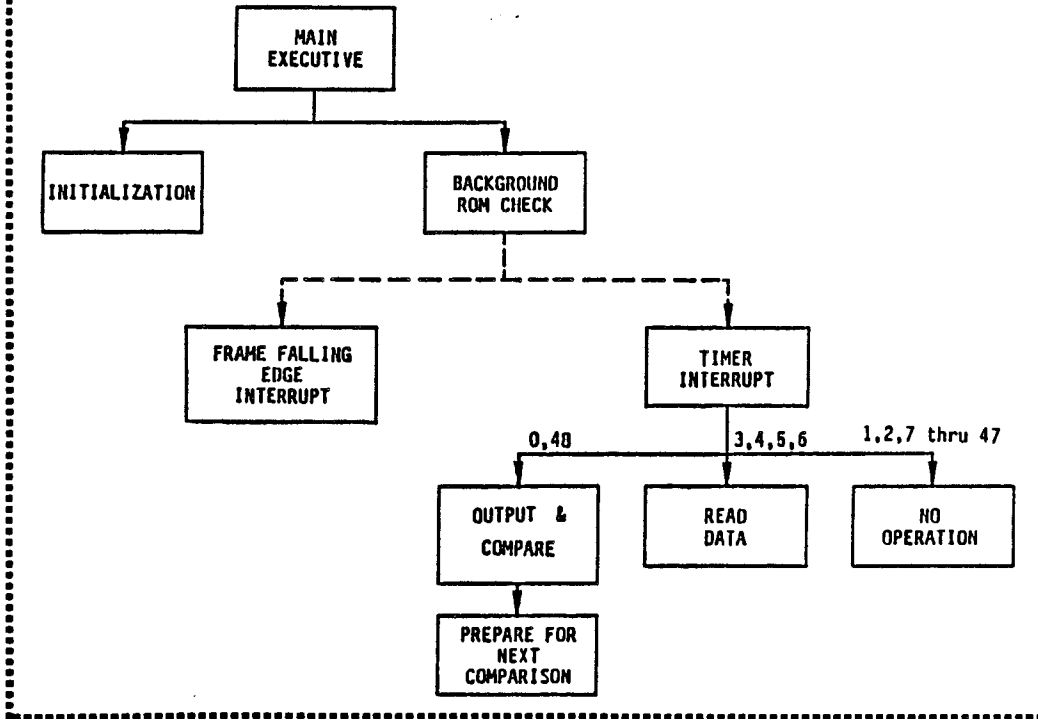


FIGURE 3.2-5
SPEED LIMIT CHECKER PROCESSING TIMING

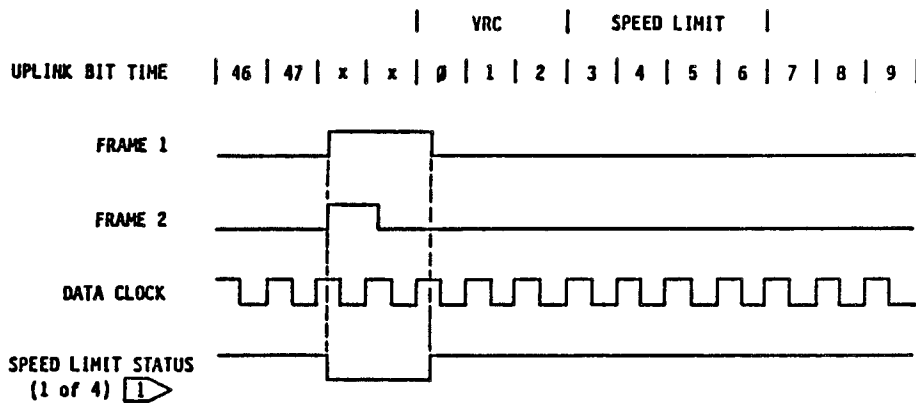


DIAGRAM SHOWS RESULTS WHEN SPEED LIMIT IS CORRECT FOR PRIOR FRAME AND ALL SELF-CHECKS PASS

3.3 ODOMETER DATA DOWNLINK COLLISION AVOIDANCE SYSTEM (ODDCAS) DESIGN SUMMARY AND RESULTS

This section provides a summary and results of the microprocessor-based ODDCAS design. The focus is directed to UMTA's defined issues and program goals as noted in Section 3.0.

Like Section 3.1 on the VCU, the emphasis of this section is directed to the incorporation of the safety criteria in the hardware and software design of the ODDCAS. Section 4.3 provides the ODDCAS subsystem description. Reference 42 provides a detailed documentation of the ODDCAS hardware and software design.

SPECIFICATION CONTROL

The final AGRT-EDS system safety review, as discussed in Section 3.1 on the VCU, applies also to ODDCAS. Safety criteria from the AGRT-EDS System Specification were also allocated to the ODDCAS Specification. The ODDCAS specification, like the VCU specification, sets forth Quality Assurance requirements to provide "traceability" to an urban deployed system.

ODDCAS DESCRIPTION

As noted in Section 3.0 and Figures 3.0-2 and 3.0-4, ODDCAS consists of 1), a Vehicle Collision Avoidance System (VCAS) which when integrated with the VCU, becomes the Vehicle Command and Control Subsystem, and 2), a Wayside Collision Avoidance System (WCAS) which when integrated with the GCU, becomes the Guideway Command and Control Subsystem.

As the name implies, ODDCAS utilizes on-board vehicle odometer data to monitor vehicle speed and position throughout the guideway. The design employs eight and sixteen bit microprocessors and incorporates unique self-exercised software to detect potentially unsafe latent failures within the hardware.

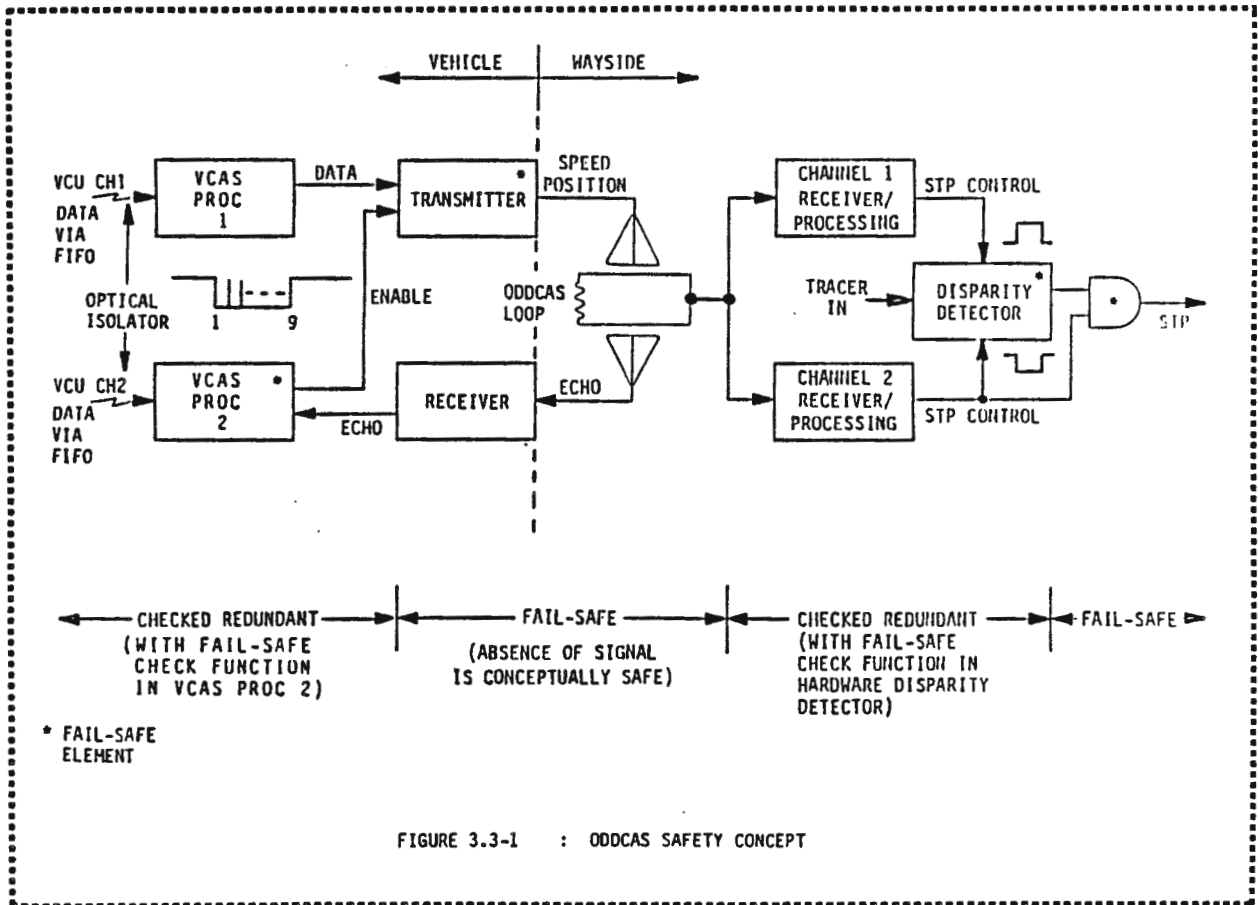


FIGURE 3.3-1 : ODCAS SAFETY CONCEPT

4.0 SYSTEM AND SUBSYSTEM OVERVIEW

This section focuses on the program analysis phase of the AGRT contract. The analysis phase established requirements that subsequently were incorporated in System and Subsystem Specifications. The following tasks were accomplished in the early analysis phase of the contract:

- Task 2. Program Implementation Plan.
- Task 3. Program Documentation Plan.
- Task 4. Test Facility Layouts.
- Task 5. Test Facility Reports.
- Task 6. Design Analysis and Trade Studies.
- Task 6.a Engineering Development Specification.
- Task 7. Critical Item Development Plan.
- Task 8. Engineering Facility Technology Verification Capability.
- Task 9. System Characteristic Studies.
- Task 10. Revised AGRT Program Proposal.
- Task 11. Stopping Distance Studies.

Activities associated with these tasks are scoped and best understood in the context of their accomplishment through System Analysis, System Management, and System Engineering methodology and techniques.

The contract analysis phase was a transitional period. It encompassed the final documentation of Phase IIA activities in the fall of 1978.

The analysis phase continued in Phase IIB with program activities associated with the development of the initial Phase IIB AGRT Specification and System Design Review held in April 1980. The analysis phase continued with the development of the superseding AGRT-EDS Specification and updated System Design Review held in July 1981.

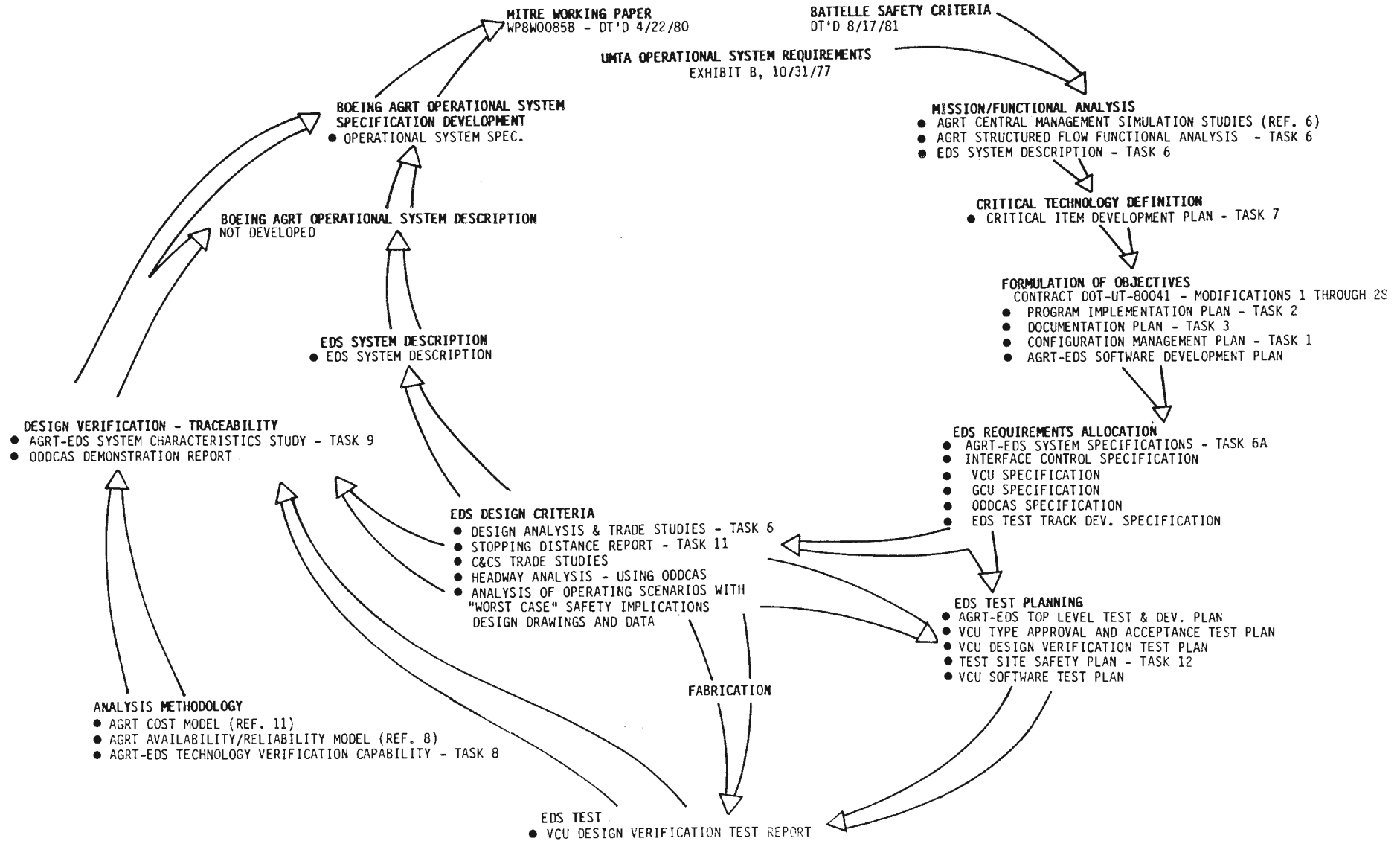
ADVANCED GROUP RAPID TRANSIT - PHASE IIB
APRIL 22, 1981

WBS

Line No.	NEW SOW ITEM No.	Description	WORK ORDER	PACKAGE #	SYSTEMS ENGINEERING												MANUFACTURING			DEVELOPMENTAL			MATERIAL					
					VEHICLE DESIGN	ELECT. & POWER	C & C S	SOFTWARE	GUIDEWAY & STRUCTURES	DESIGN ANALYSIS	TEST	MANUFACTURING	QUALITY ASSURANCE	SUPERVISION & CLERICAL	DEVELOPMENTAL	D.L. PLANNING	PROC / PTC / MFG DD	SUBCONTRACT	PE/PM, DEV MTL	TRAVEL								
1	0	AGRT Program Phase IIB																										
2	1	Program Management	7E772	00																								
3	2	Program Implementation Plan	7E752	00																								
4	3	Documentation Plan	7E752	00																								
5	4	Test Track Facility Plans (Completed)	7E752	00																								
6	5	Test Facility Report (Completed)	7E752	00																								
7	6 & 6A	Design Analysis (Completed)	7E751 7E750	5A 06																								
8	7	Critical Item Development Report	7E752	00																								
9	8	EDS Technology Verification Capability	7E752	00																								
10	9	System Characteristic Study	7E751	09																								
11	10	AGRT Revised Proposal (Completed)	7E750	00																								
12	11	Headway/Stopping Distance Report (Completed)	7E750	11																								
13	12	Test Site Safety Plan	7E750	12																								
14	13	Vehicle Auto. Fire Prot. Study/Report (Deferred)	7E750	13																								
15	14	Engineering Development System Design																										
16	14.1	System Engineering																										
17	14.1.1	Requirements Analysis	7E753	20																								
18	14.1.2	Interface	7E753	30																								
19	14.1.3	Reliability	7E753	50																								
20	14.1.4	Safety	7E753	70																								
21	14.2	Vehicle																										
22	14.2.1	Passenger Module	7E754	11																								
23	14.2.2	Vehicle Chassis	7E754	21																								
24	14.2.3	Vehicle Integration and Assy	7E754	30																								
25	14.3	Command and Control																										
26	14.3.1	Test Track Command Control	7E755	11																								
27	14.3.2	Guideway C&CS	7E755	21																								
28	14.3.3	Guideway CAS																										
29	14.3.3.1	Reflectometer	7E755	27																								
30	14.3.3.2	Wayside CAS Alternative EDS Wayside CAS	7E755	29 25																								
31	14.3.4	Vehicle Command and Control																										
32	14.3.4.1	Vehicle Controller Subsys	7E755	31																								
33	14.3.4.2	Casbar Subsystem	7E755	32																								
34	14.3.4.3	Integration and Assembly	7E755	33																								
35	14.4	Wayside and Power Distribution	7E755	10																								
36	14.5	Support Equipment	7E757	10																								
37	14.6	Software Design																										
38	14.6.1	Test Track Software	7E758	10																								
39	14.6.2	Support Software	7E758	20																								
40																												
41																												
42	14.7	Test Track Design	7E759	00																								
43	15	Engineering Development Hardware																										
44	15.1	Vehicle																										
45	15.1.1	Passenger Module	7E762	10																								
46	15.1.2	Vehicle Chassis	7E762	20																								
47	15.1.3	Vehicle Integration	7E762	30																								
48	15.2	Command and Control																										
49	15.2.1	Test Track Command and Control	7E763	10																								
50	15.2.2	Guideway C & C Subsystem	7E763	20																								
51	15.2.3	Guideway CAS																										
52	15.2.3.1	Reflectometer	7E763	50																								
53	15.2.3.2	Other	7E763	51																								

FIGURE 4.1-1

FIGURE 4.1-2 SYSTEM MANAGEMENT - METHODOLOGY - ROAD MAP



System Engineers and Subsystem Designers as derived from computer simulation. This activity subsequently was documented in Task 11, "Stopping Distance Report".

The System Engineering organization, encompassing safety and reliability engineering, was responsible for the System Specification; the EDS System Description; System Characteristic studies; and coordination and firming of system interfaces.

The Subsystem design organizations (Vehicle, C&CS, Guideway Structures, and Power Distribution) were responsible for Conceptual design trades and supporting Laboratory testing. Conceptual design trades such as Test Track alignment, Propulsion systems concepts, and steering and switching concepts, impacted requirement analyses being developed by System Engineering and Design Analysis.

In System Management "parlance" this analysis phase culminated in the definition of the "Functional Baseline". During this analysis phase, periodic technical interchanges were held with UMTA and UMTA's supporting consultants. Program and Safety Reviews provided detailed information pertinent to all aspects of the developing program. The System Design Review (SDR) established the functional baseline. The AGRT System Specification and system interfaces were approved following the SDR. Subsequent changes to the released System Specification and defined interfaces were subject to System Management Control per the Configuration Management Plan.

Figure 4.1-3, from the PIP, shows the relationship of baseline progression to major reviews. This figure has been modified per the AGRT-EDS-C³ program. As shown in the Figure, completion of the SDR on July 15, 1981 authorized the start of preliminary design in accord with the System Specification. Subsystem design proceeded in accordance with selected design concepts and allocated requirements to subsystems within the constraint framework of system level documentation. The end result of this process was the definition of an "allocated" design baseline through the development of sub-

system specifications. When sufficient design was completed, a subsystem "Preliminary Design Review" (PDR) was held. Following PDR, subsystem specifications were approved and placed under configuration control by system management.

The PDR marks the establishment of formally allocated design restraints by system management. Detailed design and procurement of long lead items were authorized by system management. The preparation of procurement specifications, through which we control subcontracted equipment such as the vehicle propulsion subsystem, started at this time.

When detailed designs were completed to a point where fabrication could start, Critical Design Reviews (CDR) were held. The aggregate of specifications and design documentation, e.g., drawings, define a "Product" baseline. Top level test plans (see Figure 4.1-2), as well as detailed test plans defining principal tests through which the achievement of contract objectives could be evaluated, were completed. Like specifications and other program documentation, test plans and documented test procedures were placed under system management change control after release so that uncontrolled changes could not subvert the purpose or validity of a test.

The VCU test set design review provided the basis for approval of the VCU test set design and authorization of its fabrication. The review also validated the capability of the simulation lab for verification of the critical technologies. Test procedures and "as run" test reports were documented during system simulation testing in the development lab. Test results and reports provided information from which specification (and contract) compliance were evaluated.

FIGURE 4.1-4 Simulation Ensemble Summary

<p>AGRT analytical model</p> <ul style="list-style-type: none"> • Expected value • Perfect merges • Ideal trip times • Evenly spaced vehicles • Parametric output • Easily modified/inexpensive <p>Coarse network simulation</p> <ul style="list-style-type: none"> • Individual passengers and vehicles • Station throughput—dwell only or simplified moveup • Follows quantized time-varying passenger demand • Functionally reflects deceleration/acceleration of vehicles • Functional merge/demerge models • Outputs service-related performance measures <p>Detailed network simulation</p> <ul style="list-style-type: none"> • Individual passengers and vehicles • Follows time-varying passenger demand • Detailed vehicle kinematics • Reflects deceleration/acceleration of vehicles • Performs action at same time as actual system • Performs same procedure as actual system; e.g., precise station, merge, dispatch, headway management algorithms • Outputs all service-related performance measures <p>Station simulation</p> <ul style="list-style-type: none"> • Precise vehicle-movement timing • Stochastic vehicle arrivals • Stochastic vehicle strings on local guideway (impacts dispatch opportunities) • Stochastic model for door cycle time (models passengers obstructing closure) <p>Headway simulation</p> <ul style="list-style-type: none"> • Jerk and acceleration-limited speed profiles • Variable EB delay and vehicle length • Separate lead and trailing vehicle speed profiles • Calculates stopping-distance margin based on worst case minimum safe headway for the transition <p>Local control simulation</p> <ul style="list-style-type: none"> • Individual vehicles with detailed onboard controller <ul style="list-style-type: none"> • Mode selection • Jerk and acceleration limiting • Brake/motor command generation • Status and fault monitoring • Communication to message level <ul style="list-style-type: none"> • Vehicle/wayside • Local control/central management • Easily reconfigured to represent different guideway configuration by changing data base • Time resolution to 0.00025 sec • Flexible output • Built-in debugging aids 	<p>Analytic dependability model (standard link)</p> <ul style="list-style-type: none"> • Computer cumulative annual passenger delay • Individual vehicles and wayside elements <ul style="list-style-type: none"> • MTBF and TR • System operating parameters <ul style="list-style-type: none"> • Line speed • Operating and minimum safe headways • Cushion utilization • Load factor • Passenger wait time • Station dwell time • Low-cost operation for parametric sensitivity studies <p>Monte Carlo dependability model (standard link)</p> <ul style="list-style-type: none"> • Completes cumulative annual passenger delay and delay distribution • Individual vehicles and wayside elements <ul style="list-style-type: none"> • Failure and restoration distribution functions • System operating parameters (same as analytic dependability model) • Wide selection of outputs <p>Network dependability model</p> <ul style="list-style-type: none"> • Computer cumulative annual passenger delay • Models any trip in network as series of dissimilar links and nodes • Individual vehicles and wayside elements on route • System operating parameters for each link (same as analytic dependability model) • Entirely analytic, provides economic support to large number of network configurations and system studies <p>Life cycle cost model</p> <ul style="list-style-type: none"> • Based on UMTA WBS • Twenty-year vehicle life • Thirty-year life for remaining fixed assets • Computes capital, operating, and maintenance costs • Computes break-even fares for variety of financing options <p>Demand generator</p> <ul style="list-style-type: none"> • Based on UMTA-supplied demand model • Includes individual and batch (bus, train, . . .) arrival models • Generates individual party, time-varying demands <p>Longitudinal control simulation</p> <ul style="list-style-type: none"> • Thirtieth order nonlinear analytic model • Based on test data verified MPRT model • Primary tool for verifying onboard point-follower control system <p>Lateral control simulation</p> <ul style="list-style-type: none"> • Twenty-eight degree-of-freedom model • Accounts for any longitudinal motion interactions • Steering system design tool • Verifies vertical ride comfort
---	--

From D336-10043-1
Phase II Executive Summary

ANALYSIS TOOLS

- LOCAL CONTROL SIMULATION

Multiple Vehicle Analysis Tool (Developed in Phase IIA)

Uses -- Wayside Control Algorithm Development
Definition of Guideway Layout Constraints
System Performance Prediction/Extrapolation

- VEHICLE LCS SIMULATION

Single Vehicle Analysis Tool (Based on MPM Simulation)

Uses -- Onboard Control Algorithm Development
Dynamic Performance & Stability Studies
Performance Prediction/Extrapolation

- HYBRID LCS SIMULATION

VCU H/W & S/W Validation Tool

Used to Verify VCU/Odometer Concept Feasibility in Phase IIA
Needed to Support Phase IIB VCU/Odometer Development Effort

- IMPACT OF REVISED EDS PROGRAM

Must Update Simulations to Reflect Use of STTF & MPM Vehicles

FIGURE 4.1-5

BAC SYSTEMS APPROACH

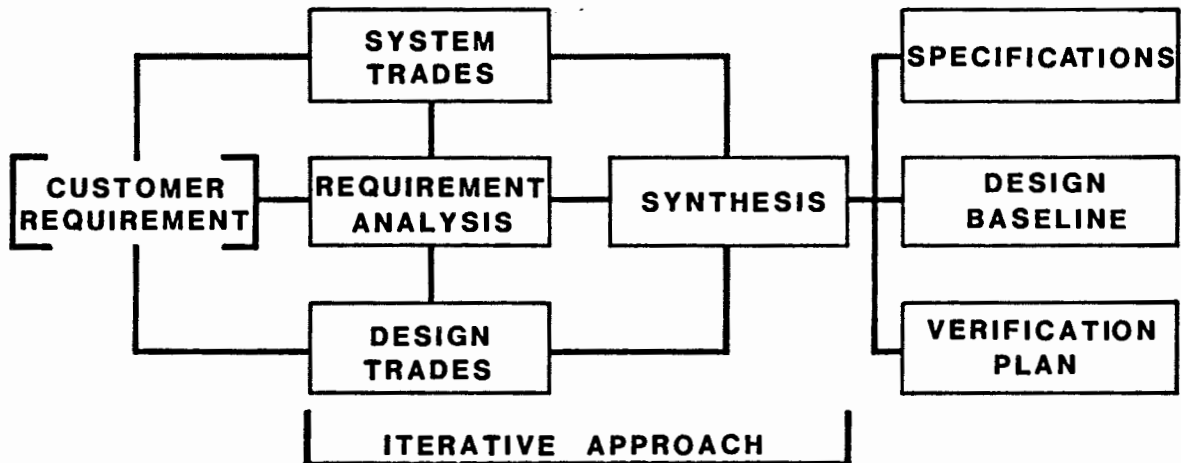


FIGURE 4.1-6

ULTIMATE GOALS

1. Top-down traceability of requirements
2. Control of system baseline
3. Discipline to design process
4. Integration of development of all system elements
5. Reduced downstream cost, schedule and technical risk

FIGURE 4.1-7

From BAC presentation entitled: "System Engineering for Managers" given at System Engineering and Project Management Symposium, Univ. of Washington, Oct. 1984

SYSTEM ENGINEERING - SAFETY

Figure 4.1-8, "Boeing AGRT Design Process", was presented in the AGRT Collision Avoidance (CAS) Safety review in March 1981. This figure shows the top level sequence for ensuring that all design and safety requirements are met. As the design process moves from requirements to functional allocation to design concept formulations and so on, a parallel safety effort ensures that the applicable safety criteria are met at each stage and that the criteria for the next stage are consistently defined and enforced. This process takes place whether the equipment is being designed and built in-house or by a subcontractor. The safety analysis at each design level consists of hazard identification, fault tree analysis, criteria specification, and "next level" criteria formulation. Figure 4.1-9, "Development of System Safety", taken from the system safety review of October 5 1982, reflects in more specific detail the parallel flow of system and safety requirements.

SYSTEM ENGINEERING TOOLS

FUNCTIONAL ANALYSIS:

Figure 4.1-10, "AGRT Function Tree", is an extraction from Phase IIA document D190-90505, "AGRT Operations Management/Control System Functions". This figure shows a portion of the function tree from the document, and highlights the principal functions in the Engineering Development System. Numbers with the functions refer to paragraphs in the document.

FUNCTIONAL ANALYSIS PROVIDES RESPONSES TO THE FOLLOWING QUESTIONS:

- o What do we need to do to manage the AGRT?
- o What resources do we need to manage?
- o What system responses do we expect?
- o What system requirements and objectives are needed to control how we manage the system?

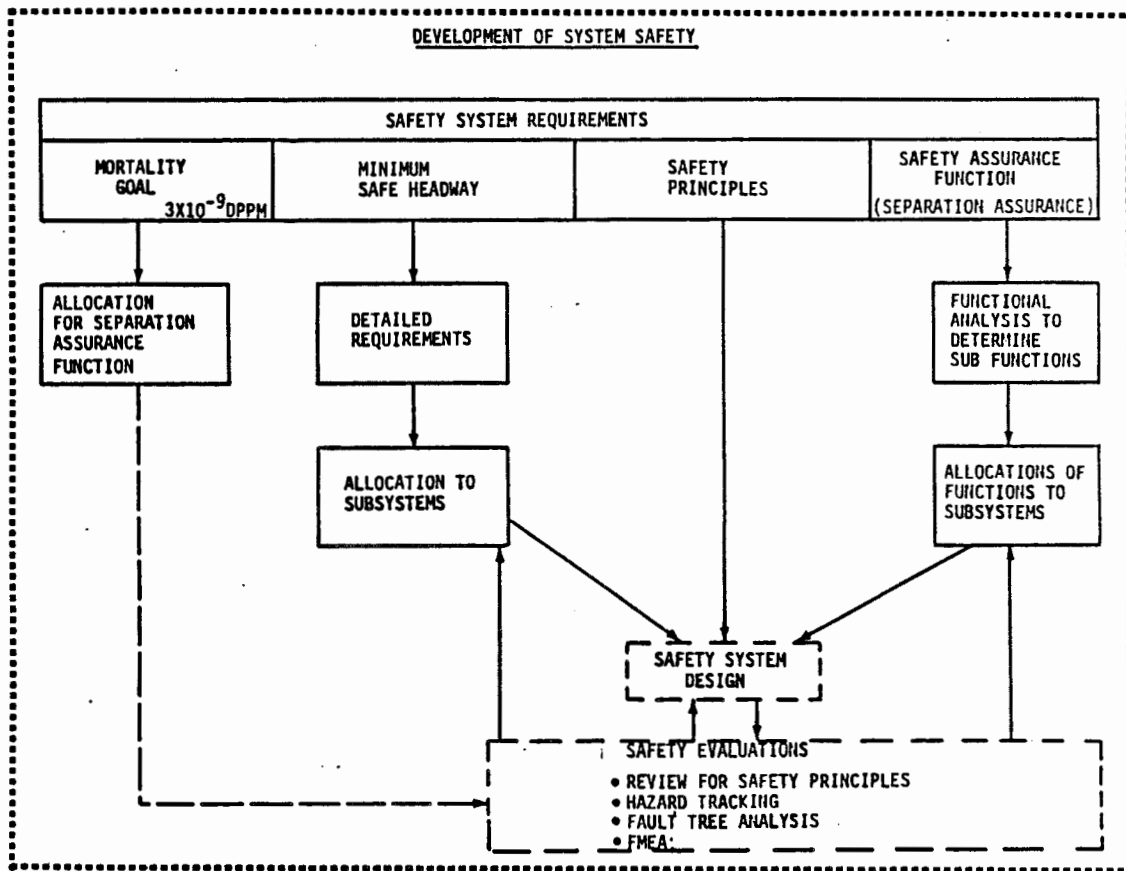


FIGURE 4.1-9

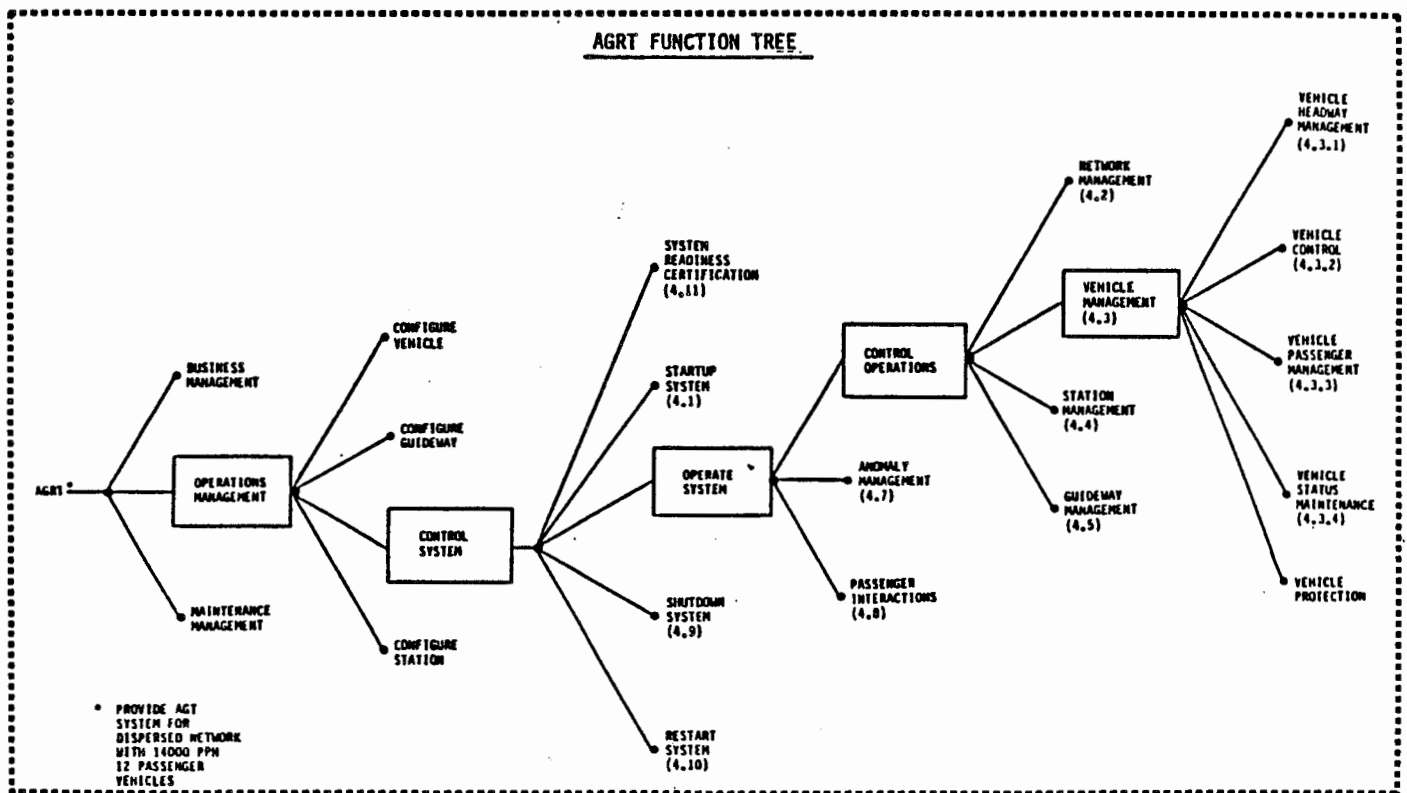


FIGURE 4.1-10

Figure 4.1-11 is an example of the LAMDA-TAU (λ, τ) evaluation technique developed in the Aerospace industry to quantify safety. The method combines individual component failure rates assigned to fault events at the bottom of the tree to obtain a probability number at the top of the tree.

Figure 4.1-12 shows follow-through of this quantitative analysis technique to determine time between checks of the VCU checked redundant design.

WORST CASE ANALYSIS (CIRCUIT, TIMING, AND ERROR ANALYSIS)

Safety engineers conducted several worst case analysis studies. An example is an internal documented study entitled: "Vehicle Control Electronics (VCE) Timing Synchronization - Safety Analysis." This was a safety evaluation of the watchdog timer circuits that withhold punch-ins to the brake amplifiers if the master oscillator drifts. The analyses led to the recommendation for a daily start-up check to detect latent failures.

MODELS/SIMULATIONS

Usage of models and simulations has been noted (Figure 4.1-4) previously; the repetition here is to note its significance as another tool of system engineering. Generic use of models include:

- o System performance predictions
- o Derivation of operations sequence
- o Optimization of system design

PROGRAM CHANGE CONTROL

It should be noted that our AGRT organization was Research & Development (R&D). Hence, fabrication (Task 15) items on the WBS were built as "breadboard" items and were not prototype or production units. The main thrust of a "breadboard" unit is to validate the basic design to specification through limited verification testing.

The change control process deferred changes that would enhance dependability for future design efforts. The VCU documentation (reference 43) reflects these concerns, as well as noting that a production design VCU would use military specification temperature range parts and one channel of a production unit would fit in a package approximately 5 inches by 10 inches and would contain four printed circuit cards. Each channel would require approximately 18 watts of power.

The system management-system engineering methodology established a disciplined environment. This discipline was maintained by assuring that all changes to released engineering following System and Design Reviews could only be made by authorized changes. Accordingly, from the initial release of the System Specification following the System Design Review, Change Control was initiated. Program controlled changes are summarized as follows:

EIGHT CLASS I CHANGES

Class I changes are changes requiring revisions to released engineering as a result of contract changes requested by UMTA.

Example: Engineering Change Proposal (ECP) #5 incorporated Contract Mod. 28. This change accounted for all engineering changes and program action required to terminate the MPM vehicle and STTF track and implement the simulation program.

SIXTY-THREE CLASS II CHANGES

Class II changes are design requested changes; included are eighteen deferred or partially deferred changes.

Example: PRR (Production Revision Record) 1003 - "Position Update Algorithm Revisions." This change was identified in hybrid testing and required revisions to the released VCU specification, VCU software product specification and VCU firmware.

SECTION SUMMARY

The major thrust of this section and section 4.0 was to show how the VCU, GCU, and ODDCAS designs evolved from AGRT program objectives, requirements, and specifications as determined in the analysis phase of the contract.

Of equal intent was to acquaint the reader with the comprehensive nature of the complete "Automated Transit System Analysis". The AGRT Command and Control system that evolved from the analysis phase is not intrinsically different from command and control systems developed and implemented by Boeing in such systems as the Airborne Warning and Control System (AWACS), Airborne Launch Cruise Missile (ALCM), and the Apollo Technical Integration and Evaluation (Apollo-TIE).

and convenience would be possible. Such service should dramatically increase ridership. The service level is made possible because the short headways allow high throughput with small vehicles. During the morning rush hour the small vehicles would pick up passengers on the low demand outer legs of a network and converge on the Central Business District (CBD). Links in the CBD would utilize the short headway capability of the system to handle the dense vehicle traffic.

Dependability would be maximized by the development of systems utilizing solid state digital electronic hardware, and software approaches which have been proven to be inherently reliable in today's commercial, military, and space systems. Downtime would be minimized by providing redundancy, reset, and manual override capability. Stops on the guideway would be minimized by maximizing the use of cushion (vehicle spacing in excess of minimum headway).

Safety would be maximized by requiring the use of fail-safe, checked redundancy, or safe-life design principles. This is a highly desirable development in itself because it meets the traditional railroad safety criteria with a modern electronic high performance system.

Life cycle costs would be minimized by reducing O&M (recurring) costs through use of microminiaturized integrated circuits which have low production costs and high reliability (as evidenced by hand held calculators, walk-around stereos, and digital watches).

Analysis performed during the AGRT program has shown that a transit system based on the elements being developed on this contract can meet O&M costs from the fare box.

The AGRT-EDS program was initially structured to construct and test critical "Local Control" portions of the operational system. In an operational system, automation is achieved with a four level control hierarchy (see Figure 4.2-1). The control hierarchy consists

of central, region, zone, and vehicle. Each level would include one or more computers, their associated software, and command and control hardware elements. Central oversees the entire operation and exerts control over functions which require information from two or more regions. All of the system operators, the central and region computers, and the administration/business offices are located in the central facility.

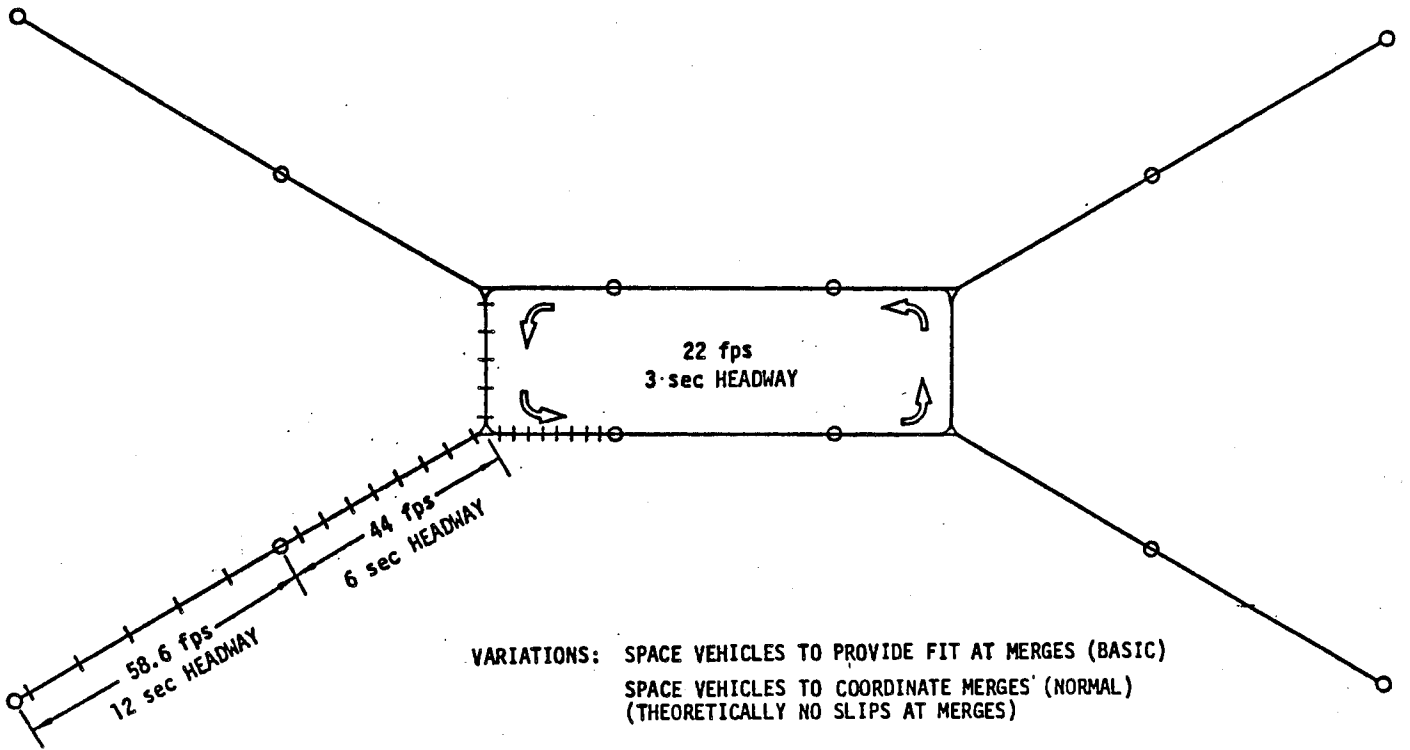
The regions oversee zones and exert control over all functions which require information from two or more zones. The zones directly control vehicle dispatches, merges/diverges, normal stops, and restarts. The zone also monitors vehicle-to-vehicle headway at least every 1000 feet and commands position corrections, if necessary.

The onboard Vehicle Command and Control Subsystem (VCCS) directly controls acceleration, deceleration, speed/position regulation, and emergency braking. The onboard VCCS is a highly accurate point-follower which follows an internally-generated ideal time-distance-speed trajectory. The combination of this accurate onboard point-follower and the position corrections from zone allows headway errors to be controlled to within three sigma accuracy of 0.22 to 0.55 seconds depending on vehicle speed.

The vehicle and stations carry out the commands of the control system. Primary features of the vehicle are: electric propulsion, a simple side-rail steering system, vehicle on-board switching, positive restraint with retention at intersections, and closed-loop brakes. Primary features of the stations are: automatic fare collection and passenger management, platform doors which are synchronized with the vehicle doors, elevators/escalators, and passenger security systems.

Use of the above control hierarchy and philosophy would allow a modular structure in which direct control functions are performed at the zone-vehicle level and supervisory functions at central and

FIGURE 4.2-2
FLEET MANAGEMENT (QUASI SYNCHRONOUS)



the wayside. To perform this update, the wayside (Guideway Command and Control Subsystem) also calculates an ideal trajectory and compares the actual vehicle position to the ideal position at presence detectors on the guideway. This is accomplished by storing the arrival time at each presence detector (PD) of a perfect vehicle, then when the vehicle activates the PD, measuring the deviation from the ideal wayside point, and giving the vehicle a correction command to return it to the ideal point as calculated by the wayside. This is accomplished by adjusting the vehicle speed within ± 2 fps. PD's are located no more than 1000 feet apart, allowing vehicles to maintain a high degree of separation accuracy as is shown in Table 1.

COLLISION AVOIDANCE

In the AGRT System, a moving block "odometer data downlink" collision avoidance system continuously monitors the position and speed of all vehicles on the guideway. If the distance between vehicles becomes less than the minimum safe distance established for the measured vehicle speed, irrevocable emergency rate stopping is invoked for all vehicles in the area where the headway violation occurred. This is accomplished by the removal of the Safe-To-Proceed (STP) signal from the guideway. The reaction time from this detection of an unsafe condition to the initiation of an emergency stop is no longer than 0.15 seconds. This short reaction time, combined with the accurate vehicle-to-vehicle regulation and the closed-loop emergency stopping system, allows headways as low as 3 seconds. This headway is accomplished with a commanded emergency rate deceleration of 0.34 g's (11 fps²). (A "brickwall" stop of the lead vehicle is assumed in headway calculations.)

4.3 SUBSYSTEM DESIGN OVERVIEW

COMMAND AND CONTROL SYSTEM (C&CS)

The Command and Control System (C&CS) is responsible for the overall management and control of the AGRT system in both normal and anomalous modes of operation. Overall control is provided by electronic hardware and associated software operating in a hierarchical, modular structure.

OPERATIONAL C&CS

The C&CS for an operational system would be functionally divided into a four-level hierarchy:

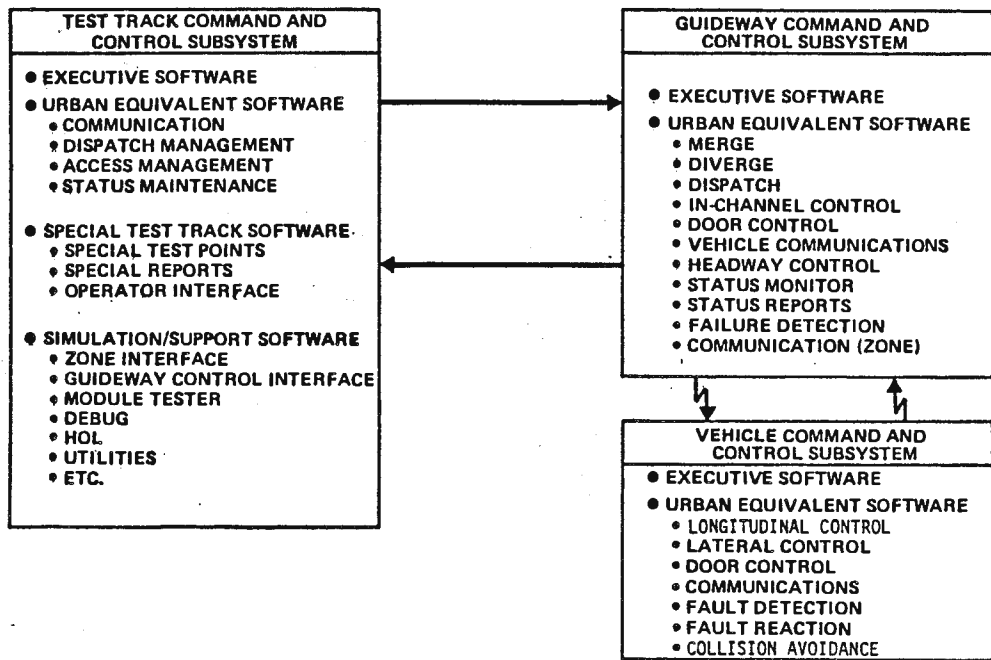
- 1) A Central Command and Control Subsystem (CCCS) would set system policy, collect and analyze system performance data, and supervise all system functions.
- 2) A Regional C&CS (RCCS) would automatically implement these policies among network sections.
- 3) A Zone C&CS (ZCCS) would be responsible for station operation, automatic motion commands of individual vehicles, and data collection on resulting vehicle operations.
- 4) A Vehicle C&CS (VCCS) would be located on each vehicle of the fleet to safely control each vehicle according to the commands of the ZCCS.

The ZCCS would be comprised of the Zone Controller Subsystem, Guideway Controller Subsystem, and the Zone Communication Subsystem.

Functions which would be primarily accomplished by the ZCCS are: position corrections every 1000 feet to adjust vehicle separation interval, slot-slip position corrections at merges,

FIGURE 4.3-1

EDS BASELINE -SOFTWARE

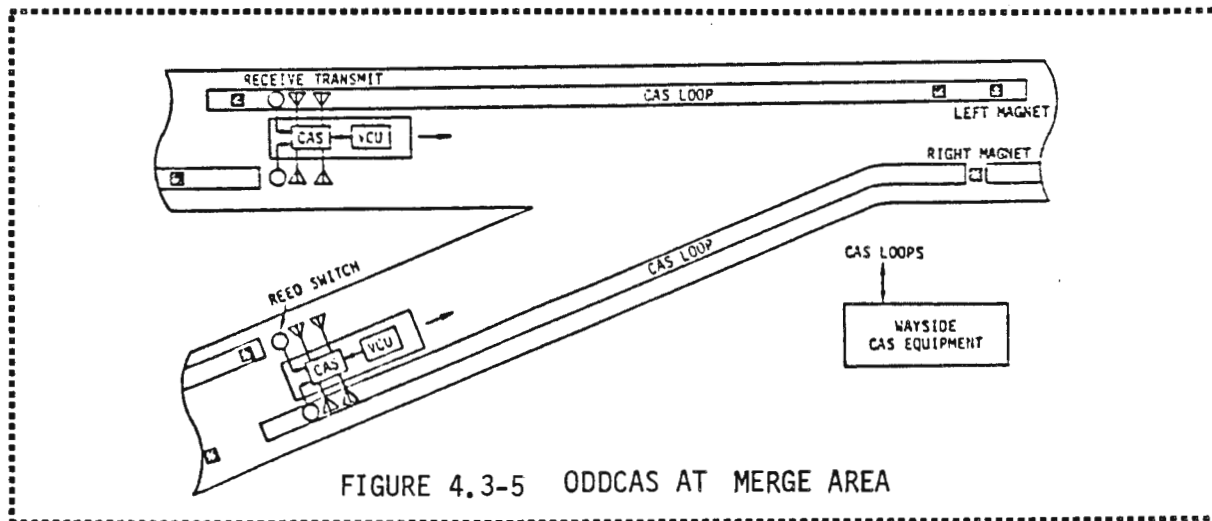
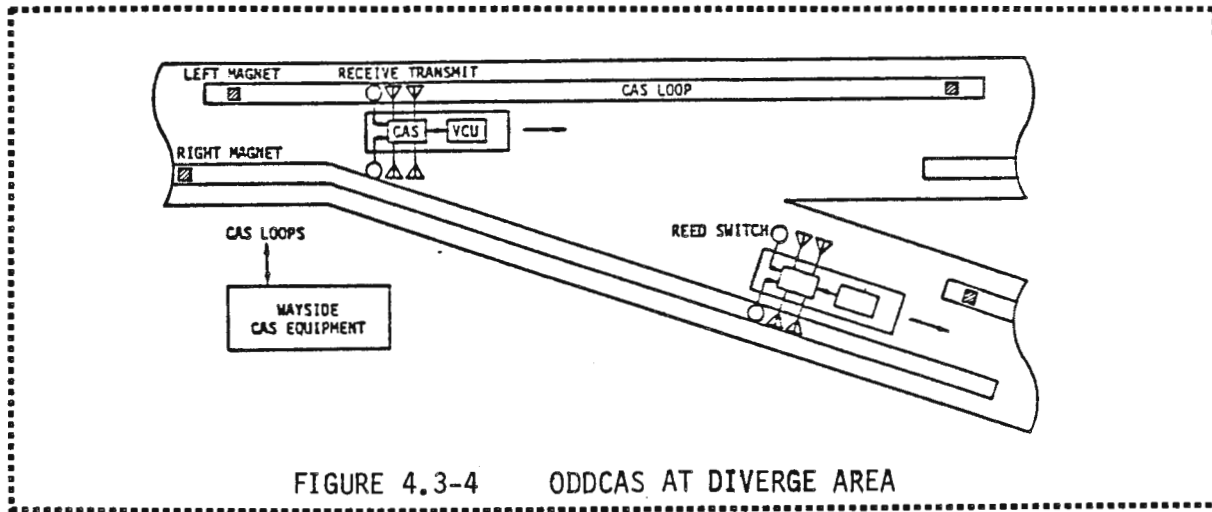
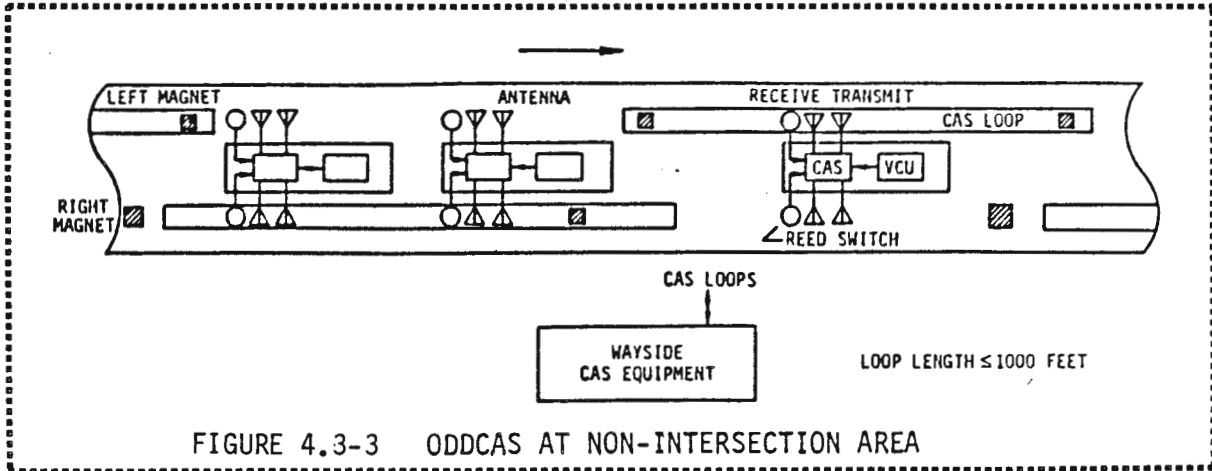


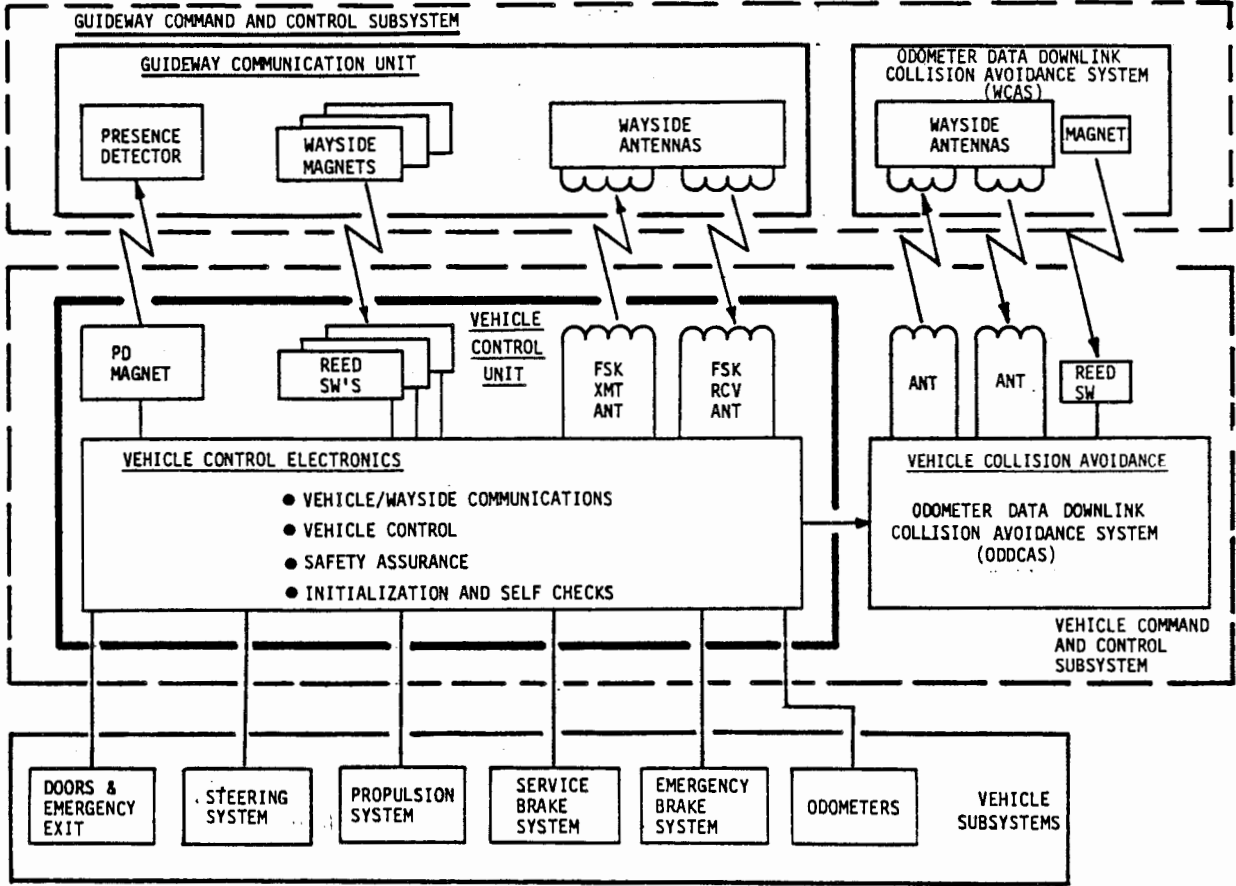
GUIDEWAY COMMAND AND CONTROL SUBSYSTEM (GCCS)

The GCCS is that portion of the control hierarchy responsible for the communications interface between station equipment and the vehicles on the guideway. The GCU contains an inductive communication link, a vehicle presence detection system, and magnetic guideway markers. This communications link also has the responsibility for providing failsafe speed limit information and safe-to-proceed (STP) control to the vehicles throughout the guideway.

A major part of the communication between the station and the vehicles is performed by equipment in a subsystem within the GCU called the Inductive Communication Subsystem (ICS). The ICS uses an inductively coupled link between the guideway and the station through which binary frequency shift keyed (FSK) data is transmitted and received. The coupling is accomplished by the use of wire loops embedded in the running surface of the guideway; these couple inductively with vehicle borne coil antennas. The loops and antennas provide both station to vehicle communication (uplink) and vehicle to station communication (downlink). Each guideway segment, which can be as long as 1000 feet in length, possesses a pair of such inductive loops: one in the right half of the guideway for uplinks, and one in the left half for downlinks. Associated with each loop pair is a set of inductive communication equipment to perform the FSK transmission and reception. Downlink messages are sent by vehicles only when prompted to do so by the wayside or when anomalous conditions occur which much be reported to the station. Uplink messages, on the other hand, are sent continuously with a safe-to-proceed (STP) signal encoded in the uplink. Presence of this STP signal is required by the VCCS before vehicle motion is permitted. Absence of this STP signal on a guideway loop results in an emergency stop of all vehicles over the loop. (STP removal is commanded by the Collision Avoidance System when a headway violation occurs.)

The GCCS software is basically the same as would be found in an urban system except in those areas not originally programmed for





VEHICLE COMMAND AND CONTROL BLOCK DIAGRAM

FIGURE 4.3-6

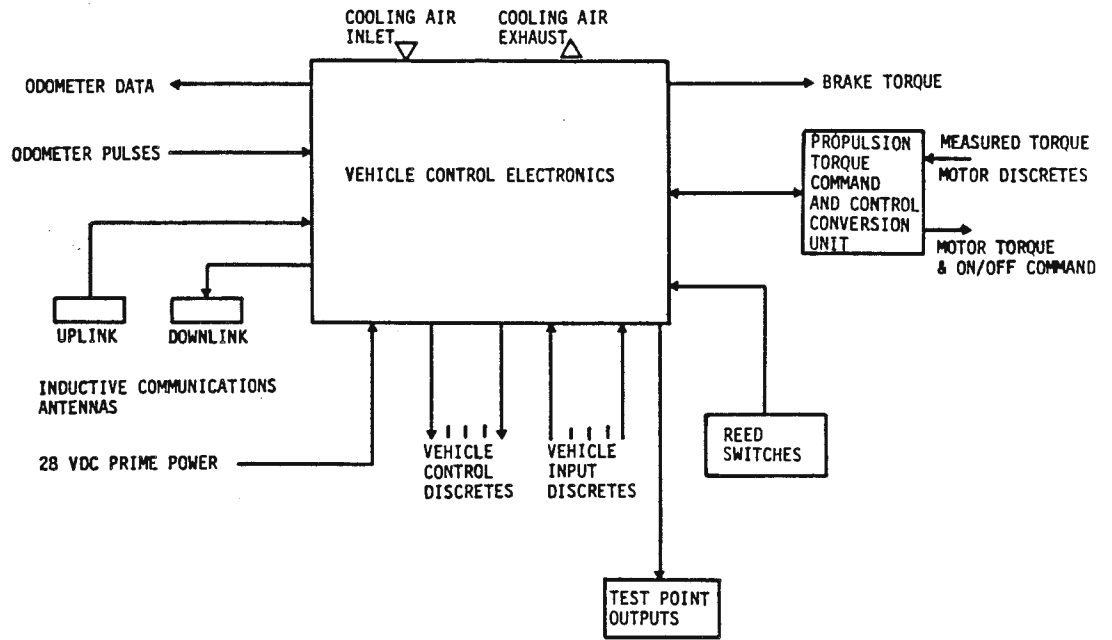
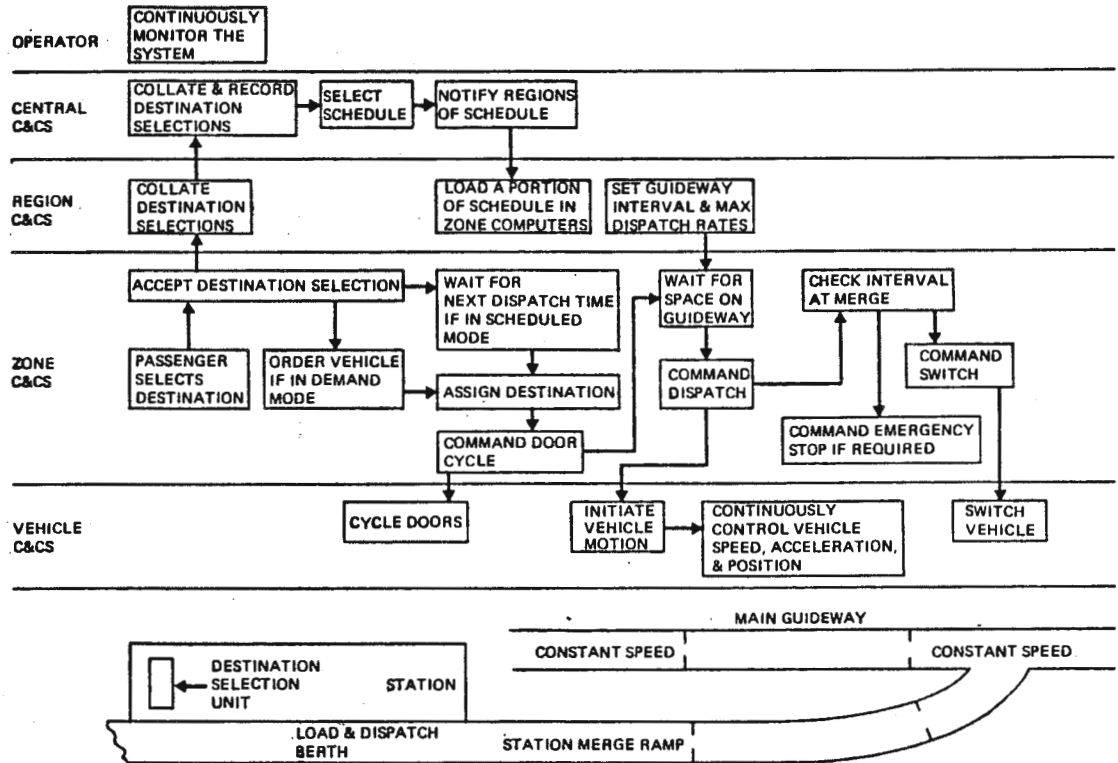
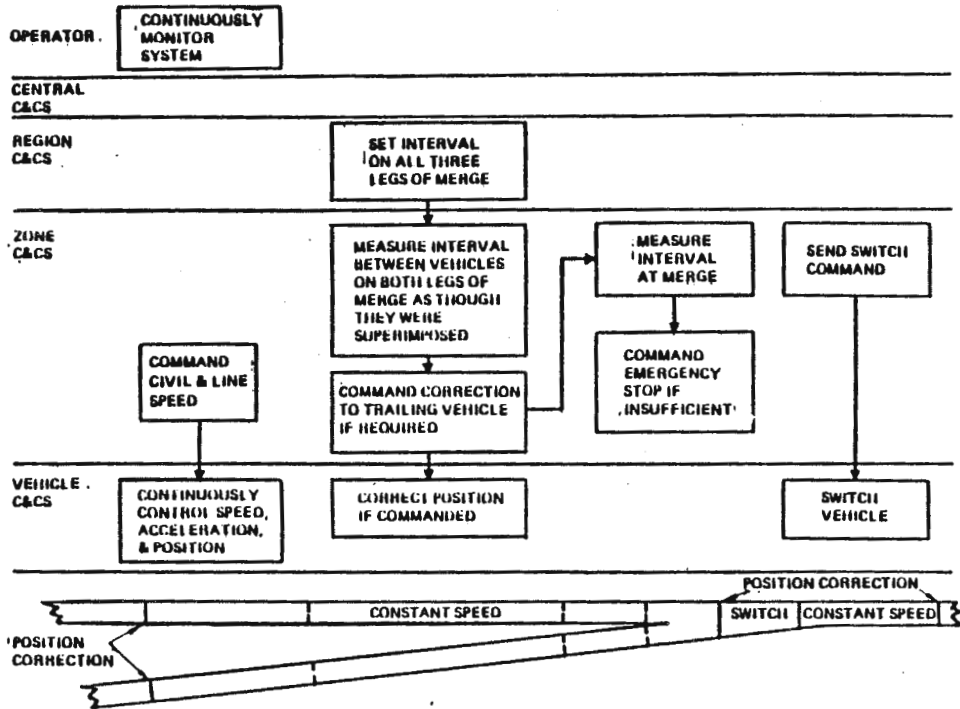


FIGURE 4.3-7 VEHICLE CONTROL ELECTRONICS INTERFACES



VEHICLE LOAD AND DISPATCH-URBAN SYSTEM
 FIGURE 4.3-8



CONTROL THROUGH A MERGE
FIGURE 4.3-9

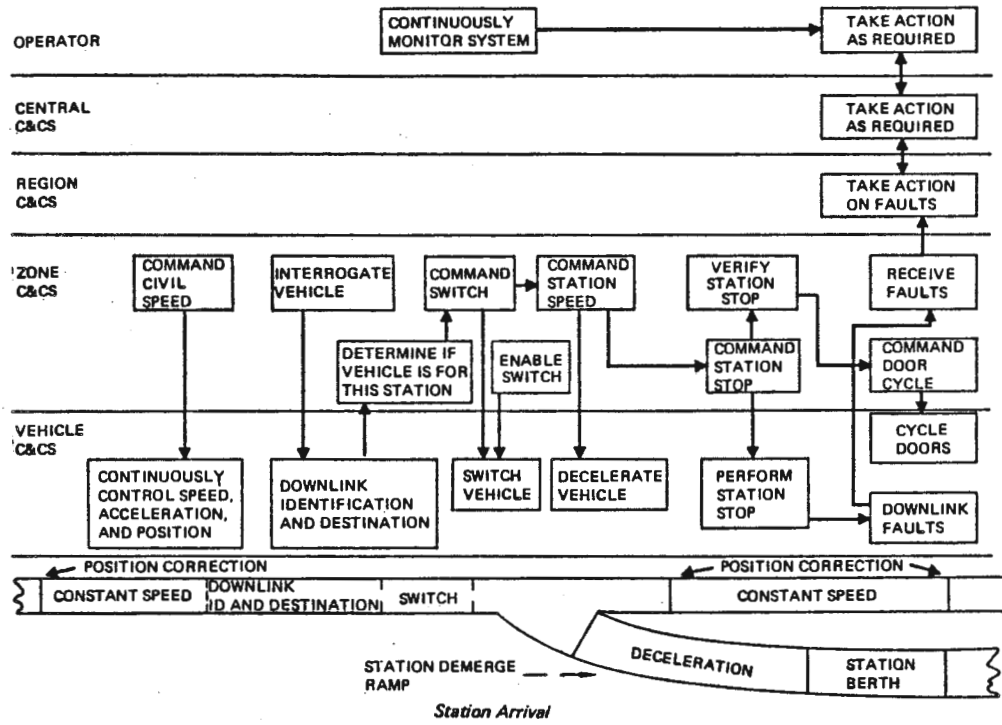


FIGURE 4.3-10

TABLE 2

FAILURE MANAGEMENT FUNCTIONS

DETECTION AND REPORTING

Vehicle

Exits not closed
VCCS power supply out of tolerance
Loss of microcomputer sanity
Speed or position error limit during closed-loop emergency braking
Wheel slide
Torque command disparity
Loss of service brake pressure supply
Loss of air suspension pressure
Reflectometer range limit
Loss of FSK carrier
FSK emergency brake command
Loss of reflectometer
Retention verification disparity
Motor polarity disparity
Loss of vehicle power
Battery voltage limit
Loss of pneumatic pump
Invalid FSK data
Loss of propulsion
Brake temperature limit
Reflectometer disparity
Speed limit violation
Propulsion overspeed
Retention command disparity
Reduced propulsion performance
Loss of propulsion redundancy
Loss of brake redundancy
Loss of one control microcomputer
Motor torque out of tolerance
Excessive brake/motor interaction
Brake pressure disparity
Speed error limit
Position error limit
Calibration factor limit
Odometer disparity
Excessive FSK errors

Guideway and Station

Speed/position disparity as measured by FSK checks, presence detectors
and ID magnets
Merge control reflectometer detected conflict
Station berth position error

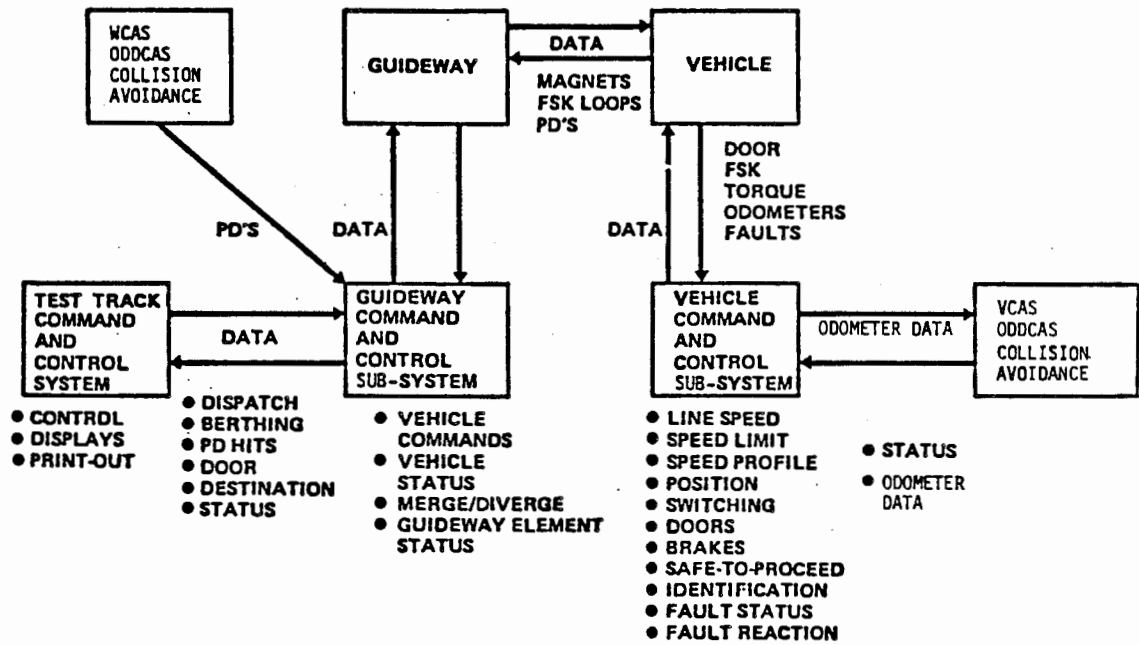
REACTION

Stop vehicle (emergency and normal rate)
Slow vehicle
Override guideway switching

RECOVERY

Remote reset/restart
Manual override control unit
Reduce performance

FIGURE 4.3-11 EDS BASELINE COMMAND AND CONTROL SYSTEM SYSTEM TRANSACTIONS



closed loop torque servo and provides propulsion and braking torques in the direction specified by commands from the VCCS.

Control of the motor is performed by an armature controller (chopper) for speeds up to 24 MPH. Beyond 24 MPH, the field controller (chopper) is used to control torque as commanded by the VCCS.

For regenerative braking, the armature chopper is shut down and the field controller is used to control braking torques down to 24 MPH. The field current is increased to increase braking torque.

GUIDEWAY AND STATION

Table 3 identifies major features of the baseline AGRT test track. Sufficient design trades were accomplished to assure that all vehicle/C&CS/guideway interfaces were identified. Mechanical interfaces included guidewheel/rail, capture wheel/rail, and power collector/power rail. Electrical and electronic interfaces included presence detectors, enabling magnets, and communication antenna loops. The designed and documented interfaces were applicable to a deployed system.

Requirements for the Power Distribution System were determined. This system would be similar to that provided at the zone level for an urban system.

Guideways and structures concepts and civil requirements were presented in the System Design Review of April 7, 1980.

The effort expended on the vehicle design and the EDS test track, as previously noted, determined operational parameters for the simulation program design effort. Section 7.0 provides a brief summary of the simulation program design.

5.0 PROGRAM AND SAFETY REVIEWS AND TECHNICAL INTERCHANGES

A logical, integrated series of formal reviews aided internal design discipline and fostered customer communication throughout the AGRT program. As noted earlier, these formal reviews are significant milestones: completion of a System Design Review (SDR), a Preliminary Design Review (PRD), or a Critical Design Review (CDR) constitutes authority to proceed with the next program activity.

This section covers the Quarterly Program Reviews, the System Safety Reviews, and the Technical Interchange meetings. (The SDRs, PDRs, and CDRs are covered in the following Section 6.0.)

The Quarterly Program Reviews provide formal interactive customer contact. Although they are called "quarterly" reviews, the actual frequency was dependent on program status. Also, design reviews and safety reviews replaced the quarterly reviews when appropriate. Quarterly Review material covered all aspects of our work, including:

Major analysis and synthesis results; design trades; incorporation of safety and program requirements; development test data and test plans; design and fabrication status (hardware and software); experienced or potential problems; pending changes; conclusions; proposed technical solutions and recommendations; and cost and schedule performance.

Safety reviews emphasized the importance of safety in the program. The reviews addressed the safety criteria and the methods and means by which the criteria was incorporated into the specifications, designs, and fabricated hardware and software.

Technical Interchanges were held throughout the program. These technical working sessions were periodic meetings, requested by either UMTA or ourselves, to review technical data, problems,

5.1 PROGRAM REVIEWS

Program reviews consisted of extensive prepared presentations. The reviews and excerpts from these reviews are noted below.

FIRST QUARTERLY REVIEW - September 29, 1979

This presentation was given in Washington, D.C. Attendees included representatives of the Department of Transportation - OST, Urban Mass Transportation Administration (UMTA), DOT-Transportation System Center (TSC), American Public Transit Association (APTA), Applied Physics Lab (APL) of Johns Hopkins University, MITRE Corp., and Battelle.

This program review covered the analysis phase activities. Figure 5.1-1, EDS specification major interfaces, was included in this presentation. It reflects how analysis phase activities shaped the EDS Specification and provided traceability to an urban deployed system.

Extensive design trades in all subsystems were presented. In Figure 5.1-2 are excerpts from the review showing AGRT Command and Control Systems, Inductive Communication System, Loop Driver Design Trades, and development tests.

QUARTERLY REVIEW - February 14, 1980

This quarterly review was presented to UMTA, MITRE, APL, Battelle, DOT-TSC, and DOT-OST at Boeing's Rosslyn, Virginia office. An overview of the program was presented to APTA at UMTA the previous day.

Figure 5.1-3 shows the review agenda and a presentation chart, "EDS Track Computer Configuration Utilizing BAC Capital Equipment". This chart reflects the BAC procurement of the Morgantown Software Development Integration Lab (SDIL) that was described in Section 4.3, Test Track Command and Control Subsystem.

FIGURE 5.1-2

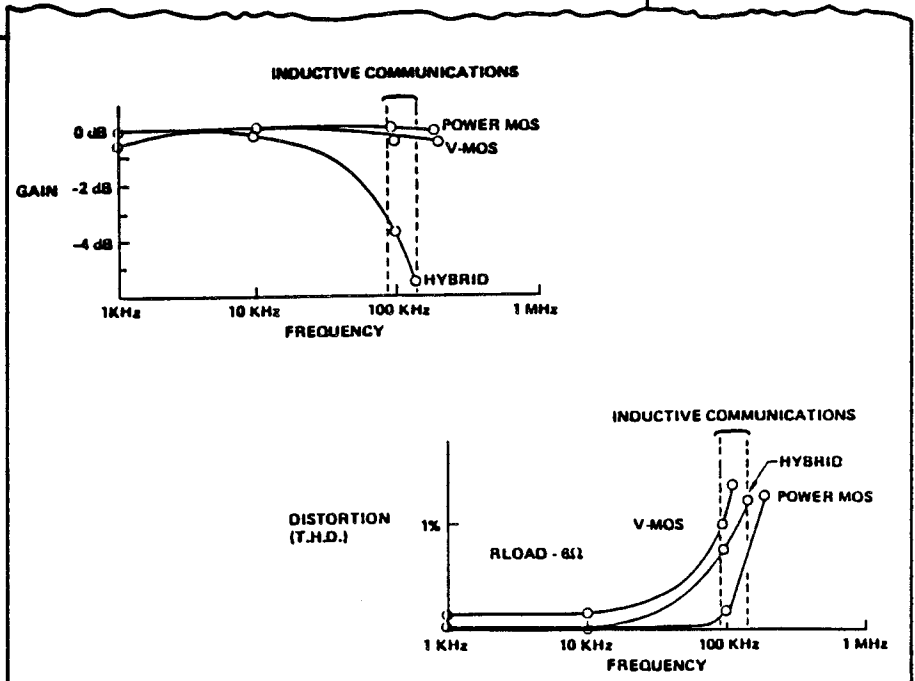
FIRST QUARTERLY REVIEW - AGRT UPLINK DRIVER

- MPM loop driver optimized for AGRT application (AGRT utilizes all FSK, eliminates low frequency tones)
 - Investigate alternatives including new technologies
 - Bipolar
 - Hybrid (phase II MPM)
 - V-MOS ▷
 - Power MOS
 - Breadboarded/evaluated potential designs
 - Hybrid
 - V-MOS
 - Power MOS
 - Preliminary recommendation
 - Utilize power MOS
 - Derate for reliability
- ▷ "Vertical metallic oxide semiconductor"

AGRT UPLINK LOOP DRIVER

THE MORGANTOWN UPLINK LOOP DRIVER HAS BEEN REDESIGNED FOR THE AGRT APPLICATION WHICH DELETES THE LOW FREQUENCY TONES FOR SAFETONE, SPEED TONE, STATION STOP (ETC.). SEVERAL NEW TECHNOLOGIES WERE INVESTIGATED AND TWO OF THESE WERE BREADBOARDED AND COMPARED WITH THE MORGANTOWN DESIGN.

BASED ON THE LOOP DRIVER TEST RESULTS SHOWN IN THE FOLLOWING FIGURES WHICH COMPARE THE DESIGNS AS A FUNCTION OF GAIN AND DISTORTION VS FREQUENCY, THE POWER MOS DESIGN IS RECOMMENDED. THE RELIABILITY OF THE POWER MOS DEVICE IS SUBSTANTIALLY IMPROVED IN THIS APPLICATION BY ITS DERATING.



(continued)

FIGURE 5.1-3

AGRT QUARTERLY REVIEW - FEBRUARY 14, 1980 AGENDA

- I. INTRODUCTION AND PROGRAM OVERVIEW
- II. PROGRAM SCHEDULE AND SCHEDULE STATUS
- III. FINANCIAL STATUS
- IV. TECHNICAL STATUS, PROGRESS, PLANS
 1. OVERVIEW OF CRITICAL TRADES, ANALYSES, STUDIES
 2. SYSTEMS ENGINEERING
 - a. EDS SPEC (TASK 6A)
 - b. EDS SYSTEM DESCRIPTION DOCUMENT (TASK 6)
 - c. SYSTEM CHARACTERISTICS STUDIES (TASK 9)
 3. DESIGN ANALYSIS/TRADE STUDIES (TASK 6A11)
 4. EDS DESIGN (TASK 14)
 - a. DESIGN ANALYSIS AND VERIFICATION
 - b. SYSTEMS ENGINEERING
 - c. COMMAND & CONTROL SYSTEM
 - 1) VEHICLE CCS
 - 2) GUIDEWAY CCS
 - 3) COLLISION AVOIDANCE SYSTEM (CASBAR)
 - 4) SOFTWARE AND COMPUTERS
 - d. VEHICLE DESIGN
 - e. VEHICLE PROPULSION AND ELECTRICAL
 - f. POWER DISTRIBUTION
 - g. GUIDEWAY AND STRUCTURES
- V. SUMMARY

EDS TEST TRACK COMPUTER CONFIGURATION UTILIZING BAC CAPITAL EQUIPMENT

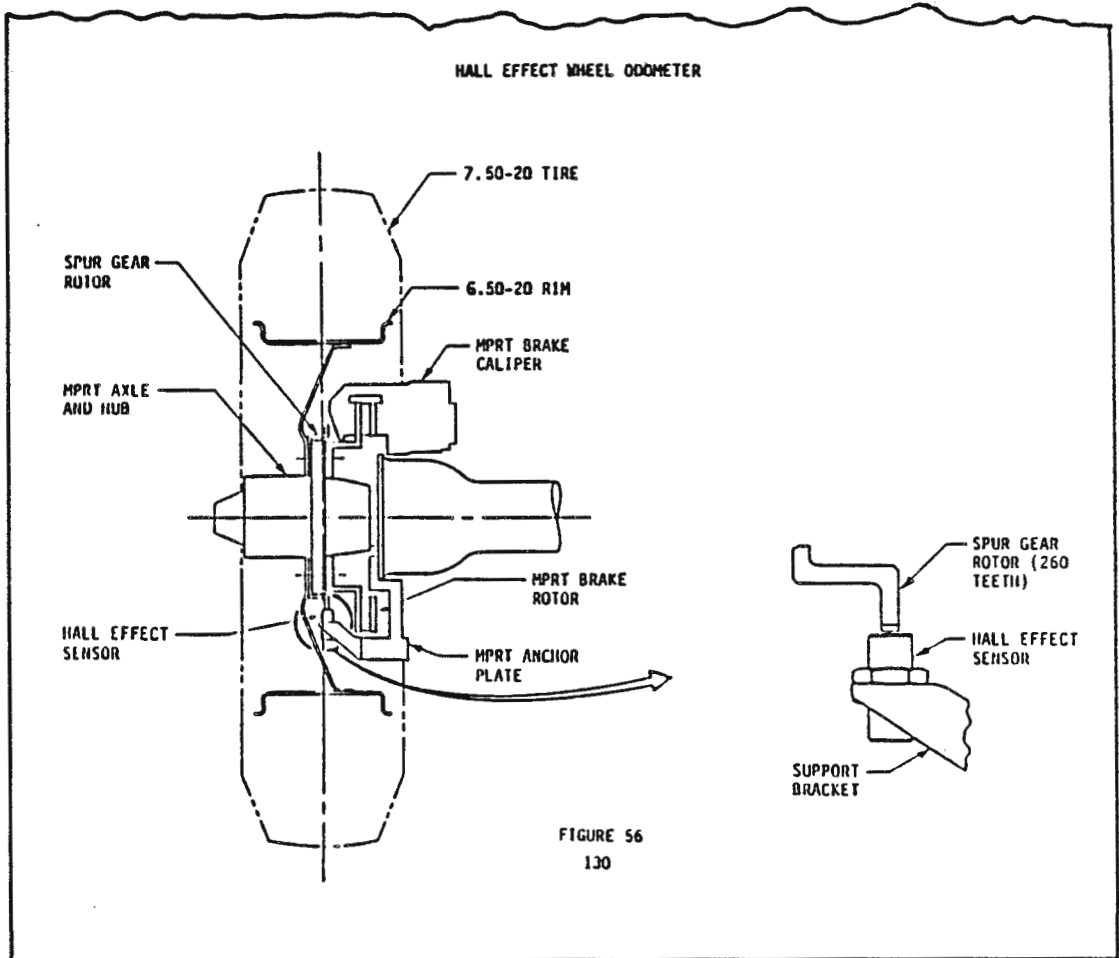
AS PART OF THE INITIAL PROPOSAL ACTIVITIES, THE COMPUTATIONAL REQUIREMENTS WERE ESTABLISHED FOR EDS. THESE REQUIREMENTS RESULTED IN THE PROPOSED SDIL FACILITY WHICH WAS PLANNED FOR USE IN DEVELOPING THE ZONE SOFTWARE AND SUBSEQUENTLY FOR OPERATING THE TEST TRACK. THE SDIL INCLUDED AN ECLIPSE S/250 COMPUTER AND A SMALL SET OF PERIPHERALS. DURING THE LAST QUARTER, AN OPPORTUNITY TO PURCHASE THE MORGANTOWN SOFTWARE DEVELOPMENT FACILITY HARDWARE OCCURRED. THIS FACILITY INCLUDED SEVERAL COMPUTERS AND A LARGE CADRE OF PERIPHERALS. AN EVALUATION OF THE MORGANTOWN FACILITY HARDWARE FOR AGRT USE INDICATED SEVERAL ADVANTAGES.

- THE ADDITIONAL HARDWARE (PRESENTED CONFIGURATION) ALLOWS US TO RETURN TO THE INITIALLY (DECEMBER 1978) PROPOSED CONFIGURATION WITH ITS ASSOCIATED LOWER DEVELOPMENT RISK AND ABILITY TO SEPARATE TEST TRACK SPECIFIC SOFTWARE FROM THAT ZONE SOFTWARE WHICH IS EXPANDABLE TO AN OPERATIONAL SYSTEM.
- THE NET COST IMPACT TO THE AGRT PROGRAM FOR THE EXPANDED HARDWARE FACILITY IS ZERO. THAT IS, WE SAVE THE DOLLAR AMOUNT WHICH WAS TO BE USED TO PURCHASE THE ECLIPSE, AND ITS PERIPHERALS; BUT WE MUST NOW SPEND MORE MONEY ON THE SUPPORT SOFTWARE. THE ADDITIONAL SOFTWARE COST IS NECESSITATED SINCE THE HOL IS NO LONGER OFF-THE-SHELF (AS IT WAS FOR THE ECLIPSE) AND ADDITIONAL EXECUTIVE SOFTWARE IS REQUIRED FOR THE EXPANDED CONFIGURATION. BOEING HAS PURCHASED THE MORGANTOWN SOFTWARE DEVELOPMENT FACILITY HARDWARE AND PLANS ON USING IT TO SUPPORT THE AGRT PROGRAM IN THE CONFIGURATION SHOWN.

FIGURE 5.1-4
AGRT QUARTERLY REVIEW - JULY 2, 1980 - HALL EFFECT

HALL EFFECT WHEEL ODOMETER

CONTINUED EVALUATION OF THE WIEGAND WIRE AND HALL EFFECT TECHNIQUES OF MEASURING WHEEL ROTATION DISTANCE AND VELOCITY HAS BEEN CARRIED OUT. TWO CONFIGURATIONS OF THE HALL EFFECT SENSOR HAVE BEEN TESTED. ONE LOOKED AT THE PERIPHERY OF A GEAR AND THE OTHER LOOKED AT THE SIDES OF A GEAR. THE TECHNIQUE OF LOOKING AT THE PERIPHERY OF THE GEAR HAS SHOWN A DEFINITE ADVANTAGE IN SO FAR AS CONSISTENT SIGNAL STRENGTH AND MINIMUM EFFECT OF VARYING AIR GAP ON SIGNAL STRENGTH. FIGURE 56 ILLUSTRATES THE HALL EFFECT DEVICE LOOKING AT THE PERIPHERY OF THE GEAR. AT THIS TIME THIS REPRESENTS THE MOST PROMISING CONFIGURATION FOR A WHEEL ODOMETER.



(continued)

FIGURE 5.1-5
AGRT QUARTERLY REVIEW - SEPTEMBER 22, 1980 - C&CS TRADES

GCCS DESIGN ANALYSES AND TRADES

- LOOP DRIVER DESIGN REVIEW AND ANALYSIS
- GUIDEWAY CONTROLLER - PROCESSOR ANALYSIS
- DATA HANDLING INTERFACES REVIEW

C&CS TRADES

COMMON TO GCCS AND VCCS

FSK MESSAGE LENGTH/DATA ENCODING TECHNIQUE
FSK UPLINK/DOWNLINK DATA RATES
FSK MODULATION TECHNIQUES
FSK TRANSMITTER DESIGN STUDY
FSK RECEIVER DESIGN STUDY
MAGNETIC SIGNALLING ANALYSIS
FAILURE MODES AND EFFECTS ANALYSIS
PERIPHERAL PROCESSOR SELECTION
PRIMARY PROCESSOR SELECTION

FIGURE 5.1-6
AGRT PROGRAM OVERVIEW - MAY 20, 1983 - LCS ANALYSIS

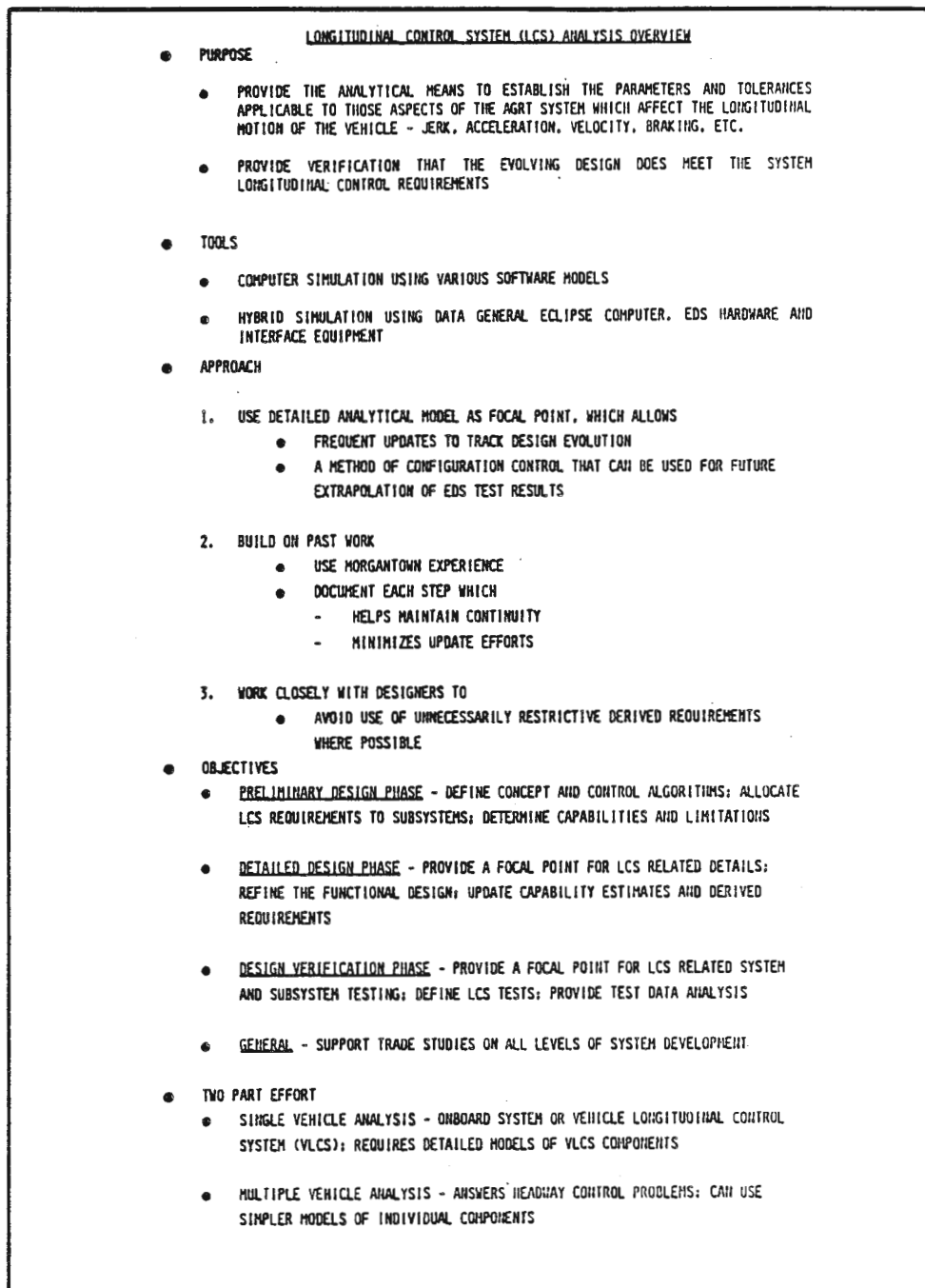
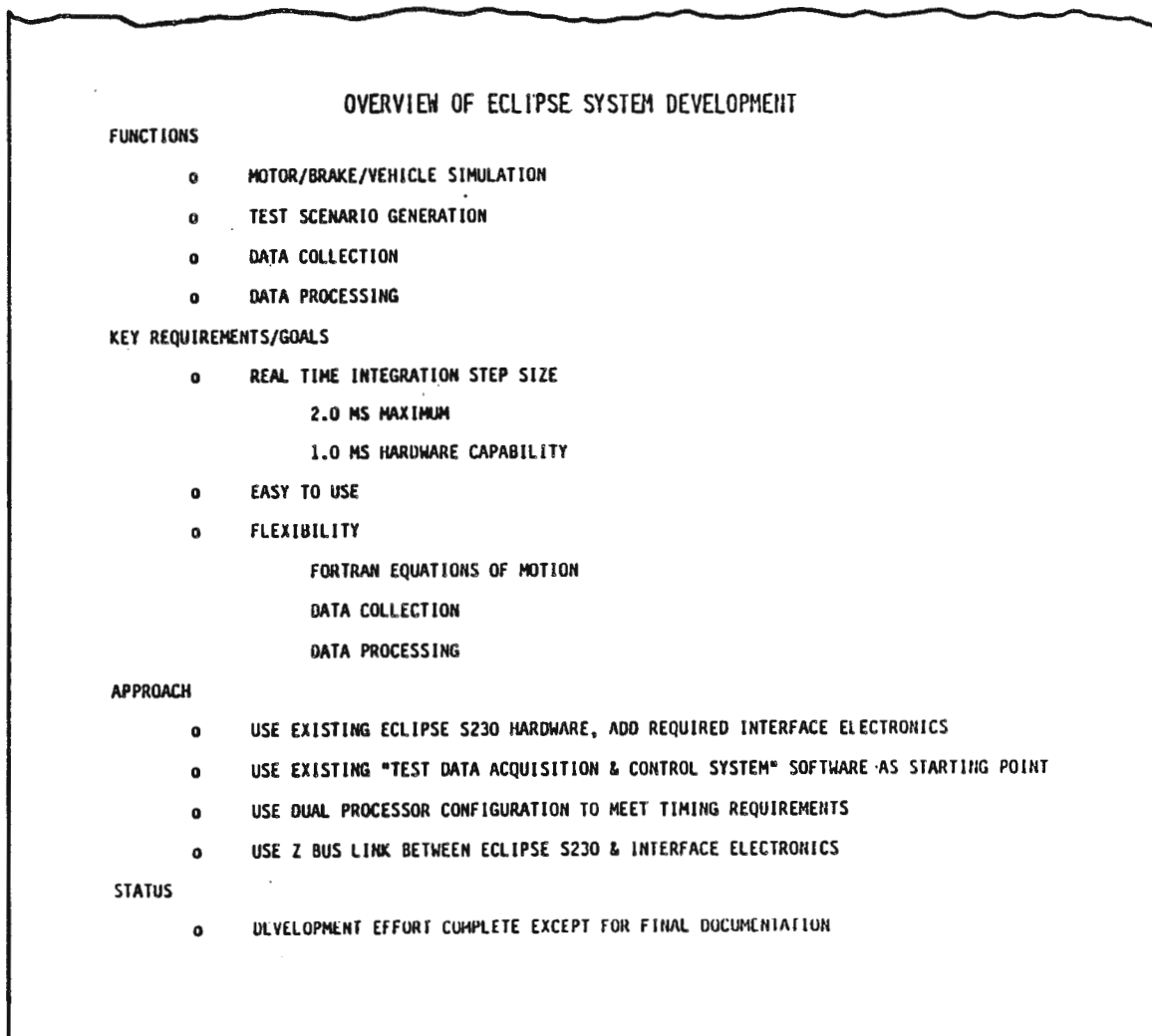


FIGURE 5.1-7 (continued)



numerical safety allocations. The monthly report added that Battelle was furnished with copies of the Nuclear Regulatory Commission handbook on Fault Tree analysis. This analysis technique was discussed at the CAS Safety meeting in hopes of a better understanding of our numerical approach to safety analysis and requirements.

The AGRT Collision Avoidance System (CAS) Safety Data was organized in four sections as follows:

- 1.0 Introduction and Summary - A quick look at the Boeing design process, the overall safety criteria, and the conceptual approach for the baseline system.
- 2.0 System Engineering Analysis,
- 3.0 CAS Safety System - This is the main body of technical data relating to the design process, the safety program and safety requirements, and the design concept and safety criteria for the vehicle CAS (VCAS) and the merge/diverge CAS (WCAS).
- 4.0 Technical appendices as follows:
 - o CAS Fault Tree analysis (including WCAS concept -qualitative safety evaluation).
 - o Dissimilar software approaches
 - o Functional allocation to EDS specification paragraphs

VEHICLE SEPARATION ASSURANCE SYSTEM REVIEW - December 2, 1981

This review, attended by Sperry and UMTA, was presented at Boeing's Rosslyn, Virginia office.

The objectives of the review were:

- o To describe the vehicle-to-vehicle collision avoidance safety system.

FIGURE 5.2-1
SAFETY REQUIREMENTS - SENSOR SIGNAL SELECTION

THE SAFETY ANALYSIS CONCLUDES THAT THE SENSOR SIGNAL SELECTION CONCEPT FOLLOWS SAFETY CRITERIA. IMPLEMENTATION SHALL MEET THE FOLLOWING REQUIREMENTS:

- o THE COMPARISON FUNCTIONS (DISPARITY DETECTION) SHALL BE EITHER
 - o FAIL-SAFE (UNSAFE FAILURE < 1 IN A MILLION YEARS)
 - OR
 - o PERIODICALLY CHECKED (VERIFY UNEQUAL INPUTS GENERATES A DISPARITY)
- o THE SELECTION FUNCTION (VOTERS) SHALL BE EITHER
 - o FAIL-SAFE (UNSAFE FAILURE < 1 IN A MILLION YEARS)
 - OR
 - o PERIODICALLY CHECKED (VERIFY THAT SAFEST SIGNAL WILL BE SELECTED)
- o REDUNDANT SIGNAL SENSORS AND PROCESSORS SHALL BE ISOLATED FROM EACH OTHER TO PREVENT A FAILURE IN ONE PROPAGATING TO THE OTHER
- o UNSAFE COMMON OR CORRELATED FAILURES THAT COULD GO UNDETECTED SHALL MEET THE SAFETY CRITERIA

FIGURE 5.2-3

FINAL SAFETY REVIEW AGENDA - SEPTEMBER 24, 1984

TIME	SUBJECT
8:30 A.M.	I. INTRODUCTION
10:00 A.M. 10:15 A.M.	PURPOSE OF REVIEW AND SCOPE HISTORICAL CONTEXT Contractual Requirements for Safety Program Directives SDR's System Safety Review - 10/5/82 PDR's and CDR's Contract Mod 28 Summary of Present Program
11:30 A.M.	II. SYSTEM SAFETY METHODOLOGY
	BASIC CONCEPT HI-TECH APPLICATIONS SAFETY INDEPENDENT OF CONTROL TEST LEVELS AND CONFIDENCE
12:00 Noon	III. SYSTEM LEVEL SAFETY VERIFICATION REQUIREMENTS (LUNCH)
1:00 P.M.	IV. SYSTEM SAFETY REQUIREMENTS, DESIGN APPROACH, AND VERIFICATION DATA
2:30 P.M. 2:45 P.M.	(SYSTEM SPEC. SECT. 2) Break
4:30 P.M.	(End of First Day)

SEPTEMBER 25, 1984 (Second Day)	
TIME	SUBJECT
8:30 A.M.	V. SUBSYSTEM SAFETY REQUIREMENTS, DESIGN APPROACH, AND VERIFICATION DATA
10:00 A.M. 10:15 A.M.	(SYSTEM SPEC. SECT. 3) Break
12:00 Noon	(LUNCH)
1:00 P.M.	VI. TEST FUTURE Safety Related Tests
2:30 P.M. 2:45 P.M.	Break
	VII. CONCLUSIONS, SUMMARY Lessons Learned
4:00 P.M.	VIII. ACTION ITEM REVIEW (As Required)

- FINAL SYSTEMS SAFETY REVIEW DATA PACKAGE**
- I. LIST OF SAFETY RELATED PROJECT MEMOS & OTHER REFERENCES
Titles and Abstracts (includes System Engineering, Staff-Design Analysis, and C&CS Design).
 - II. COPIES OF PROJECT MEMOS LISTED
 - III. PROFESSIONAL PAPERS AS FOLLOWS:
 - o "A Distinct Software Implementation in a Vehicle Controller," W. E. Greve and R. J. Schroder presented at 33rd IEEE Vehicle
 - IV. REFERENCE DOCUMENTATION
 - o Report No. UMTA-MA-06-0048-80-9, "Morgantown People Mover Collision Avoidance System Design Summary," R. J. Schroder and
 - V. SAFETY RELATED SECTIONS FROM VCU AND GCU CDR'S

All previous action items on the EDS specification were resolved. Traceability to an urban deployed system through the EDS quality assurance tables was agreed upon. The Boeing "Stopping Distance Report" was reviewed and three action items were assigned. One action to standardize emergency braking terms was generated following the safety review. We agreed to present our design control process at SDR. UMTA/MITRE took two action items for miscellaneous changes to the UMTA/MITRE specification.

A Technical Interchange meeting, attended by UMTA, MITRE, and Battelle, was held in Seattle the week of November 3, 1980. This meeting's agenda was as follows:

- Define Traceability
- Worst Case Stopping Scenario
- Safety Design Philosophy
 - Functional Block Diagrams
 - Hardware Conceptual Block Diagrams
- Verification
 - FMEA (Failure Modes and Effects Analysis)
 - Safety Traceability

Figure 5.3-1, Safety Design Philosophy, was included in the detailed T.I. minutes transmitted to UMTA November 14, 1980.

A T.I. meeting was held between Boeing and Battelle in Columbus, Ohio during February 2-6, 1981 to address safety concerns. Areas discussed included:

- o Baseline Description Documentation
- o Safety Goals/Criteria
- o Communication Methodology - (Fault Tree Based)
- o Battelle Approach to Safety Analysis - Qualitative
- o Boeing Approach to Safety Analysis - Quantitative
- o Review of Quantitative Criteria

- o Collision Avoidance Concept (Separation Assurance)
- o Software Development Plan
- o Battelle AGRT Safety Criteria Document
- o Philosophy for getting through Safety Approval Gates (Minimize Resets)

Additional information was provided to Battelle relative to motor overtorque safety concerns.

The "AGRT Collision Avoidance System Safety Data Package", noted previously in safety reviews, was the result of several weeks of interactive work with Battelle, MITRE, and Sperry. Technical Interchange meetings were held in Columbus and Seattle in February and March of 1980 in which the CAS design methodology, safety criteria, and design concept were reviewed. It should be noted that the CAS safety criteria developed for the Sperry CASBAR were applicable to the Boeing ODDCAS design.

TECHNICAL INTERCHANGES - BOEING/SPERRY - CASBAR

The baseline Collision Avoidance System (CAS) identified as the baseband reflectometer system was briefly noted in Section 4.3. This system was closely monitored by Boeing through Technical Interchanges; a few interchanges included UMTA and Battelle. The initial interchange, documented June 9 and 10, 1980, was followed by others throughout 1980, 1981, and 1982. The concluding T.I. was held on January 28, 1983.

Figure 5.3.2 contains extracts of the minutes of the Technical Interchange meeting of October 30 and 31, 1981.

TECHNICAL INTERCHANGES - ALTERNATIVE COLLISION AVOIDANCE SYSTEM (CAS)

A Technical Interchange meeting held in Seattle, September 14, and 15, 1981 discussed in detail the alternative CAS systems that we studied and documented per UMTA's direction. (See Figure 5.3-3)

Technical Interchanges provided a means to resolve in-depth technical problems prior to formal reviews noted in Section 6.0

FIGURE 5.3-3
TECHNICAL INTERCHANGE - CAS ALTERNATIVE
CONCEPT EVALUATION TABLES

REFLECTOMETER

CRITERION	OVERALL EVALUATION			RATIONALE
	MARGINALLY ACCEPTABLE	ACCEPTABLE	VERY GOOD	
<ul style="list-style-type: none"> • PERFORMANCE • DEVELOPMENTAL COST • CAPITAL PLUS O&M COST • DEPENDABILITY • SAFETY • TECHNICAL RISK 		X X X	X X X	LOW SPEED VERSATILITY SURFACE WAVEGUIDE DESIGN CONCERNS COMMONALITY WITH ONBOARD CASBAR UNITS IN MERGE/DIVERGE ONLY CHECK FEATURES EMBEDDED IN THE CONCEPT SURFACE WAVEGUIDE DESIGN CONCERNS

PRESENCE DETECTORS

CRITERION	OVERALL EVALUATION			RATIONALE
	MARGINALLY ACCEPTABLE	ACCEPTABLE	VERY GOOD	
<ul style="list-style-type: none"> • PERFORMANCE • DEVELOPMENTAL COST • CAPITAL PLUS O&M COST • DEPENDABILITY • SAFETY • TECHNICAL RISK • SUBSTITUTABILITY 	X X X	X X	X X	POOR SPEED VERSATILITY DESIGN PRINCIPLES ARE APPLIED IN W. VA. PARTS COUNT PARTS COUNT FALSE CHECKOUT AND LOST MAGNET CONCERNS DESIGN PRINCIPLES ARE APPLIED IN W. VA. PARTS COUNT

GATES AND PRESENCE DETECTORS

CRITERION	OVERALL EVALUATION			RATIONALE
	MARGINALLY ACCEPTABLE	ACCEPTABLE	VERY GOOD	
<ul style="list-style-type: none"> • PERFORMANCE • DEVELOPMENTAL COST • CAPITAL PLUS O&M COST • DEPENDABILITY • SAFETY • TECHNICAL RISK • SUBSTITUTABILITY 	X X X X X	X	X	SUPERIOR SPEED VERSATILITY GATE AND SENSDR DESIGN CONCERNS EXCESSIVE PARTS COUNT EXCESSIVE PARTS COUNT FALSE CHECKOUT AND GATE CONCERNS GATE AND SENSOR DESIGN CONCERNS ONBOARD CASBAR NEEDED - HIGH PARTS COUNT

ODOMETER DATA DOWNLINK

CRITERION	OVERALL EVALUATION			RATIONALE
	MARGINALLY ACCEPTABLE	ACCEPTABLE	VERY GOOD	
<ul style="list-style-type: none"> • PERFORMANCE • DEVELOPMENTAL COST • CAPITAL PLUS O&M COST • DEPENDABILITY • SAFETY • TECHNICAL RISK • SUBSTITUTABILITY 		X X X X	X X	SPEED VERSATILITY TIME MULTIPLEX FEATURE VEHICLE-BORNE PARTS COUNT VEHICLE-BORNE PARTS COUNT CHECK FEATURES EMBEDDED IN THE CONCEPT HEXADECIMAL MESSAGE ERROR CHECKS WAYSIDE PARTS COUNT IS RELATIVELY LOW

WIGGLE WIRE

CRITERION	OVERALL EVALUATION			RATIONALE
	MARGINALLY ACCEPTABLE	ACCEPTABLE	VERY GOOD	
<ul style="list-style-type: none"> • PERFORMANCE • DEVELOPMENTAL COST • CAPITAL PLUS O&M COST • DEPENDABILITY • SAFETY • TECHNICAL RISK • SUBSTITUTABILITY 		X X X X	X X	SPEED VERSATILITY FREQUENCY MULTIPLEX FEATURE VEHICLE AND WAYSIDE PARTS COUNT VEHICLE AND WAYSIDE PARTS COUNT WEAKNESS OF REASONABLENESS CHECKS AND POSSIBILITY OF UNDETECTED CUMULATIVE POSITION ERRORS ANTENNA SIZE AND ASYNCHRONOUS PROCESSING WAYSIDE PARTS COUNT COMPARATIVELY LOW

6.1 SYSTEM DESIGN REVIEWS

System Design Reviews (SDR) establish the contract functional baseline. Phase IIA mission analysis and Phase IIB analysis activities, as noted in Section 4.1, Figure 4.1-2, were the source for development of the initial system specification and two subsequent iterations. The SDR presentation provides the definition of the system, its physical, and functional requirements. The system specification is released and placed under configuration control following completion of action items and approval of the SDR. Normally, a program would have one SDR. Because the EDS system was significantly changed after the initial baseline, we had two SDRs:

The baseline contract SDR called for two new AGRT vehicles (with MPM modules) and testing on a new AGRT test track.

The second SDR was required by the program restructuring that replaced the two new AGRT vehicles with two modified "MPM" vehicles, and used the existing test track rather than the AGRT test track.

At this juncture, the nature of the program restructuring can be brought into sharper focus. This restructuring, necessitated by continuing funding limitations was never precipitous. All restructuring efforts were the result of alternate proposals that we prepared and presented to UMTA.

Throughout this restructuring, every effort was exerted to preserve the technical thrust of the critical technologies identified as the Vehicle Longitudinal Control System (VLCS) and the Collision Avoidance System (CAS).

This preservation is reflected in an examination of the initial and two superseding specifications relating to the VLCS and CAS. The performance envelope of the modified "MPM" vehicle was slightly degraded from that of the AGRT vehicle, but the VLCS and CAS

FIGURE 6.1-1

AGRT - SDR/QUARTERLY REVIEW DATA PACKAGE AND AGENDA

Gentlemen:

Enclosed are eight copies of the preliminary system design review (SDR)/Quarterly Review data package, in accordance with Article II paragraph C Item 1 and 2M of the subject contract. This data package is in accordance with our commitments made during the technical interchange meetings of March 3 through 6. The package includes the following:

- (1) EDS Specification - SS362-90000-2C
- (2) EDS Interface Specification S362-90001-1
- (3) EDS Documentation Plan D362-60002-1 Rev. A
- (4) Draft Charts of Quarterly/System Design Review
- (5) Package explaining the Boeing Design Control Process
- (6) A list of analysis and trades which are required prior to preliminary design reviews (PDR's). The applicable PDR's are scheduled to be held in late 1980 per the subject contract. A matrix of the previously noted analysis and trades vs the system, subsystem and procurement specifications is in preparation.
- (7) Preliminary civil requirements review package

The data package as noted above is for your review prior to the SDR to be held during the week of April 7, 1980.

THIRD QUARTERLY REVIEW AND SYSTEM DESIGN REVIEW OUTLINE

- I. PROGRAM SCHEDULE PAGE 1
- II. AGRT SUMMARY AND REVIEW PAGE 7
 1. AGRT GOALS AND OBJECTIVES
 2. BOEING AGRT CONCEPT
 - a. SYSTEM EVENT DIAGRAM
 - b. IMPLEMENTATION CONCEPTS - AGRT SUBSYSTEMS
- III. REVIEW OF EDS DESIGN PAGE 17
 1. EDS PROGRAM OBJECTIVES
 2. GENERAL EDS REQUIREMENTS
 3. EDS EVENT DIAGRAM AND FUNCTIONAL ANALYSIS
 4. EDS CONCEPT - SYSTEM LEVEL DESCRIPTION
 5. EDS PROGRAM CONTROLS
 - a. DEVELOPMENT OF SPECIFICATIONS AND DOCUMENTATION
 - b. CHANGE AND CONFIGURATION CONTROL
 - c. VERIFICATION OF COMPLIANCE
 6. EDS SYSTEM AND INTERFACE CONTROL SPECIFICATIONS
 - a. EDS SPECIFICATION
 - 1) PURPOSE
 - 2) PREPARATION
 - 3) ORGANIZATION
 - b. EDS INTERFACE CONTROL SPECIFICATION
 - 1) PURPOSE
 - 2) PREPARATION
 - 3) ORGANIZATION
 - c. AGRT (UMTA) SPECIFICATION - IMPLEMENTATION AT EDS
 - 1) PERFORMANCE
 - 2) DEPENDABILITY
 - 3) SAFETY
 - 4) COST
- IV. MAJOR ANALYSES AND TRADE STUDIES PAGE 67
 1. HEADWAY AND STOPPING DISTANCE
- V. DESCRIPTION OF EDS SUBSYSTEM CONCEPTS PAGE 83
 1. COMMAND AND CONTROL SYSTEM (C&CS)
 2. SOFTWARE AND COMPUTERS
 3. VEHICLE REQUIREMENTS
 4. POWER DISTRIBUTION
 5. GUIDEWAY AND STRUCTURES 167 THRU 210

No SDR was held for the laboratory simulation that was subsequently programmed to support VCU verification testing. However, action was initiated to upgrade the Software Development Integration Lab (SDIL) and the VCU Test Set. The SDIL and VCU Test Set were in place and supported VCCS, GCCS, and ODDCAS development testing. VCU single string integration testing was in process.

Recognizing the importance of the upgraded VCU Test Set to support VCU verification testing, a VCU Test Set design review was held March 14, 1984.

The VCU Test Set design review addressed the continuing requirement of verifying VLCS and CAS specifications traceable to a deployed system. System Specification SS362-90000-4 (superseding SS362-90000-3C) delineated the specifications of AGRT-EDS-C³ to be verified through simulation testing.

Figure 6.1-3 from this review notes that the only major categories of testing that weren't covered by simulation testing were lateral control (captive steering), door control, and interfaces (physical).

FIGURE 6.2-1

TEST TRACK SOFTWARE AND
VCU PDR DATA PACKAGE AND AGENDA

Gentlemen:

Enclosed is the agenda and data package for the Test Track Software and VCU Preliminary Design Reviews (PDR) to be held at our facility in Seattle, February 2 through 4, 1982.

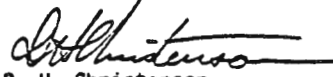
The scheduled PDRs are in accord with program schedules.

The PDRs will provide the technical basis for the detail design of the Test Track Software and the VCU. The detail design will be presented at the Critical Design Reviews (CDR).

The subject PDRs are based on the subsystem requirements as contained in the system specification and as established at the System Design Review. Accordingly, no review of system requirement analysis will be included.

If we can assist you in any way with travel reservations, please advise.

Very truly yours,



D. H. Christenson
AGRT Program Manager
Automated Transportation Systems

TEST TRACK SOFTWARE PDR AGENDA - FEBRUARY 2, 1982

ITEM	SPEAKER	TIME
● Introduction	Dick Alberts	} 8:30 A.M. - 9:30 A.M.
● Schedule	Dick Alberts	
● Requirements	Dick Alberts	
● Correlation to -3 Systems Specification		
● Development Plan	Dick Alberts	
● Preliminary Design		
● Executive Software		
- System Startup	Bob Berg	} 9:45 A.M. -
- TCP Operating System	Bob Berg	} 10:45 A.M.
● Application Software		
- Test Management	John Neider	10:45 - 11:45 A.M.
- Guideway Management	Bob Schroder	1:00 - 2:00 P.M.
● Analysis		
● Critical Algorithms and Processes	Bob Schroder, Bob Berg	} 2:00 P.M.
	John Neider, Steve Cuspard	
● Time and Memory Estimates	Bob Schroder	} 4:00 P.M.
● Conceptual Test Plan	Bob Schroder	
● Schedule of Activities to CDR	Bob Schroder	
● Action Item Review and Concluding Remarks	Dick Alberts	

(continued)

FIGURE 6.2-2

TEST TRACK/S/W AND VCU PDR ACTION ITEM CLOSURES

Included in the presentation data forwarded in the reference letter were action items identified and assigned during the test track software and VCU PDR. The VCU action item 9, "Provide System Change Notices (SCN's) to correct system specification inconsistencies" was completed and closed with SCN's coordinated, released and enclosed in the reference.

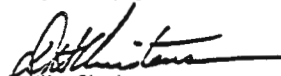
This letter includes data, as noted on the attachment, which coordinated, and closed further action items.

The "Action Item Closure Confirmation" format included in the data was used as a vehicle to coordinate analysis and obtain concurrence by all AGRT technical support functions.

We will respond to any questions you may have regarding the enclosed material.

Closure action will be provided on all action items still open.

Very truly yours,



G. H. Christenson
AGRT Program Manager
Automated Transportation Systems

TEST TRACK SOFTWARE PDR ACTION ITEMS CLOSURE DATA (*)

Action Item No. 1	Action Item Closure Confirmation
Action Item No. 2	Action Item Closure Confirmation
Action Item No. 3	Action Item Closure Confirmation
Action Item No. 4	Action Item Closure Confirmation Memo 2-1033-SYST-093 Dt'd 2-16-82
Action Item No. 5	Action Item Closure Confirmation Memo 2-1033-SW&C-037 Dt'd 2-16-82

VEHICLE CONTROL UNIT PDR ACTION ITEMS CLOSURE DATA (*)

Action Item No. 1	Action Item Closure Confirmation Memo 2-1033-C&CS-122 Dt'd 2-9-82
Action Item No. 2	Action Item Closure Confirmation Memo 2-1033-SYST-092 Dt'd 2-23-82 Rev. A

Action Item No. 9	Previously Closed
-------------------	-------------------

* System Design - R. E. Alberts includes Software, Vehicle and Design Analysis functional concurrence if not specifically noted.

System Engineering - F. Burns includes Safety confirmation if not specifically noted.

(continued)

report, without the engineering effort expended on vehicle requirements and design to define the C&CS interfaces. This PDR identified how the allocation of system requirements would be incorporated into the vehicle design.

The Manual Override Control Unit (MOCU) allows operation of a vehicle without the VCU. The AGRT MOCU design was based upon the MPM MOCU. The AGRT MOCU was fabricated to support acceptance testing of the propulsion unit.

The EDS brake amplifier was designed and built. This unit allowed implementation of the brake amp function with an AGRT VCU but using the MPM vehicle. The brake amp was also a component of the VCU test set-up.

Figure 6.2-3 is a small sample of data from this PDR pertinent to vehicle design. The PDR delineated vehicle design activities to CDR. On March 1, 1983, the Randtronics subcontract was completed with delivery of two tested propulsion systems.

GUIDEWAY COMMAND AND CONTROL SUBSYSTEM PDR - December 20 - 21, 1982

The GCCS PDR delineated flow down of requirements from the system specification to the GCCS specification, S362-90011-1. Figure 6.2-4, from the presentation, shows an example of flow down of requirements from the system specification to subsystem specifications.

Figure 6.2-5, GCCS PDR outline, reflects the organization and comprehensive coverage of the presentation. Figure 6.2-6 is a sample of action item identification and closure.

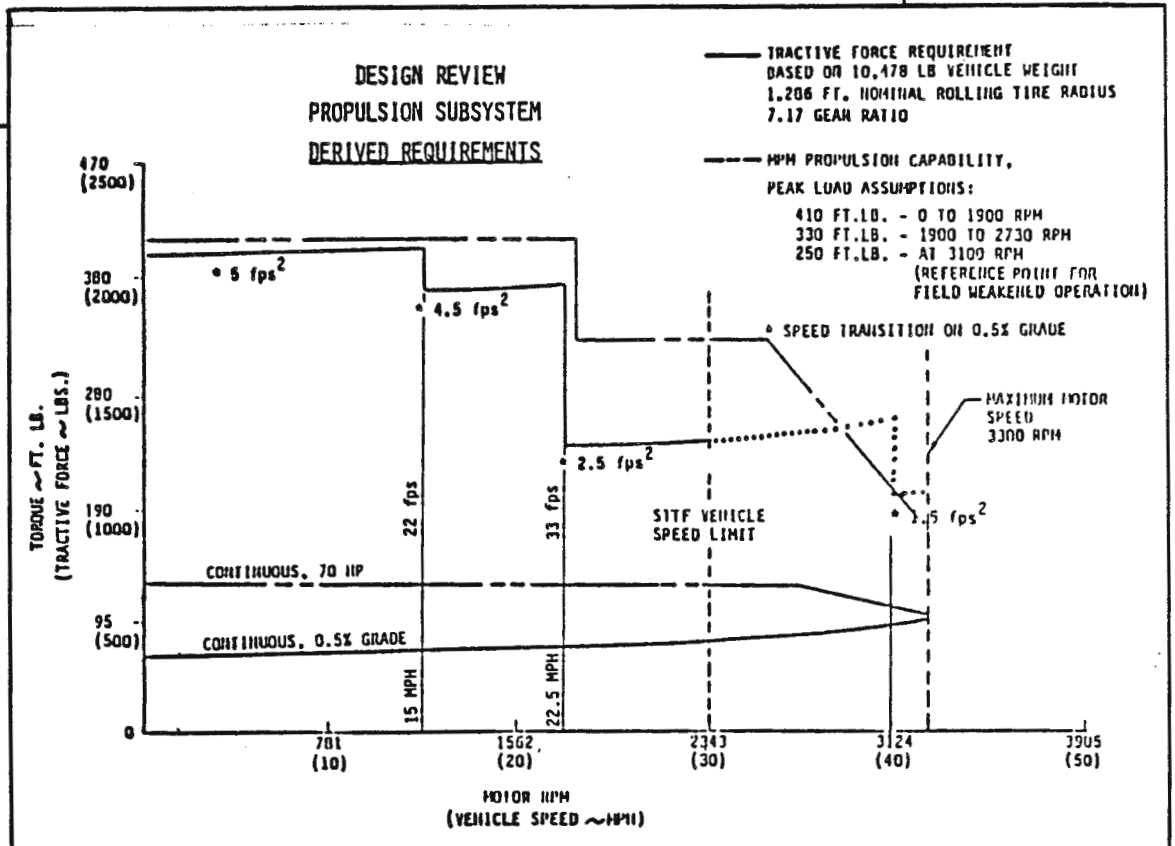
ODOMETER DATA DOWNLINK COLLISION AVOIDANCE SYSTEM PDR

July 27 - 28 1983

The ODDCAS PDR was presented at UMTA's offices in Washington, D.C. In January, 1983 UMTA issued contract modifications which

FIGURE 6.2-3 (CONTINUED)

<u>TRADE STUDIES</u>		
	<u>MPRT II</u>	<u>EDS</u>
HYDRAULIC SYSTEM		
PRESSURE INDICATION	PRESSURE SWITCH 250 PSI (2 EACH)	200 PSI TRANSDUCER (2 EACH)
	PRESSURE SWITCH 340-380 PSI	1000 PSI TRANSDUCER
	PRESSURE SWITCH 380-430 PSI	1000 PSI TRANSDUCER
REASON FOR CHANGE:		
PRESSURE SWITCHES INDICATE THAT PRESSURE IS EITHER BELOW OR ABOVE PRESSURE SETTING WHILE TRANSDUCER INDICATES PRESSURE AT ALL TIMES WHICH GIVES BETTER ANOMALY MANAGEMENT. USED ALSO FOR TEST INSTRUMENTATION		
PRESSURE LIMITING		PRESSURE LIMITER FOR REAR BRAKES SET AT 620 PSI
REASON FOR CHANGE:		
TO PREVENT REAR WHEELS FROM SKIDDING WHEN AN OPEN LOOP BRAKE STOP IN WET CONDITIONS OCCURS		



From Vehicle PDR June 1982

FIGURE 6.2-5 (continued)

III. HARDWARE

A. Overview

1. Hardware Block Diagram
2. Traceable vs. Non-Traceable Hardware

B. Internal Interfaces

1. Interface Groundrules
2. High Frequency Clock Distribution

C. Circuit Cards

1. Communication Processor
2. Modulator
3. Loop Driver
4. Receiver
5. Speed Limit Checker/Collision Avoidance Subsystem Processor
6. Presence Detection Electronics
7. Safe-To-Proceed Control
8. Master Clock

D. Guideway Elements

1. Loops/Antennas
2. Presence Detectors

E. Power

1. Current Requirements
2. Power Supplies
3. Grounding

F. Packaging

1. Requirements
2. Design Solution
 - a. Racks
 - b. Cages
 - c. Cables and Connectors
 - d. Cooling

IV. GCCS SOFTWARE

A. EDS Software Development Plan

B. Preliminary Design

1. Communication Processor
2. Speed Limit Checker Processor
3. Collision Avoidance Processor
4. Presence Detection Processor
5. Digital Receiver

V. GCCS TESTING

A. Operational Configuration

B. General Test Plan

C. Test Configurations

1. Inductive Communication Subsystem
2. Presence Detection Subsystem
3. Magnetic Signaling Subsystem
4. Collision Avoidance Subsystem

D. Test Documentation

IV. GCCS SCHEDULE

A. Activity to CDR

From GCU PDR

discontinued the baseband reflectometer Collision Avoidance System (CASBAR) and replaced it with the ODDCAS design.

The ODDCAS PDR presentation included material which was quite detailed due to the commonality of certain of the ODDCAS components to these of the VCU and GCU and as a result of the prior ODDCAS laboratory demonstration.

The ODDCAS Specification S362-90013-1 was approved and detailed design was authorized as evidenced by Boeing and UMTA signatures on the meeting minutes.

By this time, the System Specification, SS362-90000-3, had been revised to SS362-90000-3B. All changes were coordinated, approved, implemented, and accounted for in accordance with the program configuration plan. Engineering Change Proposal (ECP) #4, for example, programmed the replacement of CASBAR with ODDCAS.

Figure 6.2-7 shows details of the PDR data package and PDR presentation.

6.3 CRITICAL DESIGN REVIEWS

As noted previously, Critical Design Reviews (CDRs) mark approval of engineering detail design to subsystem specifications; these specifications were previously approved following the PDR.

Approval of CDR, including closure of all action items, normally constitutes authorization to start fabrication. However, because of the termination of the test track/vehicle activity, GCU and ODDCAS activities ended at CDR. The test track software effort was terminated at completion of coding. Software integration testing was cancelled.

Design effort on the "MPM" modified vehicles was terminated prior to the scheduled vehicle CDR. All vehicle design activities, including design trades, development test, etc, were compiled and documented for the record.

TEST TRACK SOFTWARE CDR - August 11, 1982

The test track software CDR provided the technical basis for the commencement of the coding and verification of the test control software to be demonstrated at EDS.

Figure 6.3-1, from the presentation, noted the current test track software status in the development cycle. Detailed design tasks that were completed since the PDR were summarized as noted.

Figure 6.3-2 is an example of how a specific system specification, "switch control", is allocated to the software development specification. The chart further identifies the incorporation of this specification in the software design module identified by the macro, "SSC"; these design modules are contained in the software development specification. Following coding, verification is established by test.

FIGURE 6.3-2
TEST TRACK S/W CDR - EXAMPLE OF ALLOCATION PROCESS

EDS SYSTEM SPECIFICATION SS362-90000-3A

The BOSINS COMPANY

3.1.2.5.6 Lateral Motion Control

3.1.2.5.6.1 Switching

The C&CS shall control the routing of vehicles on the guideway by issuing switch commands to the vehicle. After a switch command has been issued, the onboard C&CS shall determine, in a failsafe manner, if switch verification discretely indicate the commanded direction. This onboard switch verification shall be accomplished within 1.28 seconds after receipt of a switch initiate discrete. If switching is not verified as required, the C&CS shall command an emergency stop. Total time utilized by C&CS during the 1.28 seconds shall be equal to or less than 0.25 seconds. (The remaining 1.03 seconds is allocated to the vehicle.)

3.1.2.5.6.2 Ride Comfort

**** shall not cause the longitudinal steady state or sinusoidal ride

SOFTWARE SPECIFICATION SS362-90500-2A

mandated to stop and has not been commanded to advance.) If an emergency departure occurs, the vehicle shall be commanded to stop on normal brakes.

3.2.2.3.2.2 Switch Control

Each time a vehicle arrives at the last PD before a switch magnet, switch control shall issue a switch command to the vehicle. Two types of switches shall be supported: Fixed direction and destination dependent.

For a fixed direction switch, the commanded switch direction shall be independent of the vehicle destination.

The commanded direction for the test loop exit switch shall be determined by the vehicle destination. If the vehicle's completed loop count equals or exceeds the assigned destination (assigned lap count), the vehicle shall be commanded to switch left (exit test loop) unless the two-way guideway segment is occupied by or committed to a vehicle departing the station (being dispatched to the test loop). Otherwise, the completed lap count shall be incremented and the vehicle shall be commanded to switch right (remain on test loop).

If the next PD activated by the vehicle indicates that the vehicle failed to switch in the commanded direction, Report Generation shall be notified.

Report Generation shall also be notified if the vehicle is commanded to bypass its destination because the two-way guideway is occupied or committed.

INTRODUCTION - THE SOFTWARE DESIGN MEETS SYSTEM REQUIREMENTS

SYSTEM SPEC SS362-90000-3A		SOFTWARE SYSTEM DEV. SPEC S362-90500-2A		SOFTWARE PRODUCT DEV. SPEC D362-90520-1		VERIFICATION METHOD
PARA NO.	TITLE	PARA NO.	TITLE	APPENDIX	MODULE	
3.1.2.5.5	Departure Control	3.2.2.3.1.1.1	Dispatch Control	C	VHM	Test
3.1.2.5.6.1	Switching	3.2.2.3.2.2	Switch Control	C	SSC VEM	

FIGURE 6.3-3
VCU - CDR - DATA PACKAGE

Attachment A to this letter, in accord with the reference, provides a detailed VCU CDR agenda for June 14, 1983 through June 17, 1983.

Attachment B is a detail listing of the data package being forwarded under separate cover this date. Four sets of the data are being forwarded to your office and one directly to Battelle.

The data package is organized as noted on Attachment B. One copy of the "VCU Software Product Specification, dated May 9, 1983, PDL 03.06" and the "VCU communication processor software product specifications" is included in the data package for review by software specialists.

Hybrid simulation documentation, as noted in Section V of Attachment B, is not included in the data package. Detail copies can be made available on request.

VCU CDR AGENDA		
JUNE 14, 1983		
<u>TIME</u>	<u>SUBJECT</u>	<u>SPEAKER</u>
8:00 A.M.	I. INTRODUCTION A. Definition of CDR B. Definition of VCU C. Requirements Derivation D. VCU Organization E. Design Modifications since PDR	D. Freitag
9:30 A.M.	II. HARDWARE DESIGN A. Organizational Overview	D. Haberman
10:30 A.M.	B. Timing Card	
11:30 A.M.	(LUNCH)	
12:30 P.M.	J. RS-232 Card	D. Haberman
1:00 P.M.	K. Magnetic Signalling	C. Colson
1:30 P.M.	III. SOFTWARE DESIGN A. Module Level Design Procedures	W. Greve
2:30 P.M.	B. Organization: Main Processor	
4:00 P.M.	(CONCLUSION - SECOND DAY)	
JUNE 16, 1983		
2:45 P.M.	H. Configuration Control	S. Larsen
IV. SUPPORTING ANALYSES		
3:15 P.M.	A. Introduction	I. Alberts
3:30 P.M.	B. System Safety	R. Washington
4:30 P.M.	(CONCLUSION - THIRD DAY)	
JUNE 17, 1983		
A. Goals		
B. Accomplished to Date		
C. Planned		
10:00 A.M.	VI. PLANNED ACTIVITIES TO DELIVERY A. Current Status	D. Freitag

(continued)

GUIDEWAY CONTROL UNIT CDR - February 14-16, 1984

The GCU CDR was held at the Urban Mass Transportation Administration (UMTA) offices in Washington D.C. The speakers, including our GCU hardware and software designers and system engineering (safety) personnel, covered topics including detailed hardware and software design, testing philosophies, test track guideway layout, and GCU safety. Figure 6.3-4 features portions of the GCU CDR data package.

FIGURE 6.3-4 (continued)

12:30 P.M.	VI. <u>PLANNED ACTIVITIES TO DELIVERY</u>	
	A. Current Status	D. Freitag
	B. Future Activities	
1:30 P.M.	VII <u>ACTION ITEM REVIEW</u> (As Required)	D. Freitag
2:00 P.M.	VIII <u>LABORATORY TOUR</u> (GCU Single-Thread Demonstration)	E. Nishinaga/ J. Forrester

GCU CDR DATA PACKAGE

I. GCU GENERAL SPECIFICATION

S362-90011-1A (Revision A), "Performance Design and Quality Assurance Requirements for the AGRT-EDS General Specification for Guideway Command & Control Subsystem," (forwarded to UMTA 3-15-83, DTF AGRT-EDS 100).

II. DESIGN DRAWINGS

WIRE WRAP ASSY. ANTENNA DRIVER, VCU"

III. GCU SOFTWARE DESIGN

- 1) SK362-82311 - "Firmware FSK Receiver - GCCS and VCCS - AGRT"
- 2) SK362-82330 - "Firmware SLC Processor - GCU"
- 3) SK362-82310 - "Firmware Comm/PD Processor GCCS - AGRT"

IV. MEMOS DOCUMENTING THE GCU DESIGN RELEASED SINCE PDR

- 1) Memo 2-5041-C&CS-218A, dated 5-17-83, "Proposed Change to the Speed Limit Checker Implementation"
- 2) Memo 2-5041-C&CS-215, dated 5-27-83, "Vehicle/Guideway Magnetic Interface"
- 3) Memo 2-5041-C&CS-259, dated 12-6-83, "Safe-to-Proceed Control Card Design"

V. INTERFACE CONTROL DOCUMENTATION

ICD 362-90054 REV B, "Interface Control Drawing Control Elements and Rail Locations - EDS/STTF"

FIGURE 6.3-5
ODDCAS CDR AGENDA

<u>JUNE 5</u>	<u>SUBJECT</u>	<u>SPEAKER</u>
<u>LOCATION 11K1</u>		
	<u>I. INTRODUCTION</u>	D. B. Freitag
8:30 - 9:00 a.m.	A. Definition of CDR	
	B. Definition of ODDCAS	
	C. Requirements Derivation	
	<u>II. ODDCAS CONCEPTS AND ORGANIZATION</u>	
9:00 - 10:15 a.m.	A. Concepts (System Definition, Guideway Definition, Communication Links)	R. J. Schroder
	<u>BREAK</u>	
12:30 - 1:00 p.m.	<u>III. ODDCAS SAFETY AND PERFORMANCE</u>	R. E. Alberts
	A. Safety	
	B. Headway	
	<u>IV. VEHICLE HARDWARE AND SOFTWARE (Part 1)</u>	
1:00 - 5:30 p.m.	A. Vehicle Processor (VCAS) Software	D. Fielding
	<u>JUNE 6</u>	
<u>LOCATION 11K1</u>	<u>SUBJECT</u>	<u>SPEAKER</u>
	<u>V. VEHICLE/WAYSIDE INTERFACES</u>	C. W. Colson
8:30 - 9:00 a.m.	A. Inductive Communication	
	B. Magnetic Signaling	
	<u>VI. VEHICLE HARDWARE AND SOFTWARE (Part 2)</u>	
9:00 - 9:30 a.m.	A. Vehicle Processor (VCAS) Hardware	C. W. Colson
	<u>VII. WAYSIDE HARDWARE AND SOFTWARE</u>	
12:30 - 1:30 p.m.	A. FSK Receiver	W. B. Chapman
1:30 - 2:00 p.m.	B. Pre-processor (PCAS) Hardware	C. W. Colson
2:00 - 2:15	<u>BREAK</u>	
2:15 - 2:45 p.m.	C. Main Processor (MCAS) Hardware	B. G. McCrear
2:45 - 3:30 p.m.	D. Wayside Software (Overview of Software for Main and Pre-processors)	R. J. Schroder
3:30 - 6:00 p.m. (15-minute break included).	E. Pre-processor (PCAS) Software	R. J. Schroder
6:00 p.m.	END OF 2nd DAY	

(continued)

7.0 BRASSBOARD FABRICATION, DEVELOPMENTAL TESTING AND VCU VERIFICATION TESTING

As the AGRT Program continually evolved, only the Guideway Communications Unit (GCU), Odometer Data Downlink Collision Avoidance System (ODDCAS), and Vehicle Control Unit (VCU) portions of the Command and Control System actually reached the brassboard stage. Only the VCU was formally tested, although the VCU Test Set used components from the GCU and ODDCAS development.

This section summarizes brassboard fabrication, development testing, and VCU design verification efforts.

GCU BRASSBOARD FABRICATION & DEVELOPMENTAL TESTING

Guideway Communication Unit (GCU) development was stopped following the GCU CDR; however, extensive development and testing was accomplished in preparation for the CDR. Developmental, brassboard, wire wrap assemblies of each GCU board (noted below) were built and bench tested. In addition to bench tests, specific developmental tests were conducted, concluding with the GCU single thread integration testing. Extensive safety and thermal analyses were also made and documented.

Brassboard fabrication in the development lab was to design drawings that were verified at CDR to be in compliance with the GCU specification. Developmental history of fabrication was recorded on "Design Development Configuration Records" (DDCR). Reference 41 provides a detailed design description.

Listed below are the three GCU subsystems.

INDUCTIVE COMMUNICATION SUBSYSTEM

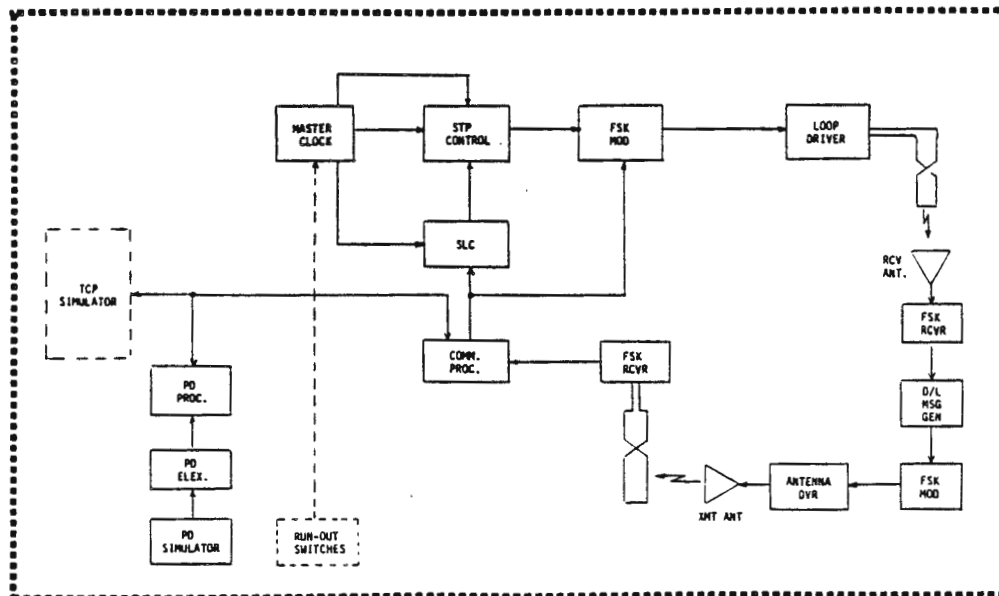
Communication Processor
Speed Limit Checker Processor

FIGURE 7.0-1
ODDCAS TESTING CATEGORIES

TESTING CATEGORIES

- 0 DEVELOPMENT TESTS -- TESTING TO ESTABLISH PHYSICAL REQUIREMENTS
TESTING TO EVALUATE DESIGN DECISIONS
- 0 BRASSBOARD BENCH TESTS -- TESTING TO VERIFY COMPLIANCE OF DESIGN AT THE
BOARD LEVEL
- 0 HARDWARE/SOFTWARE INTEGRATION TESTS -- TESTING OPERATIONAL HARDWARE AND
SOFTWARE TOGETHER
- 0 TYPE APPROVAL TESTS -- ONE TIME ONLY TESTS OF THE PROTOTYPE TO VERIFY THE
DESIGN
- 0 ENVIRONMENTAL TESTS -- TESTING UNDER EXTREME ENVIRONMENTAL CONDITIONS
(NOT PART OF THIS PROGRAM -- PRODUCTION TYPE
PACKAGING NOT EMPLOYED)
- 0 ACCEPTANCE TESTS -- LIMITED TESTING OF EACH UNIT TO VERIFY PROPER
FABRICATION
- 0 GCU/TCCS INTEGRATION TESTS -- PRIMARILY TESTING OF GCU TO TCCS INTERFACES
- 0 OPERATIONAL TESTS -- TESTING OF ALL SYSTEM ELEMENTS TOGETHER AT THE TEST
TRACK

FIGURE 7.0-2
ODDCAS GCU SINGLE-THREAD TEST



ODDCAS DEMONSTRATION

Three communication prototype units were constructed, consisting of two vehicle units and one wayside unit. The two vehicle units were set up to communicate with the wayside unit through an inductive link which consisted of transmit and receive coil antennas and wire loops taped to the floor. Each unit was built with transmit and receive capabilities. The scope of the demonstration was limited to demonstrating that the two vehicle units could transfer time multiplexed data reliably to the wayside unit even in the most severe electromagnetic environment.

Following the demonstration test it was concluded that the use of time multiplexed hexadecimal FSK for downlinking odometer data can result in the development of a relatively simple collision avoidance system.

Fabrication and development testing of the Vehicle Collision Avoidance System (VCAS) and the Wayside Collision Avoidance System (WCAS) was initiated following the PDR. Design drawings of the tested units were approved following the CDR. Reference 42 provides a detailed design description.

VEHICLE COLLISION AVOIDANCE SYSTEM

Figure 7.0-3 is a block diagram of the VCAS equipment on the vehicle. The VCAS performs the following functions:

1. Receive processed odometer data (vehicle speed and incremental traveled distance) from the Vehicle Control Unit (VCU) and send position and speed messages to the wayside based on this data. (Onboard monitoring of the transmitted messages is performed to detect transmission errors.)
2. Detect guideway magnet pairs, measure the distance between the pair, and perform the coded function.

3. Receive uplink signals and use the information in the time multiplexing downlinks with other vehicles in the loop. New time slot assignments are accepted only when a new loop magnet pair is detected by the onboard equipment.

Most of the hardware used on board the vehicle is identical to that used on the wayside. The only vehicle-unique elements are the vehicle antennas and the Vehicle CAS Processors.

WAYSIDE COLLISION AVOIDANCE SYSTEM

Figure 7.0-4, ODDCAS wayside equipment, shows the WCAS pre-processor in relation to the WCAS main processor and inductive communication components. The main processor services up to 16 pre-processors.

ODDCAS WAYSIDE INTEGRATION TEST

An ODDCAS wayside integration test was conducted as configured in Figure 7.0-5. Implementation of test software in the WCAS pre-processor concluded that the wayside hardware was functional with respect to wayside loop communication.

Portions of the developmental ODDCAS, as well as GCU developmental units, were subsequently incorporated into the upgraded VCU Test Set to support integration and system simulation testing.

VCU BRASSBOARD FABRICATION - SOFTWARE IMPLEMENTATION - DEVELOPMENTAL AND VCU VERIFICATION TESTING

The Vehicle Control Unit, together with the electrical propulsion system, the friction brake system, and the vehicle itself, constitute the Vehicle Longitudinal Control System (VLCS).

An overview of the VCU brassboard fabrication and the extensively developed and implemented supporting software is noted here. An overview of the upgraded VCU Test Set is provided. A concluding summary of hybrid simulation, VCU integration, and VCU verification testing in the developmental laboratory follows.

FIGURE 7.0-5

ODDCAS WAYSIDE TEST CONFIGURATION

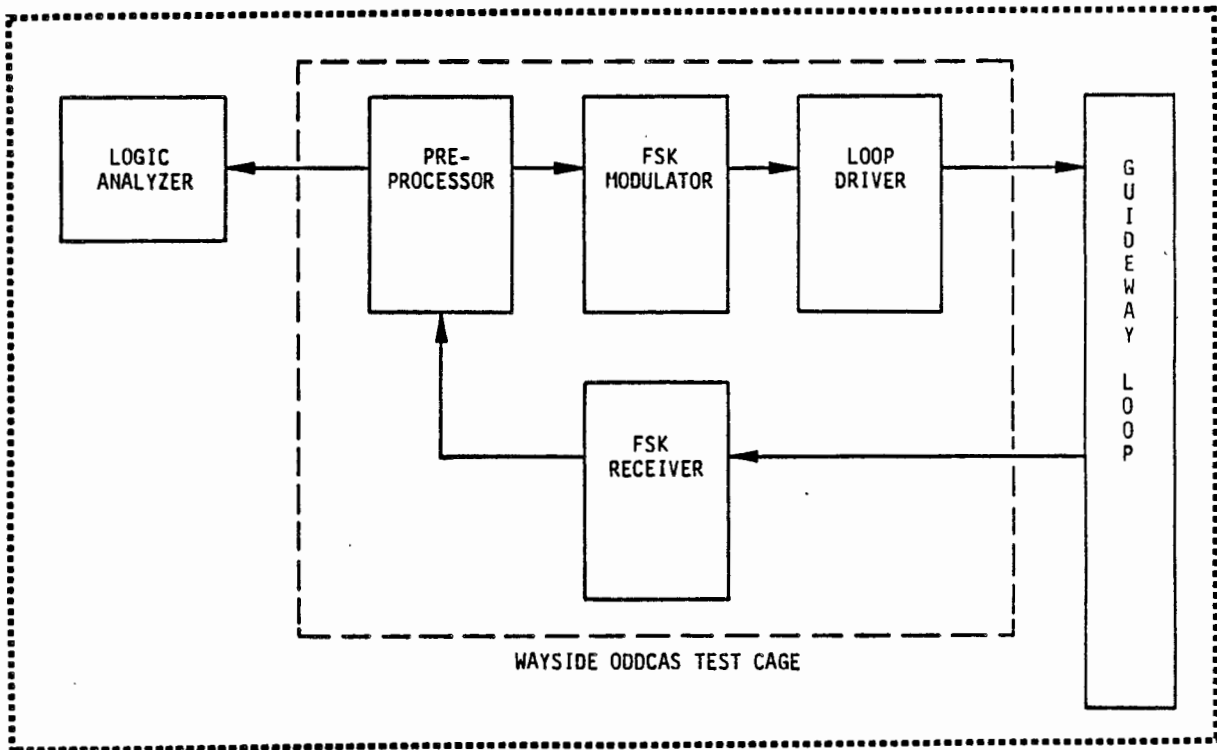
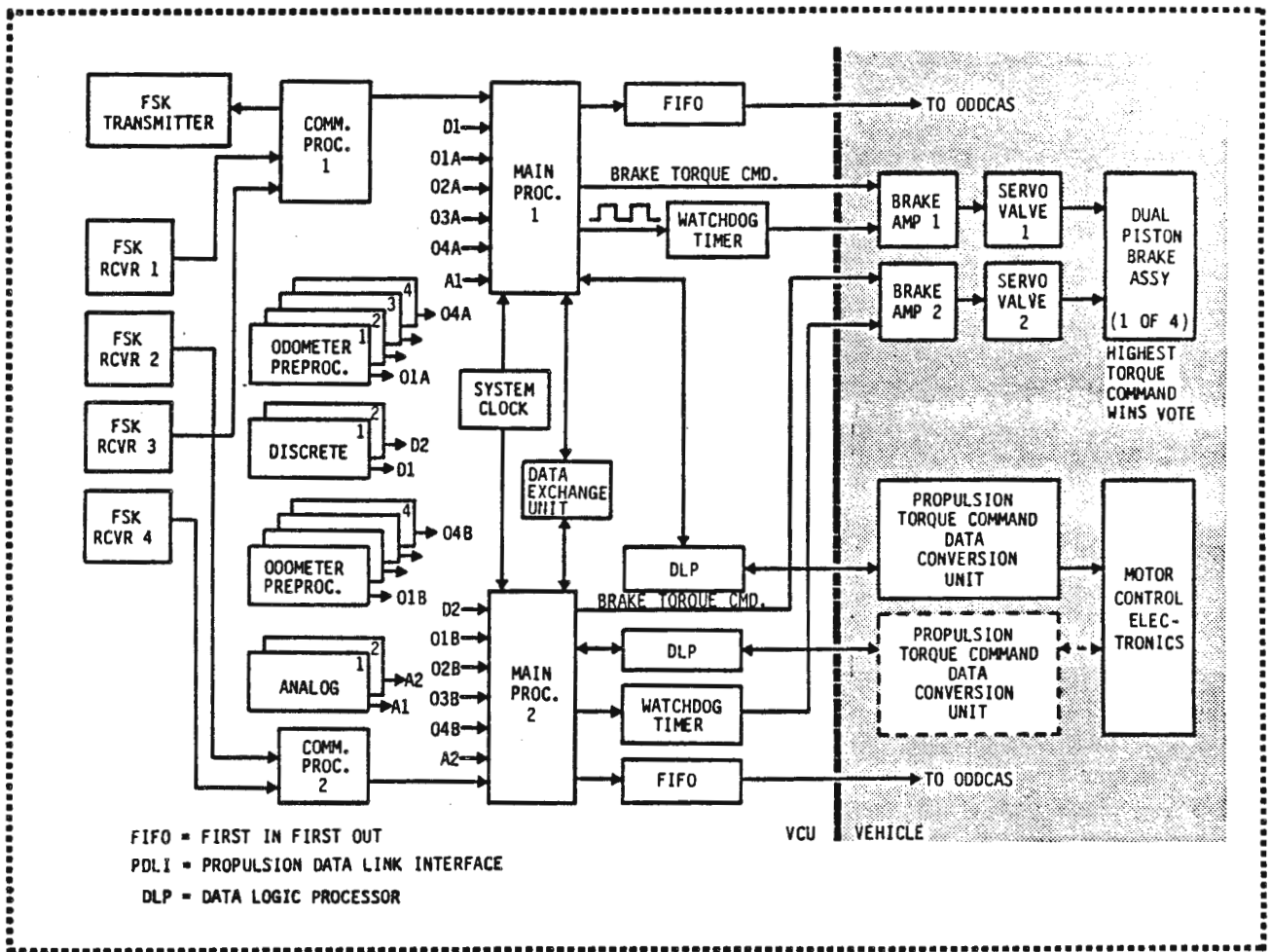


FIGURE 7.0-6

VCU CHECKED DUAL REDUNDANT



In other words, each processor has a separate input/output port to a single memory bank, and each processor can read and write, in turn, to every location in this shared memory.

All signals between the Main Processor and the remainder of the vehicle are processed as parallel data transfers on the address/data bus. The processing necessary to convert analog and serial pulse train signals to parallel form and vice versa is performed by circuits peripheral to the Main Processor. In particular, the propulsion signals and the odometer data from each wheel are manipulated by separate 8-bit microprocessor units.

Figure 7.0-8 is the top VCU brassboard assembly drawing. This drawing represents the final configuration of the Vehicle Control Unit, incorporating all controlled changes through VCU integration and VCU verification testing. The VCU Communication Processor wire wrap assembly cards, part numbered 362-40101-2, are shown in both channel A and B. Similarly, the Main Processor wire wrap assemblies are part numbered 362-40100-4. Other wire wrap assemblies include the timing card (channel 1 only), the RS 232 card, FSK receiver (2 cards each channel), the digital input/output card, and the analog input/output card.

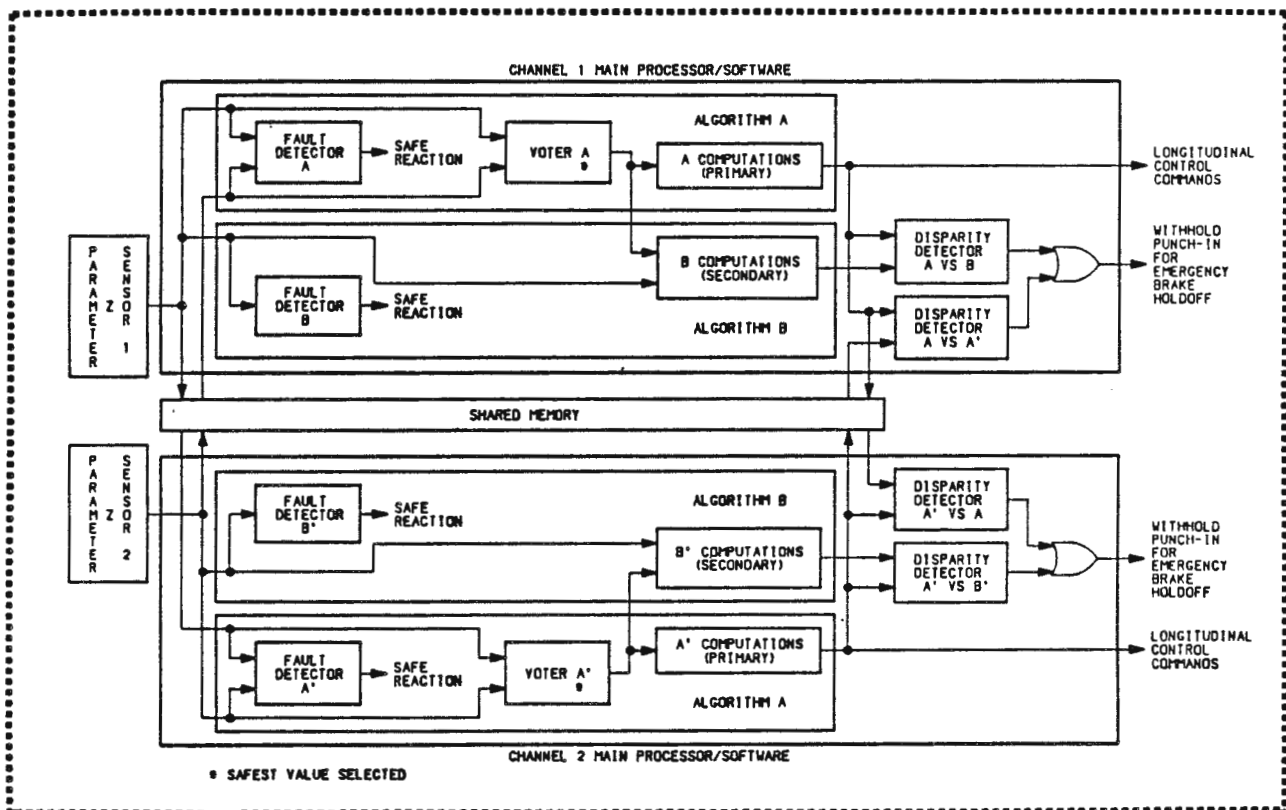
Prior to the start of formal testing, all elements of this assembly, including the final rack assembly, were verified to the design drawings by a team consisting of the Engineering (hardware and software) Designer, the Engineering Design Manager, and Configuration Management. All subsequent revisions required during testing were implemented with controlled changes. The initial configuration of the Main Processor at start of test was 362-40000-1; the final configuration noted on the drawing was 362-40000-5.

VCU SOFTWARE IMPLEMENTATION

The VCU software design employs dissimilar algorithms to detect hardware failures and embedded software errors. Figure 7.0-9 (from

FIGURE 7.0-9

SYMMETRICAL DUAL-DISSIMILAR SOFTWARE
WITH REDUNDANT SOFTWARE



MAIN PROCESSOR SOFTWARE

The Main Processor is composed of three distinct elements:

- 1) the initialization process,
- 2) vehicle control duty, and
- 3) background self checking.

PHYSICAL ORGANIZATION OF THE SOFTWARE

The design of the code was represented in a Program Design Language in a document called the Software Product Specification*. This design document presents the modules in the logical order, i.e., in the order in which they are called. The logical organization of the software was based on a division by function and a stepwise refinement of those functions into individual tasks. There are 167 separately compiled modules. Most of these modules are limited to a single task with subtasks called as needed. Any modification to a task was, therefore, limited in its effect on the overall assemblage of software pieces. The linking of these pieces and the generation of checksum totals used in the self-tests were automated.

The physical placement of modules within the vehicle control code memory is of no importance. For simplicity's sake they were inserted in alphabetical order. The variables were also allocated space within the random access memory in alphabetical order.

QUALITY ASSURANCE

VCU software module unit testing summary and methodology was internally documented. It should be noted that system engineering-safety oversaw all software module designs. The PDL specifically identified safety critical modules.

- * S362-80501-1A is the Program Design Language (PDL) for version 20 of the embedded VCU Main Processor software. S362-80501-2A is the PDL for version 3 of the embedded VCU Communication Processor software. Versions noted are final versions following incorporation of all changes at end of VCU verification testing.

only be adequately tested when the VCU is operating in a real-time closed-loop environment similar to what it will see in actual operation. The VCU test was developed to allow real-time closed-loop testing of the VCU in the laboratory.

Basic elements were initially tested on a single string version of the VCU. Redundancy and communication elements were then added to support formal testing. This phased approach allowed early identification of problems and avoided the situation of having to trouble-shoot a large number of problems at one time.

Program plans specified system simulation testing in the SDIL lab prior to test track testing. This simulation test capability was upgraded to fully support VCU verification testing.

VCU TEST FACILITY DESCRIPTION

A block diagram of the VCU Test Set-up is shown in Figure 7.0-10. The major elements shown are the Test Scenario Generator (TSG), the Test Vehicle Simulator (TVS), and the article to be tested, the VCU. Figure 7.0-11 is a picture showing the VCU and the TSG, and Figure 7.0-12 is a picture showing the TVS. Physically, the equipment shown in each picture is located in adjoining rooms, electrically connected by an overhead ribbon cable.

The function of the TSG is to simulate the wayside, i.e., to provide the command sequences that a vehicle would receive from the wayside in actual operation. This function is provided by means of hardware and software specifically developed for this purpose. A Zilog Z8002 based microcomputer system was designed to utilize previously developed hardware and software experience. The design objectives of the TSG were to provide the test operator the capability to quickly generate virtually any sequence of commands that might be required to create a desired open or closed-loop test condition.

FIGURE 7.0-11
TEST ARTICLE & TSG

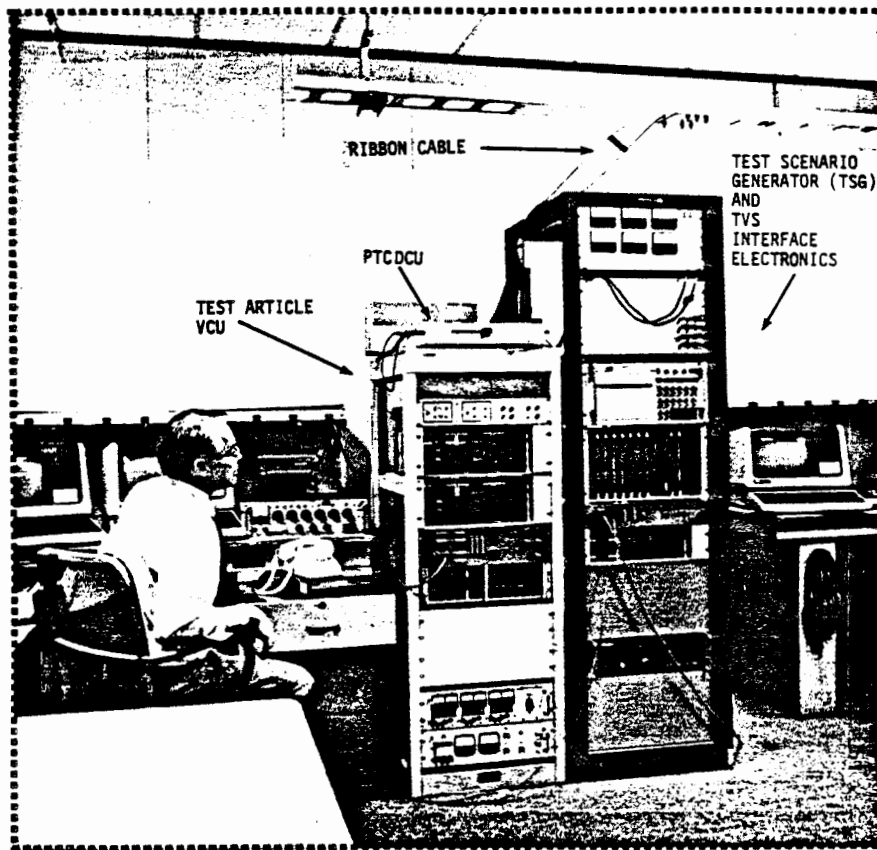


FIGURE 7.0-12
TEST VEHICLE SIMULATOR

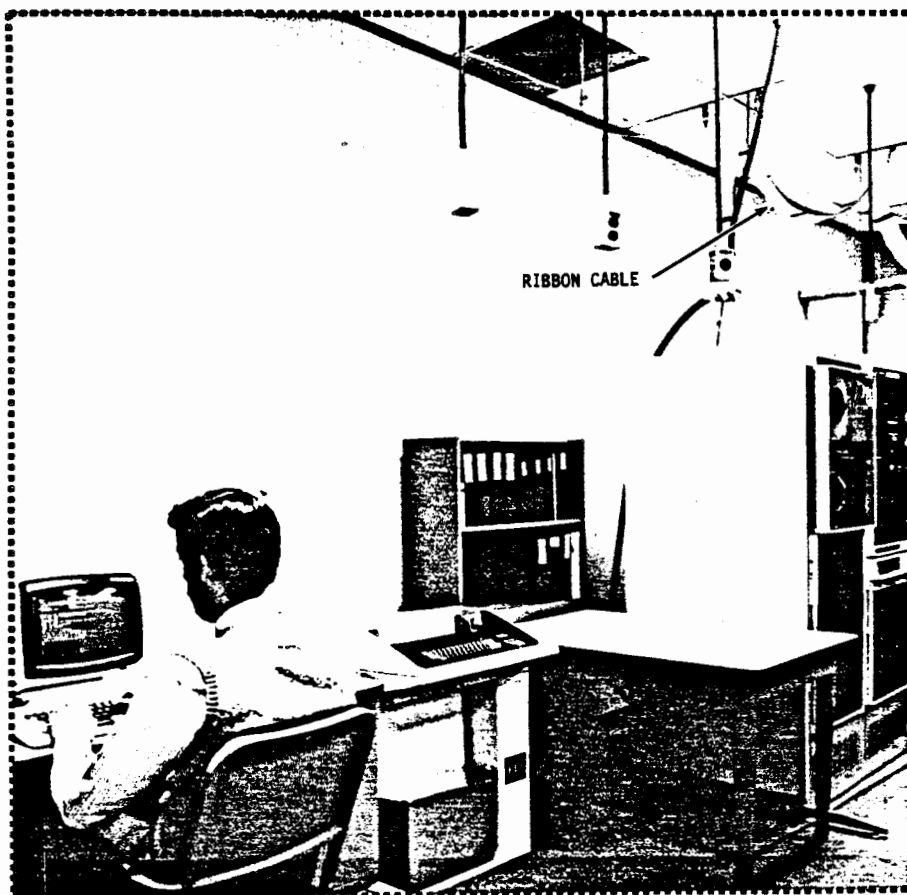
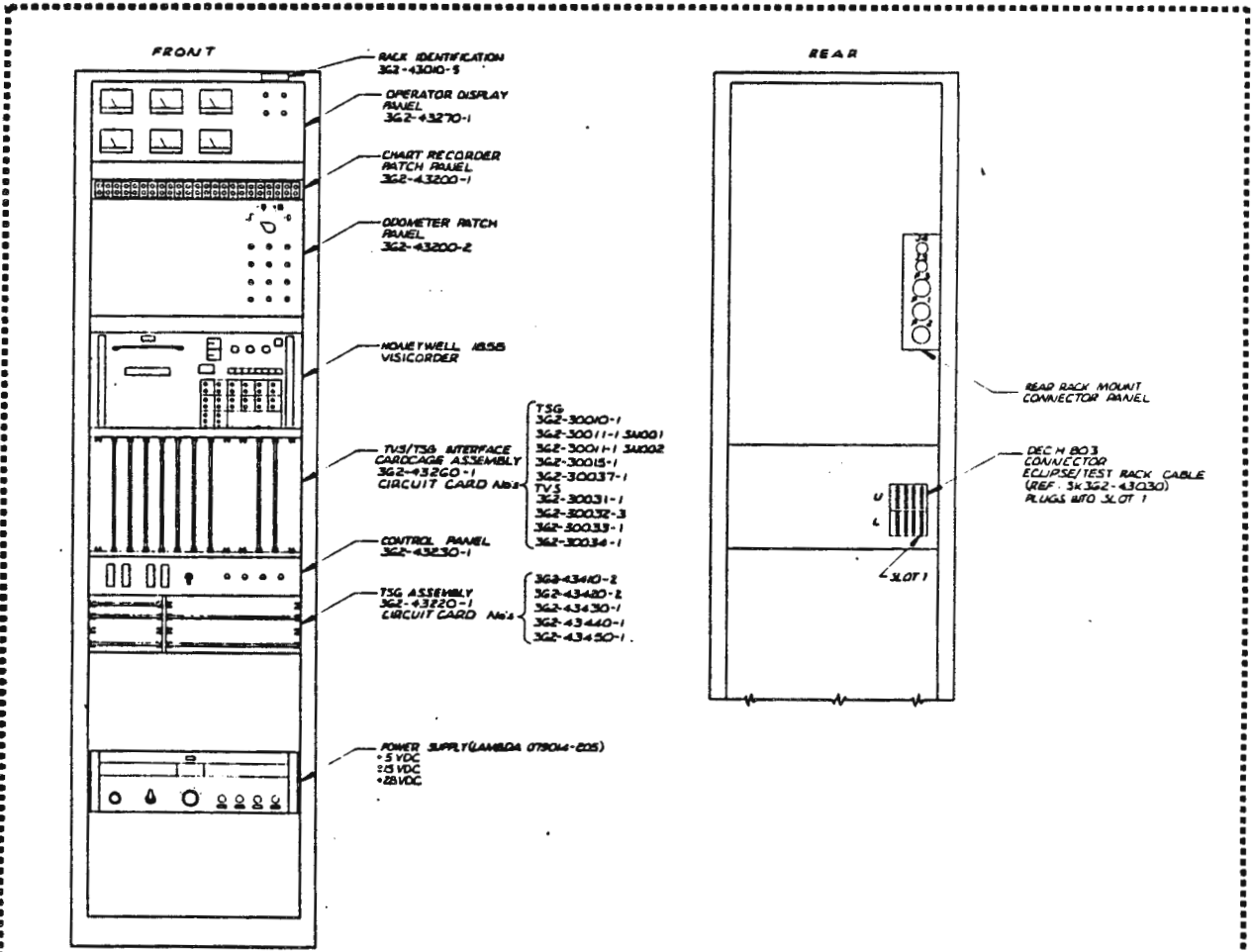


FIGURE 7.0-13

VCU TEST ASSEMBLY - TOP DRAWING



BOEING COMPANY & TELEPHONE PER ANNUAL 1968 1873 LINE 150 OTHERS SPECIFIED DIMENSIONS ARE IN INCHES UNLESS OTHERWISE SPECIFIED DECIMALS ARE: .0001 INCHES .001 INCHES .01 INCHES .05 INCHES .1 INCHES .2 INCHES .5 INCHES 1 INCHES DIMENSIONS AND SURFACE FINISHES OF UNLESS OTHERWISE SPECIFIED PLATING OR FINISH (SEE DRAWING)	REVISIONS & APPROVALS DATE: 11/16/68 BY: C. G. GEHRI	CONTRACT NUMBER DOT-UT-80041 DRAWN BY: C. G. GEHRI CHECKED BY: J. H. BATES DATE: 11/16/68	BOEING CORPORATION SEATTLE, WASHINGTON 98148
	TITLE: VCU TEST RACK ASSEMBLY DRAWING NO: SK362-43010 SHEET NO: 1 OF 1	PART NUMBER: D81205 REV: 1	DATE: 11/16/68 BY: C. G. GEHRI

DUAL-STRING SIMULATION INTEGRATION TESTING

Following VCU single string simulation testing, the VCU Test Set was extensively upgraded to support dual string integration testing. It was during this time frame that the test track testing was terminated. The VCU Test Set design review was held and action to implement the formal simulation test facility was set in motion. Dual string integration tests were documented similar to that noted for single string tests. Integration tests were as follows:

- o VLCS Stability Margin Verification
- o VLCS Basic Response Characteristics
- o VLCS Position Update Basic Response Characteristics
- o VLCS Basic Closed-Loop Emergency Stopping Characteristics
- o VCCS Odometer Performance Verification

VCU VERIFICATION TESTS

The philosophy in the VCU Verification Test Plan was to concentrate on high risk areas; items which are critical to the overall design and items that are largely application independent. In many areas, a spot check approach was selected in place of the exhaustive testing originally planned. The overall objective was to learn as much as possible on the operation of the VCU and, at the same time, avoid the costs normally associated with a formal acceptance test program.

Table 4 provides an overview of the revised test program. Each function entry represents a test or test series. Included in the table are the applicable System and VCU Specification paragraphs for the function under test. In most cases, a formal test was performed to verify compliance with requirements; however, given the groundrule that the VCU was not to be altered in response to specific test requirements, there are some functions where explicit tests are not possible at the subsystem level. In these cases, analysis results or the results of software module level testing are used to demonstrate compliance with requirements.

TABLE 4 EXECUTIVE SUMMARY OVERVIEW (cont.)

FUNCTION	OBJECTIVES	Test Type	SPEC PARA (System / VCU)	SUCCESS CRITERIA
3.0	LONGITUDINAL CONTROL - Special Purpose		S-2.3.2	
3.1	Position Update Response	S	V-3.2.1.2.1 3.2.2.1.1 3.5.2.7.1.1.1	Properly initiate and terminate position corrections and speed changes.
3.2	Station Stop & Berth Moveup	S	V-3.2.1.2.1	Station stop (SS) initiated upon detection of SS discrete, completed within 6" of designated position, within jerk and acceleration limits.
	Verify forced brakes applied after stopping.	S	V-3.5.2.7.1.1.5 3.5.2.7.1.1.6	When closed loop stop is complete, forced brakes are commanded and continue until dispatch.
	Verify berth moveup (single and multiple).	S	V-3.5.2.7.1.1.2	Moveup speed profile correct.
4.0	LONGITUDINAL CONTROL - Emergency Stop		S-2.3.2	
4.1	Closed Loop Emergency Stop	S	V-3.2.2.2 6.4 V-3.2.2.1 3.3.3.1.4 3.5.2.7.1.1.4	Response within 20 ms of condition requiring emergency stop. Stopping distance, jerk, and acceleration within limits.
	Verify forced brakes applied after stopping.	S	S-2.3.3 3.1.2.5.7.3 V-3.5.2.7.1.1.5 3.5.2.7.1.1.6	Reset accepted following completed resettable stop. When closed loop stop is complete, forced brakes are commanded. Command continues until dispatch.
4.2	Open Loop Emergency Stop	S	V-3.2.2.2 S-2.3.3 3.1.2.5.7.3.3 V-3.5.2.11.4 6.4	Interrupt "EB Holdoff" within 50 ms following violation of specified closed loop emergency stop error limits or other anomalies requiring open loop EB.
5.0	INTERFACES			
5.1	VCU-VCAS Interface	S	V-3.2.3.1 3.4.2.9 3.5.2.11.1	Properly formatted Odometer data and status transmitted via FIFO every 40 ms. Handshaking signals provided as specified.
	Verify response to CAS data transmission failure.	S	V-3.5.2.11.1	Closed loop emergency stop initiated in response to FIFO failure (improper signals). (— FIFO failure reported)
5.2	FSK Message Processing	S	V-3.2.1.1.1 3.2.1.1.2 3.4.1.1 3.4.2.1 3.5.2.2 3.5.2.5	Uplink and downlink messages processed.

TABLE 4 EXECUTIVE SUMMARY OVERVIEW (cont.)

FUNCTION	OBJECTIVES	Test Type	SPEC PARA (System / VCU)	SUCCESS CRITERIA
6.5 Power Monitoring	Verify power anomalies reported.	S	V-3.5.10.1	When 28 VDC power is < 21.5 V or > 28.8 V, warning message is sent. When voltage drops below 25.2 V charger loss is reported.
	Verify safe response to VCU power failure.	A	S-2.4.1	Power failures which adversely affect safety critical functions interrupt the emergency brake hold-off.
6.6 Status Monitoring	Verify response to brake caliper pressure anomalies.	S	V-3.5.1.4.2 3.5.2.10.1	Out of tolerance brake pressure is reported. Closed loop emergency braking commanded when both measurements (A & B) are low.
	Verify response to conflict between propulsion and brakes.	S	V-3.4.2.10.1	Conflict reported and closed loop emergency braking commanded when brake pressure (A or B) exceeds 200 psig while torque command exceeds 150 ft-lb for 80 ms or more.
	Verify response to hydraulic system anomalies.	S	V-3.4.1.4.1 3.5.2.10.2	Indication of temperature failure reported. Indication of accumulator failure reported. Normal rate braking commanded for single accumulator failure indication. Closed loop emergency rate braking commanded for dual failure indication.
	Verify response to overheated brake pads.	S	V-3.5.2.10.2	Indication of brake pad over temperature reported and normal rate stop commanded.
	Verify response to propulsion anomalies.	S	V-3.4.1.3.2 3.5.2.10.2	Propulsion anomalies reported. Normal rate stop commanded except for over temperature or loss of battery charger. Stop irrevocable when propulsion shut down indicated or measured propulsion exceeds command by more than tolerance.
	Verify Response to communication processor failure.	S	SV-3.5.2.10.2	Irrevocable normal rate stop commanded when communication failure is indicated.

SUMMARY AND CONCLUSIONS OF DESIGN VERIFICATION TESTS

A total of thirty-seven VCU problems were identified during formal testing. Most of these were minor in nature and most were corrected during the test effort. The significant problems tended to be in areas involving interfaces or interactions between elements, i.e., problems that did not show up in lower level testing. In a few cases, problem correction was deferred to be resolved as a part of future application efforts. In all cases, careful problem tracking and correction records have been maintained to support potential future uses of the current design.

Numerous problems were identified and resolved during the single string developmental and dual string integration testing that preceded formal testing. As a result of this effort, a relatively low number of problems were encountered during formal design verification tests. Extensive software module testing was also helpful in this regard, although in hindsight, it might have been appropriate to place less emphasis on module level tests and more emphasis on subsystem tests.

From the simulation testing, the following observations were noted:

- 1) At no time did the VCU take an unsafe reaction to an anomaly. Although this is not conclusive proof, it does add considerable confidence to the safety approach taken.
- 2) Closed-loop testing with prototype VCU hardware and software is a necessity. Many of the problems identified could not have been realistically identified in any other manner.
- 3) The extensive data collection and processing capability built into both the VCU and the Test Set proved invaluable, both in troubleshooting and in the quality of testing that could be performed. In many cases, the ability to obtain a precise record of the sequence of VCU calculations allowed quick identification of problems that would have taken months to resolve using more conventional methods. This capability also allowed a very precise verification of requirements in areas where such a check is important.

8.1 SIGNIFICANCE TO EXISTING TRANSIT SYSTEMS

This section examines the significance of our achievements to existing properties, including manually operated and semi-automated systems.

SAFETY DESIGN AND EVALUATION STANDARDS

The AGRT Command and Control System meets the Program safety requirement to "be as safe as modern rapid rail", although other performance requirements ruled out the use of conventional vital elements used in the control and safety systems of modern rapid rail. Our design, which uses off-the-shelf microelectronics, proves the efficacy of microprocessor based equipment to critical transit applications (safety, control, etc.).

We discovered, however, a lack of uniform, meaningful safety design and evaluation standards within the transit community. The AGRT program identified serious limitations of existing qualitative techniques, identified quantitative (analytical) tools and techniques, and proved their applicability to transit.

Microprocessors are rapidly proliferating in all types of products from kitchen blenders to automobiles to spacecraft: few other implementations provide the flexibility, reliability, and control possibilities realizable with a programmable controller. Indeed, existing transit suppliers currently offer, or are developing, microprocessor based communication, control, and safety components. A microprocessor based system, however, contains complex hardware and software working in synergism to provide a desired function. This hardware and software must be fully analyzed, understood, tested, and evaluated prior to revenue service. No longer is it possible to certify a system as "safe for revenue service" based upon the "fail-safe application of fail-safe (vital)" components.

The system engineering design approach and statistical safety techniques have been developed and thoroughly proven across several

We conclude that implementation of such a system would reduce troubleshooting time and hence, vehicle downtime. This reduction in maintenance turn around time should translate to reduced maintenance costs and possibly to fewer spare vehicles on a given line.

This demonstration, conducted under UMTA's sponsorship, was conducted in June 1984. The technology demonstration was successful.

stop whenever possible, the safety criteria should be studied to determine the acceptable frequency and allowable deceleration rates for open loop emergency stops. We need to trade the risk of a failure in the closed-loop braking system against the very real possibility of throwing a passenger against interior vehicle surfaces during a worst-case open-loop stop.

This report summarizes UMTA's extensive research and development commitment to enhance the productivity of surface transportation systems. Specific conclusions are summarized in Section 9.0. The studies and papers referenced in Section 10.0 reflect the breadth and depth of this research and development effort.

We believe, as previously noted, that the technology is in place to partially automate existing transit operations. Here, we note that the potential exists to more fully automate new systems. As noted in the Foreword, we regard this report as a starting point rather than an ending.

The thrust of this recommendation is coupled with the conclusion that the technology implemented in an orderly engineered and professionally managed way, will mitigate the need for transit subsidies.

However, the following concern that remains today was succinctly stated as follows in the OTA studies:

"Potential transit system suppliers find it increasingly difficult to justify major corporate investments in transit innovation, given a history of uncertain federal support, unrealistically tight development timetable, complex institutional barriers and the lack of established stable markets".

- 6) The partial implementation of automation, noted in section 3, needs to be coupled with establishment of safety design and evaluation standards.

Here too, the implementation can be enhanced by the cooperative effort of the transit, UMTA, and research and development communities. The action group noted above could formulate mechanisms to coordinate implementation of the technology, establish required safety standards, resolve problems, collect data, and disseminate results.

As stated in the Foreword, we directed this writing to those professionals engaged in the managerial, operations, and maintenance activity of the transit community.

We believe that the transit community should provide the cooperative effort to move the technology forward, and implement the technology that can eventually eliminate government subsidies.

6. D336-10037-2, "AGRT Central Management Simulations Studies Final Report," dated February 1978, by K. Johnson, W. White and F. W. Burns.
7. D336-10038-2, "Local Control Simulation Report-Final", February 1978, by R.A. Hammond and Dr. P. Hawkins.
8. D336-10039-2, "System Availability and Reliability Report", March 1978, by R. Tidball.
9. D336-10040-2, "Final Report-AGRT Automatic Training Studies", February 1978, by R. Dawson and Dr. R. Lang.
10. D336-10041-2, "Final Report-Guideway/Vehicle Cross-Section Minimization Study", February 1978, by W. McLean.
11. D336-10046-1, "AGRT Cost Model and Trades", March 1978, by R. Brock and F.W. Burns.
12. D336-10047-2, "DNS Technical Specification", December 1977, by K. Johnson, D. Striffset, D. Heil, M. Brotherton.
13. D336-10049-1, "AGRT Local Control Simulation Technical Description", January 1978, by R. Hammond, J. Ray and Dr. P. Hawkins.
14. D336-10052-1, "Feasibility Demonstration and Testing of a Collision Avoidance Radar for AGRT", February 1978, by P. D. Drew.
15. D336-10054-1, "Final Report-AGRT Phase IIA Steering/Positive Retention Studies", February 1978, by R. Dawson.
16. D336-10056-1, "AGRT Engineering Test Program Summary Report", October 1978, by L.P. Flesher.
17. D336-10057-1, "AGRT Life Cycle Cost Summary Report", October 1978, by R. Brock and F.W. Burns.

28. "Morgantown People Mover Service Availability, and O&M Costs, History and Projections", Technical Paper, March 1979, by R. Hacker and R. Bates (WVU)
29. "Boeing AGRT Analytic Network Model", Technical Paper 11th, Southeastern Conference on Combinatorics Graph Theory and Computing, March 1980, by G.L. Snider.
30. "The Role of Technology in Urban Transportation-Barriers to Technology Deployment", Presentation Paper, TRB Meeting-Advanced Transit Association, January 1981, by R.M. Hacker.
31. "Some Human Factor Aspects of Computer Controller Transportation Systems", Technical Paper, 26th Annual meeting of proceedings of Human Factor Society.
32. "Morgantown People Mover System Reliability Experience", Technical Paper, 33rd Vehicular Technology Conference-IEEE, May 1983, by R.E. Alberts and W.H. Swan.
33. "Office of Management and Budget (OMB) Circular A-109: New Direction in Major System Acquisition." Issued by the Executive Office of the President, Office of Management and Budget. Became effective May 5, 1977. The primary focus, briefly noted, established formal mission-oriented structure at the front end and extended use of competition beginning earlier and continuing on through the system acquisition process.
34. "Mag-Transit Development at Boeing", Technical Paper, 29th Vehicular Technology Conference-IEEE, March 1979, by R.G. Gilliland.
35. "Combined Magnetic Levitation & Propulsion - The Mag-transit Concept", Technical Paper, 30th. Vehicular Technology Conference-IEEE, February 1980, by R.G. Rule and R.G. Gilliland.

46. "Failsafe Synchronization of Redundant Microprocessor Control Systems", 32nd Vehicular Technology Conference - IEEE Technical Paper, May 1982, D.E. Haberman.
47. "A Vehicle Collision Avoidance System Using Time Multiplexed Hexadecimal FSK", 33rd Vehicular Technology Conference - IEEE Technical paper, May 1983 by C. Colson, E. Nishinaga.
48. "Microprocessor Based Speed and Measurement System", 33rd Vehicular Technology Conference - IEEE Technical Paper, May 1983, by Dr. R.P. Lang and D.J. Warren.
49. "An Implementation of Distinct Software in a Vehicle Controller", 33rd Vehicular Technology Conference - IEEE Technical Paper, May 1983, by W.E. Greve and R.J. Schroeder.
50. "Effects of System Architecture on Safety and Reliability of Multiple Microprocessor Control Systems", 34th Vehicular Technology Conference - IEEE Technical Paper, May 1984, by R.C. Milnor, and R.S. Washington.