

UMTA-WA-06-0011-84-3

# **Advanced Group Rapid Transit Vehicle Control Unit Design Summary**

**William E. Greve  
Donald E. Haberman  
Robert P. Lang**

**FINAL REPORT  
MAY 1985**

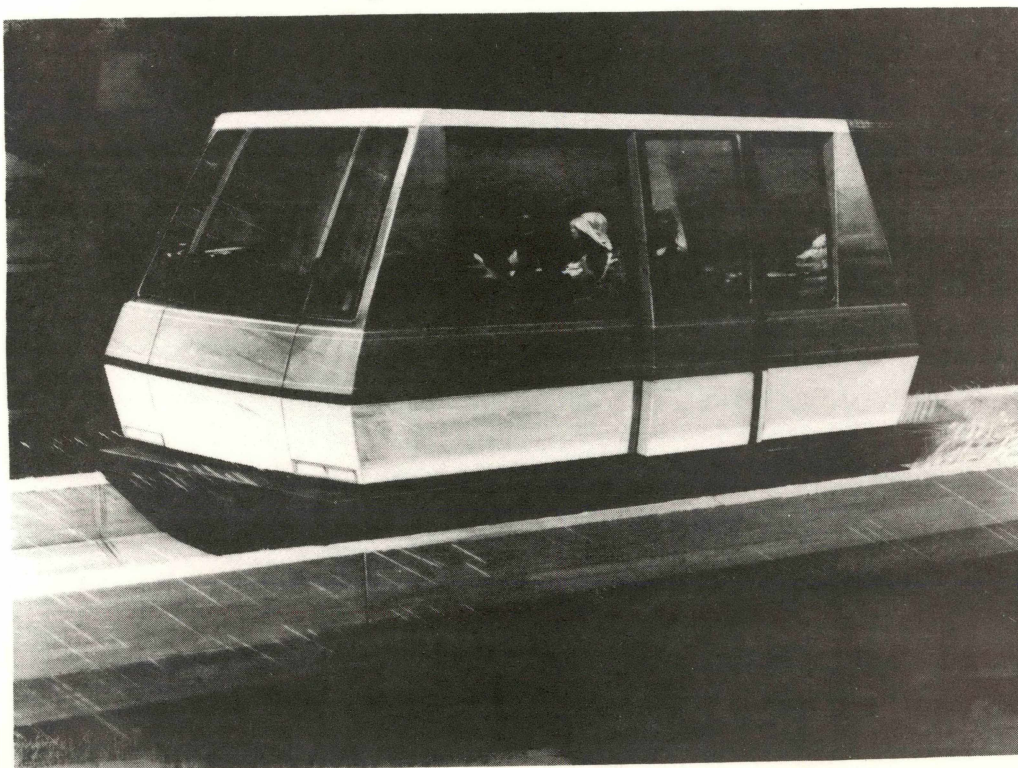
**Boeing Aerospace Company  
Automated Transportation Systems  
Seattle, Washington 98124**



**U.S. Department  
of Transportation**

**Urban Mass  
Transportation  
Administration**

**Office of Technical Assistance  
Washington, D.C. 20590**



#### 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-06-0011-84-3		2. Government Accession No. PB86-169596/AS		3. Recipient's Catalog No.	
4. Title and Subtitle  Advanced Group Rapid Transit Vehicle Control Unit Design Summary.				5. Report Date May 1985	
				6. Performing Organization Code	
				8. Performing Organization Report No.	
7. Author(s) W. R. Greve, D. E. Haberman, and R. P. Lang				10. Work Unit No. (TRAIS) WA-06-0011	
9. Performing Organization Name and Address Boeing Aerospace Company Automated Transportation Systems Seattle, Washington 98124				11. Contract or Grant No. DOT-UT-80041	
				13. Type of Report and Period Covered Final Report September 1978-May 1985	
12. Sponsoring Agency Name and Address U.S. Department of Transportation Urban Mass Transportation Administration 400 Seventh Street, S.W. Washington, D.C. 20590				14. Sponsoring Agency Code	
15. Supplementary Notes					
16. Abstract The purpose of the Advanced Group Rapid Transit (AGRT) program was to develop an advanced automated guideway transit system capable of providing high passenger volumes, short waiting times, and high levels of passenger service. The system is the development of a transportation system consisting of small, automated vehicles operating on a single lane guideway at short headways with unmanned, off-line stations. This report documents the design, development and test activity associated with the Vehicle Control Unit (VCU) for the AGRT program. The VCU is that part of the AGRT control hierarchy carried onboard a transit vehicle that is responsible for overall vehicle control and safety. The vehicle control function involves implementation of wayside commands conveyed to the vehicle by inductive communications and magnetic vehicle status measurements. The VCU controls longitudinal motion (jerk, acceleration, speed, and position); switching; closed-loop emergency stop-ping; and vehicle doors. Safety assurance tasks include overspeed protection, emergency removal of tractive effort, door control, status monitoring, fault protection, and system initialization. The VCU is described in detail, including conclusions as well as recommendations.					
17. Key Words Automated Guideway Transit System; Advanced Automated Guideway Transit System; Advanced Group Rapid Transit Program; Failsafe; Microprocessors; Safety; Vehicle Control and Safety; Vehicle Control Unit Design; Vehicle Longitudinal Control			18. Distribution Statement  This report is available to the public through the National Technical Information Service in Springfield, Virginia 22161.		
19. Security Classif. (of this report) Unclassified		20. Security Classif. (of this page) Unclassified		21. No. of Pages 261	22. Price A12

1. Report No. UMTA-WA-06-0011-84-3	2. Government Accession No.	3. Recipient's Catalog No.	
4. Title and Subtitle Advanced Group Rapid Transit Vehicle Control Unit Design Summary		5. Report Date May 1985	
		6. Performing Organization Code	
		8. Performing Organization Report No.	
7. Author(s) William E. Greve, Donald E. Haberman, Robert P. Lang		10. Work Unit No. (TRAIS)	
9. Performing Organization Name and Address Boeing Aerospace Company Automated Transportation Systems Seattle, WA 98124		11. Contract or Grant No. DOT-UT-80041	
		13. Type of Report and Period Covered Final Report Sept. 1978 - May 1985	
		14. Sponsoring Agency Code URT-12	
12. Sponsoring Agency Name and Address U.S. Department of Transportation Urban Mass Transportation Administration 400 Seventh Street, S.W. Washington, D. C. 20590			
15. Supplementary Notes			
16. Abstract  <p>This report documents the design, development and test activity associated with the Vehicle Control Unit (VCU) for the Advanced Group Rapid Transit (AGRT) program. The AGRT program is the development of a transportation system consisting of small, automated vehicles operating on a single lane guideway at short headways with unmanned, off-line stations. The VCU is that part of the AGRT control hierarchy carried onboard a transit vehicle that is responsible for overall vehicle control and safety.</p> <p>The vehicle control function involves implementation of wayside commands conveyed to the vehicle by inductive communications and magnetic vehicle status measurements. The VCU controls longitudinal motion (jerk, acceleration, speed, and position), switching, closed-loop emergency stopping, and vehicle doors. Safety assurance tasks include overspeed protection, emergency removal of tractive effort, door control, status monitoring, fault protection, and system initialization.</p> <p>The VCU is described in detail, including conclusions as well as recommendations, so that future transit designers can benefit from the program.</p>			
17. Key Words Digital Receiver, Dissimilar Software, Checked Redundancy, Failsafe, Microprocessor, Safety, Emergency Brake, Torque Control, Vehicle Longitudinal Control, Shared Memory, Fiber Optics, Cyclic Executive		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 256	22. Price



# METRIC CONVERSION FACTORS

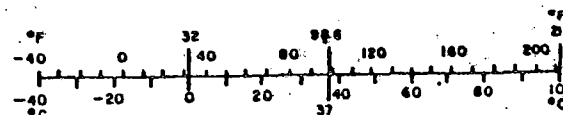
## Approximate Conversions to Metric Measures

Symbol	When You Know	Multiply by	To Find	Symbol
<b>LENGTH</b>				
in	inches	*2.5	centimeters	cm
ft	feet	30	centimeters	cm
yd	yards	0.9	meters	m
mi	miles	1.6	kilometers	km
<b>AREA</b>				
in <sup>2</sup>	square inches	6.5	square centimeters	cm <sup>2</sup>
ft <sup>2</sup>	square feet	0.09	square meters	m <sup>2</sup>
yd <sup>2</sup>	square yards	0.8	square meters	m <sup>2</sup>
mi <sup>2</sup>	square miles	2.6	square kilometers	km <sup>2</sup>
	acres	0.4	hectares	ha
<b>MASS (weight)</b>				
oz	ounces	28	grams	g
lb	pounds	0.45	kilograms	kg
	short tons (2000 lb)	0.9	tonnes	t
<b>VOLUME</b>				
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 <sup>3</sup>	cubic feet	0.03	cubic meters	m <sup>3</sup>
yd <sup>3</sup>	cubic yards	0.76	cubic meters	m <sup>3</sup>
<b>TEMPERATURE (exact)</b>				
°F	Fahrenheit temperature	5/9 (after subtracting 32)	Celsius temperature	°C

\* 1 in. = 2.54 (exact). For other exact conversions and more detailed tables, see NBS Misc. Publ. 289, Units of Weights and Measures, Price \$2.25, SD Catalog No. C13.10.286.

## Approximate Conversions from Metric Measures

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



## PREFACE

This report documents the design, development, and test activity associated with the Vehicle Control Unit (VCU) for the Advanced Group Rapid Transit (AGRT) program. The VCU is that part of the AGRT control hierarchy carried onboard a transit vehicle which is responsible for overall vehicle control and safety. The unit is described in detail, including conclusions as well as recommendations, so that future transit designers can benefit from our experience.

The work described in this report was done for the U.S. Department of Transportation, Urban Mass Transportation Administration. The VCU design and development was accomplished under contract to the Boeing Company, Seattle, Washington.

Portions of the material in this report were originally produced by other members of the AGRT program.

# AGRT VCU FINAL REPORT

## TABLE OF CONTENTS

<u>Section</u>		<u>Page</u>
1.0	SUMMARY CONCLUSIONS	1
2.0	INTRODUCTION	5
3.0	DESIGN OVERVIEW	11
3.1	VCU Major Functions	12
3.1.1	Wayside/Vehicle Communications	12
3.1.1.1	Inductive Communications	12
3.1.1.1.1	Uplink	14
3.1.1.1.2	Downlink	14
3.1.1.2	Magnetic Communications	16
3.1.1.2.1	Reed Switches	16
3.1.1.2.2	Presence Detector Magnet	17
3.1.2	Vehicle Control	17
3.1.2.1	Vehicle Longitudinal Control System	17
3.1.2.1.1	Command Module	20
3.1.2.1.2	Speed and Position Controller Module	22
3.1.2.1.3	Odometer Data Processor	23
3.1.2.1.4	Signal Conditioning	23
3.1.2.2	Emergency Stop Control	24
3.1.2.3	Lateral Control	26
3.1.2.4	Vehicle Exits	26
3.1.3	Safety Assurance Tasks	27
3.1.3.1	Vehicle Collision Avoidance	27
3.1.3.2	Wayside/Vehicle Safe To Proceed Signal	27
3.1.3.3	Overspeed Protection	28
3.1.3.4	Master Clock Supervision	28
3.1.3.5	Status Monitoring	28
3.2	VCU Safety Considerations	31
3.2.1	Safety Design Philosophy	31
3.2.2	Safety Design Approach	32
3.2.3	Safety Principles	33
3.2.4	VCU Safety Implementation	35
3.2.5	Safety Trades	38
3.3	Hardware Architecture	40
3.3.1	General Description	40
3.3.2	Hardware Safety Implementation	44
3.3.3	Internal Configuration	45
3.3.3.1	Dual Redundancy Configuration	49
3.3.3.2	Channel to Channel Data Exchange Unit	49
3.3.3.3	System Clock	51
3.3.4	External Interfaces	53
3.3.4.1	Inductive Communications Signals	57
3.3.4.1.1	FSK Receiver Signals	57
3.3.4.1.2	FSK Transmitter Signal	59
3.3.4.2	Discrete Input/Output Signals	61

**AGRT VCU FINAL REPORT**  
**TABLE OF CONTENTS**  
(Continued)

<u>Section</u>	<u>Page</u>
3.3.4.2.1 Discrete Input Signals	61
3.3.4.2.2 Discrete Output Signals	65
3.3.4.3 Analog Input/Output Signals	67
3.3.4.3.1 Analog Inputs	67
3.3.4.3.2 Analog Outputs	68
3.3.4.4 Vehicle Collision Avoidance Signals	69
3.3.4.5 Odometer Signals	70
3.3.4.6 Motor Controller Signals	70
3.3.4.7 Vehicle Brake Signals	70
3.3.4.7.1 Service Brakes	70
3.3.4.7.2 Emergency Brakes	72
3.4 Software Architecture	72
3.4.1 General Description	72
3.4.1.1 Communication Processor Software General Description	72
3.4.1.2 Main Processor Software General Description	74
3.4.2 Software Safety Implementation	74
3.4.2.1 Redundant Input Management	76
3.4.2.2 Monitoring of Redundant Processing	77
3.4.2.3 Monitoring of Logic Integrity	78
3.4.2.4 Monitoring of Integrity of the Software Processing	79
Hardware	
3.4.3 Main Processor Software	79
3.4.3.1 Initialization and Synchronization	79
3.4.3.1.1 Loading of CPU Internal Register	80
3.4.3.1.2 Software Initialization	80
3.4.3.1.3 Processor Integrity Check During Initialization	81
3.4.3.1.4 Hardware Initialization	81
3.4.3.1.5 System Synchronization and Start of Vehicle Control	82
3.4.3.2 Cyclic Execution	82
3.4.3.2.1 Punch-In	83
3.4.3.2.2 Frame Common Input Processing	83
3.4.3.2.3 Frame One - Data Input	84
3.4.3.2.4 Frame Two - Longitudinal Control	86
3.4.3.2.4.1 Command Module Function	86
3.4.3.2.4.2 Speed and Position Controller Function	87
3.4.3.2.4.3 Signal Conditioning Function	87
3.4.3.2.5 Frame Three - Safety Assurance	87
3.4.3.2.5.1 Overspeed Detection	88
3.4.3.2.5.2 Predispatch Checks	88
3.4.3.2.5.3 Missing and Extra Pulse Checks	88
3.4.3.2.5.4 Closed-Loop Emergency Stop Profile Check	88
3.4.3.2.5.5 Cross Channel Disparity Check of Vehicle Control	89
Command Data	
3.4.3.2.6 Frame Four	89
3.4.3.2.6.1 Fault Reporting	89
3.4.3.2.6.2 Downlinking of FSK Messages	91



**AGRT VCU FINAL REPORT**  
**TABLE OF CONTENTS**  
(Continued)

<u>Section</u>		<u>Page</u>
3.4.3.2.7	Duty Cycle Monitoring	92
3.4.3.3	Background Self Checking	93
3.4.4	Communication Processor Software	94
3.5	Considerations in the Design of the Software	95
3.5.1	The Executive	96
3.5.2	Fixed Point Computation	98
3.5.3	Coding Language Selection	98
3.5.4	Dissimilar Software	99
3.5.5	Code Exercisers	100
3.5.6	Process Monitoring: Test Points and Fault Reporting	102
3.5.7	Single Thread FSK Command Processing	102
3.5.8	Physical Organization of the Software	103
<b>4.0</b>	<b>DETAILED DESIGN DESCRIPTION</b>	<b>104</b>
4.1	Wayside/Vehicle Communications Elements	104
4.1.1	Inductive Communications	104
4.1.1.1	Uplink	109
4.1.1.1.1	FSK Digital Receiver	109
4.1.1.1.2	The Front End Circuit	112
4.1.1.1.3	The Digital Discriminator	118
4.1.1.2	Downlink	120
4.1.1.2.1	FSK Modulator	120
4.1.1.2.2	Antenna Driver/Antenna	120
4.1.2	Magnetic Communications	120
4.1.2.1	Reed Switches	125
4.1.2.2	Presence Detector Magnets	129
4.2	Vehicle Control Hardware Elements	129
4.2.1	Main Processor	130
4.2.1.1	Microprocessor and Memory	135
4.2.1.2	Data Exchange Unit	139
4.2.1.3	Communications Processor Shared Memory	141
4.2.1.4	Watchdog Circuit	141
4.2.1.5	Non-Volatile RAM	146
4.2.2	Communications Processor	147
4.2.2.1	Microprocessor and Memory	151
4.2.2.2	Receivers/Transmitter Interface	151
4.2.2.3	Store/Recall Pulse Generation	155
4.2.3	Timing Functions	156
4.2.4	Digital I/O	156
4.2.5	Analog I/O	163
4.2.6	External RS232 Interface	167
4.2.7	Propulsion Torque Command Data Conversion Unit	170

AGRT VCU FINAL REPORT  
TABLE OF CONTENTS  
(Continued)

<u>Section</u>		<u>Page</u>
<b>5.0</b>	<b>DESIGN VERIFICATION</b>	<b>177</b>
5.1	Test Program Overview	177
5.1.1	Design Verification Test Set	177
5.1.2	Design Verification Tests	181
5.1.3	Summary and Conclusion of Design Verification Tests	182
5.2	Test and Maintenance Features	188
5.2.1	Test Point Outputs	189
5.2.2	Duty Cycle Monitoring	189
5.2.3	Monitor Program	190
5.2.3.1	The Fault Queue	190
5.2.3.2	The Failed Self Test Register	190
5.2.3.3	The Global Data Base	191
5.3	Design Verification Test Results	191
5.3.1	VCU Initialization	191
5.3.1.1	VCU Initialization Characteristics	191
5.3.2	Longitudinal Control - Routine	193
5.3.2.1	Speed and Position Measurements	193
5.3.2.2	Speed and Position Control	195
5.3.2.3	VLCS Stability Margin	197
5.3.3	Longitudinal Control - Special Purpose	198
5.3.3.1	Position Update Response	198
5.3.3.2	Station Stop and Berth Moveup	200
5.3.4	Longitudinal Control - Emergency Stop	201
5.3.4.1	Closed Loop Emergency Stop	201
5.3.4.2	Open Loop Emergency Stop	203
5.3.5	Interfaces	204
5.3.5.1	VCU-VCAS Interface	204
5.3.5.2	FSK Message Processing	205
5.3.6	Anomaly Response	206
5.3.6.1	FSK Uplink Anomaly	206
5.3.6.2	Overspeed Protection	207
5.3.6.3	Safe-To-Proceed	208
5.3.6.4	Fault Induced Stop	209
5.3.6.5	Power Monitoring	210
5.3.6.6	Status Monitoring	212
5.3.7	General Safety	213
5.3.7.1	VCU Self Checks	213
5.3.7.2	Master Clock Tolerance	215
5.3.7.3	A/A Disparity Checks	216

**AGRT VCU FINAL REPORT**  
**TABLE OF CONTENTS**  
(Continued)

<u>Section</u>		<u>Page</u>
<b>6.0</b>	<b>CONCLUSIONS AND RECOMMENDATIONS</b>	<b>217</b>
6.1	Longitudinal Control System	217
6.1.1	Design Features	218
6.1.1.1	Jerk and Acceleration Command Limiter	218
6.1.1.2	Position Update Algorithm	218
6.1.1.3	Speed and Position Measurement System	219
6.1.1.4	Torque Control	220
6.1.1.5	Emergency Stopping Concept	221
6.1.1.6	Station Stop/Berth Moveup	222
6.1.2	Conclusions Based on Design Experience	222
6.1.2.1	General	222
6.1.2.2	Use of Microprocessors	223
6.1.2.3	Value of Analysis and Simulation	223
6.1.2.4	Specification of Requirements	224
6.1.2.5	Mode Switching	224
6.1.3	Applications	224
6.2	Safety	225
6.2.1	Safety Design Constraints	225
6.2.2	Safety Evaluation Constraints	227
6.2.3	Safety Recommendations	227
6.3	Hardware	230
6.3.1	Design Features	230
6.3.1.1	Dual Channel Configuration	231
6.3.1.2	Dual Channel Timing System	231
6.3.1.3	Data Exchange Unit	232
6.3.1.4	FSK Digital Receiver	232
6.3.1.5	Odometer Preprocessors	233
6.3.1.6	Fiber Optic Propulsion Data Link	233
6.3.2	Conclusions Based on Design Experience	234
6.3.3	Future Design Considerations Based on Advances in Technology	235
6.3.4	Applications for High Technology Hardware in the Transportation Industry	235
6.4	Software	236
6.4.1	Design Features	236
6.4.1.1	The Executive	236
6.4.1.2	High Order Language	237
6.4.1.3	Emergency Code Exercisers	237
6.4.1.4	Dissimilar Software	238
6.4.1.5	RAM and Register Checks	238
6.4.1.6	Fault Queue Management	239
6.4.2	Conclusions Based on the Design Experience	239
6.5	Test	240
6.5.1	Built in Test Points	240
6.5.2	Real-Time Closed-Loop Testing	241
6.5.3	Digital Data Acquisition and Processing	242
6.6	Availability	242
<b>7.0</b>	<b>BIBLIOGRAPHY</b>	<b>248</b>

# AGRT VCU FINAL REPORT

## LIST OF FIGURES

<u>Figure</u>		<u>Page</u>
2.0-1	EDS Command and Control Hierarchy	7
3.1.1.1-1	Inductive Link Modulation Format	13
3.1.1.1.1-1	FSK Message Formats	15
3.1.2.1-1	VCU VLCS Requirements	18
3.1.2.2-1	Closed-Loop Mode Emergency Stop Error Limits	25
3.1.3.3-1	Vehicle Speed Limit Profiles	29
3.2.3-1	Safety Design Principles - During AGRT Program	34
3.2.4-1	Checked Dual Redundant VCU	36
3.2.4-2	Symmetrical Dual-Dissimilar Software With Redundant Software Disparity Check Logic	37
3.2.4-3	Safety Hierarchy	39
3.3.1-1	Vehicle Command and Control Block Diagram	41
3.3.1-2	Vehicle Control Electronics Interfaces	43
3.3.3-1	Simplified Block Diagram of VCU Electronics	46
3.3.3-2	Basic Vehicle Control Unit Configuration	48
3.3.3.1-1	Checked Dual Redundant VCU	50
3.3.3.3-1	Timing Block Diagram	52
3.3.3.3-2	System Clock Distribution	54
3.3.4.1.1-1	FSK Receiver Signal Paths	58
3.3.4.1.2-1	FSK Transmission Signal Paths	60
3.3.4.6-1	EDS Propulsion Interface	71
3.3.4.7.2-1	Emergency Brake Command System	73
4.1-1	Wayside/Vehicle Communications Elements	105
4.1.1-1	Inductive Communications Demonstration Configuration	108
4.1.1-2	Plot of Receiver Sensitivity to Sinusoidals vs. Freq.	110
4.1.1.1.1-1	Method of Frequency Demodulation	111
4.1.1.1.1-2	Analog Front End Block Diagram	113
4.1.1.1.1-3	Digital Demodulator Block Diagram	114
4.1.1.1.1-4	FSK Digital Receiver Card	115
4.1.1.1.2-1	Effects of Sinusoidal Interference and Inpulse Noise	117
4.1.1.1.3-1	Receiver Software Structure	119
4.1.1.2-1	FSK Downlink	121
4.1.1.2.1-1	FSK Downlink Modulator	122
4.1.1.2.1-2	FSK Modulator Card	123
4.1.1.2.2-1	FSK Transmitter Antenna Driver	124
4.1.2-1	Guideway Cross-Section	126
4.1.2-2	Vehicle Reed Switch Locations	127
4.1.2.1-1	Presence Detection and Magnetic Signalling Components	128
4.2-1	Block Diagram of VCU Control Electronics	131
4.2-2	VCU Card Cage	132
4.2-3	Photograph of VCU Channels 1 and 2	133
4.2.1-1	Main Processor Card	134
4.2.1.1-1	Microprocessor and Memory	136
4.2.1.1-2	VCU Main Processor Memory Configuration	138
4.2.1.2-1	Cross Channel Data Exchange Unit	140
4.2.1.3-1	Communications Processor Shared Memory	142
4.2.1.4-1	Watchdog Circuitry	144



**AGRT VCU FINAL REPORT**  
**LIST OF FIGURES**  
(Continued)

<u>Figure</u>		<u>Page</u>
4.2.1.4-2	Timing Diagram	145
4.2.1.5-1	Non-Volatile RAM (NOVRAM)	148
4.2.2-1	Communications Processor Card Block Diagram	149
4.2.2-2	Communications Processor Card	150
4.2.2.1-1	Communications Processor Memory and Control Diagram	152
4.2.2.1-2	VCU Communications Processor Memory Configuration	153
4.2.2.2-1	Receivers/Transmitter Interface	154
4.2.3-1	System Timing Configuration	157
4.2.3-2	Timing Card	158
4.2.4-1	Digital I/O Card Functions	159
4.2.4-2	Digital I/O Card	160
4.2.4-3	Discrete Input/Output Signals	161
4.2.4-4	Basic Speed and Position Measurement System	164
4.2.5-1	Analog I/O Card Functions	165
4.2.5-2	Analog I/O Card	166
4.2.6-1	External RS232 Interface Card Block Diagram	168
4.2.6-2	External RS232 Interface Card	169
4.2.7-1	VCU/Propulsion System Interface	171
4.2.7-2	Photograph of PTCDCU	172
4.2.7-3	PTCDCU Block Diagram	174
4.2.7-4	Data Transfer in the Propulsion Data Link	176
5.1.1-1	Design Verification Test Configuration	178
5.1.1-2	Test Article and TSG	179
5.1.1-3	Test Vehicle Simulator	180
6.6-1	Comparison of Control System Configurations	243
6.6-2	Typical Intervals Between Service Interruptions	246
6.6-3	Complexity Comparison	246
6.6-4	Configuration Performance Comparison	246

**LIST OF TABLES**

<u>Table</u>		<u>Page</u>
3.3.4-1	VCU Electrical Interfaces	55
5.1.2-1	VCU Test Program Overview	183

## AGRT VCU FINAL REPORT GLOSSARY

AAR	- Association of American Railroads
ADC	- Analog To Digital Converter
AGRT	- Advanced Group Rapid Transit
A/D	- Analog To Digital
BER	- Bit Error Rate
CAS	- Collision Avoidance System
CAL	- Calibration
CDR	- Critical Design Review
CMOS	- Complementry Metal Oxide Semiconductor
CPU	- Central Processing Unit
CRC	- Cyclic Redundancy Check
CRT	- Cathode Ray Tube
CTC	- Counter Timer Chip
C&CS	- Command and Control System
DAC	- Digital To Analog Converter
DEU	- Data Exchange Unit
DIP	- Dual Inline Package
EDS	- Engineering Development System
EEPROM	- Electrically Erasable Programmable Read Only Memory
EPROM	- Erasable Programmable Read Only Memory
FIFO	- First-In-First-Out
FMEA	- Failure Mode and Effects Analysis
FPS	- Feet Per Second
FSK	- Frequency Shift Keying
F/F	- Flip-Flop
GCCS	- Guideway Command and Control Subsystem
GCU	- Guideway Communications Unit
HOL	- High Order Language
ICS	- Inductive Communication Subsystem
ID	- Identification
I/O	- Input/Output
LCS	- Longitudinal Control System
MPM	- Morgantown People Mover
MR	- Master Reset
MSI	- Medium Scale Integration
MTBF	- Mean Time Between Failures
MTBSI	- Mean Time Between Service Interruptions
MTBUF	- Mean Time Between Unsafe Failures
NMOS	- N Channel Metal Oxide Semiconductor
NOVRAM	- Non-Volatile Random Access Memory
ODD	- Odometer Data Downlink
ODDCAS	- Odometer Data Downlink Collision Avoidance System
PAL	- Programmable Array Logic
PC	- Position Correction
PD	- Presence Detector
PRF	- Pulse Repetition Frequency
PTCDCU	- Propulsion Torque Command Data Conversion Unit

AGRT VCU FINAL REPORT  
GLOSSARY  
(Continued)

RAM	- Random Access Memory
RMS	- Root Mean Square
ROM	- Read Only Memory
SIO	- Serial Input Output
SSI	- Small Scale Integration
STP	- Safe-To-Proceed
STTF	- Surface Transportation Test Facility
TCCS	- Test Track Command and Control Subsystem
TSG	- Test Scenario Generator
TTL	- Transistor Transistor Logic
TVS	- Test Vehicle Simulator
UMTA	- Urban Mass Transportation Administration
UART	- Universal Asynchronous Receiver/Transmitter
UPC	- Universal Peripheral Controller
VCAS	- Vehicle Collision Avoidance Subsystem
VCCS	- Vehicle Command and Control Subsystem
VCE	- Vehicle Control Electronics
VCU	- Vehicle Control Unit
VLCS	- Vehicle Longitudinal Control System
VRC	- Vertical Redundancy Check
WCAS	- Wayside Collision Avoidance System

## 1.0

## SUMMARY CONCLUSIONS

The Advanced Group Rapid Transit (AGRT) Vehicle Control Unit (VCU) described in this report is a microprocessor based system employing advanced technology and innovative design features not commonly found within the transportation industry in the United States. The system analysts and designers have blended together hardware, software, and safety concepts into a control system that has the capability of safely moving unmanned vehicles along a guideway. A number of design features evolving from this program merit consideration for current and future transit industry applications.

The system was designed to operate with off line stations and an extremely short three-second headway; however, the system is easily adaptable to other configurations with longer headways. The system was tested with an elaborate test set that exercised the final VCU hardware and software in a real-time closed-loop manner. It is noteworthy that at no time during the test program did the VCU respond with an unsafe reaction.

This report discusses in detail the design, development, and test of that portion of the system hierarchy responsible for the direct control of an automated transit vehicle. This control is provided by the Vehicle Control Unit (VCU) which utilizes several microprocessors, with associated software, in a distributed architecture. The heart of the Vehicle Control Unit is the onboard position and speed controller. Embedded software programs are included for safety. In combination with the uplink, the VCU enforces the speed limit and maintains safe vehicle separation. Conventional "vital" electromechanical components could not be used due to reaction speed and physical size considerations.

The VCU is a dual channel microprocessor-based controller with disparity checking and selective dissimilar software. It is responsible for the vehicle control and safety functions which, in general terms, are similar to the Automatic Train Operation (ATO) and Automatic Train Protection (ATP) functions of conventional rail systems. Unique and distinct software algorithms have been developed for these control and safety functions. This allows modification of algorithms associated



with one function without affecting the logic of the algorithms associated with the other function.

Some of the salient features of the VCU design include checked redundancy in both the hardware and software. The two hardware channels are basically identical, while the software design employs dissimilar algorithms to detect hardware failures and embedded software errors. The VCU performs many complex functions but its basic architecture is deliberately simple. The software is written in a Higher Order Language (HOL) which provides portability to other microprocessor based systems as well as enhancing testability and maintainability.

Built-in test features provide internal checks that are continually being exercised in the background as the real-time control functions safely guide the vehicle towards its destination. These internal checks ensure the integrity of the hardware and software processes.

External analog and digital outputs are provided for monitoring internal parameters and functions; these outputs proved invaluable during the checkout and testing phases of the program. These outputs provide a valuable maintenance feature and ultimately could serve as a basis for the design of automated test equipment.

An additional point for discussion: the VCU uses standard off-the-shelf parts. The VCU as tested was built using commercial grade parts but military specification temperature range parts are available for a production unit. One channel of a production unit would fit in a package approximately 5 inches by 10 inches by 10 inches, and it would contain four printed circuit cards. Each channel would require approximately 18 watts of power.

The basic VCU architecture can perform virtually any job requiring the processing of input data, storing the data, making calculations and decisions, and outputting signals based on past and present information. The VCU has the capability to input and output digital and analog information. With minimum interface modifications and the appropriate software provided, a single channel could be installed on a train and provide a number of functions; for example, it could serve as a monitor

that supplies warnings and prompts to the operator of a manually controlled train. It could be used as a maintenance diagnostic system to locate problems and predict future failures. With the addition of a non-volatile memory, status and events prior to an accident could be saved for post accident processing.

It should be mentioned that transit properties now realize that, in today's fast moving electronics industry, the half-life of a product is three to five years. Spares procurement over a thirty year system life is a valid concern. Not always will new parts support older designs. It is quite likely that a circuit card will have to be modified or redesigned; however, by keeping the design modular by function, the cost of a hardware change can be kept low.

The most costly item to develop is the software, and it is important to keep it a non-recurring cost. Although the past history of microprocessor development is one of rapid advancement, the instruction set of an early design is generally carried forward into the new generation hardware. This makes the new device upward compatible with the already developed software. The pin configuration and physical size may be different (which will necessitate a hardware change), but a costly software redesign will not be necessary.

Another consideration is that software written in a Higher Order Language can be compiled to run a microprocessor with an entirely different instruction set. Some software cost would be incurred in making the change, but the cost would be modest compared to a complete redesign/recoding.

A third consideration is that a microprocessor module could be designed to emulate the instruction set of the original microprocessor. This would be the most costly of the alternatives; however, it avoids a very expensive software redesign.

## Innovative Features

Numerous innovative design features have evolved during the development of the Vehicle Control Unit. The design is a combination of hardware, software, and safety concepts suitable for current transit industry applications. The design, in addition to safety and operability advantages, offers improvements in reliability, maintainability, volume, and cost.

Specific innovative features of the VCU design include:

- Microprocessor-Based Speed and Position Measurement System
- State of the Art Point Follower Longitudinal Controls
- Closed-Loop Emergency Stopping Controls with Open-Loop Backup
- High Performance Overspeed Protection Algorithms
- Failsafe Synchronized Dual Redundancy Architecture
- Backup Dissimilar Software for Safety Enhancement
- FSK Digital Receiver
- Dual Channel Synchronous Timing System
- Cross Channel Data Exchange Unit
- Odometer Preprocessing Function

Details of these features are contained within this report. Design details of hardware with which the VCU interfaces are contained in other National Technical Information Service (NTIS) reports; these reports are listed in the bibliography.

## 2.0

## INTRODUCTION

The Advanced Group Rapid Transit (AGRT) program was conceived shortly after TRANSP0 '72, a Department of Transportation (DOT) sponsored transportation exhibition held at Dulles Airport. The purpose of the AGRT program was to develop an advanced automated guideway transit system capable of providing high passenger volumes, short waiting times, and high levels of passenger service; this resulted in requirements with a peak line capacity of 14,000 seated passengers per lane per hour using 12-passenger (all seated) vehicles operating with off-line stations and 3-second minimum headways.

The program was initially structured as a two-phase development program with three prime contractors participating in the Phase I preliminary design competition. Phase II was originally intended to proceed with full scale test track prototype development with one contractor selected from the original three.

After the completion of Phase I, 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 which involved design refinements and laboratory testing of selected key components. As Phase II-A was nearing completion in the fall of 1977, a DOT task force was formed to again review the program and chart a course for further activity. During this review period, Phase II-A was completed and one of the three contractors, Rohr Industries Inc., withdrew from the program. At that time, Rohr Industries Inc. signed a licensing agreement with the Boeing Company granting rights to Rohr's integrated magnetic propulsion and suspension technology.

As a result of the DOT Task Force's recommendations, the period of performance was extended from 36 months to 69 months. The restructured program provided for development and track testing of "Engineering Development Systems" (EDS) by each of the two remaining contractors, the Boeing Company and Otis Elevator Company. Letter contracts were signed in the fall of 1978 to provide for limited system engineering and to



work out the detailed definition of Phase II-B. The full AGRT EDS activity commenced with the awarding of definitive contracts in June, 1979. The primary thrust of the redefined program was to develop the critical technologies associated with the AGRT concepts. Initial Phase II-B efforts at the Boeing Company included design of the Command and Control System, a new vehicle, and a new test track.

By the spring of 1981, as a result of funding limitations, it became apparent that the most critical element of Boeing's AGRT design was the Command and Control System (C&CS). Activity was cancelled on the new vehicle and test track design and development, and in early 1982 a decision was made to use Boeing's existing test track for the EDS program. (This track was used for vehicle testing during the Morgantown program). In addition, two Morgantown vehicles would be modified to accept the new AGRT Command and Control System and allow for development of the critical elements of AGRT.

In mid 1982, UMTA initiated another comprehensive program review to define the status of the program and clarify the expected results. This review resulted in the decision to eliminate all vehicle/test track testing and only allow continuation of development and laboratory testing of selected subsystems rather than the entire EDS. As a result, the AGRT program at the Boeing Company resulted in completion of the Vehicle Control Unit (VCU) hardware and software development only through laboratory (simulation) testing. The Guideway Communication Unit (GCU) and Collision Avoidance System (CAS) development were stopped at the successful completion of Critical Design Review.

Figure 2.0-1 shows the major subsystems of the EDS C&CS and their interrelationships. These subsystems consist of a Test Track Command and Control Subsystem (TCCS), a Guideway Command and Control Subsystem (GCCS), and a Vehicle Command and Control Subsystem (VCCS).

The TCCS provides operator controls and displays, guideway traffic control commands, test data monitoring, and those functions that are neces-

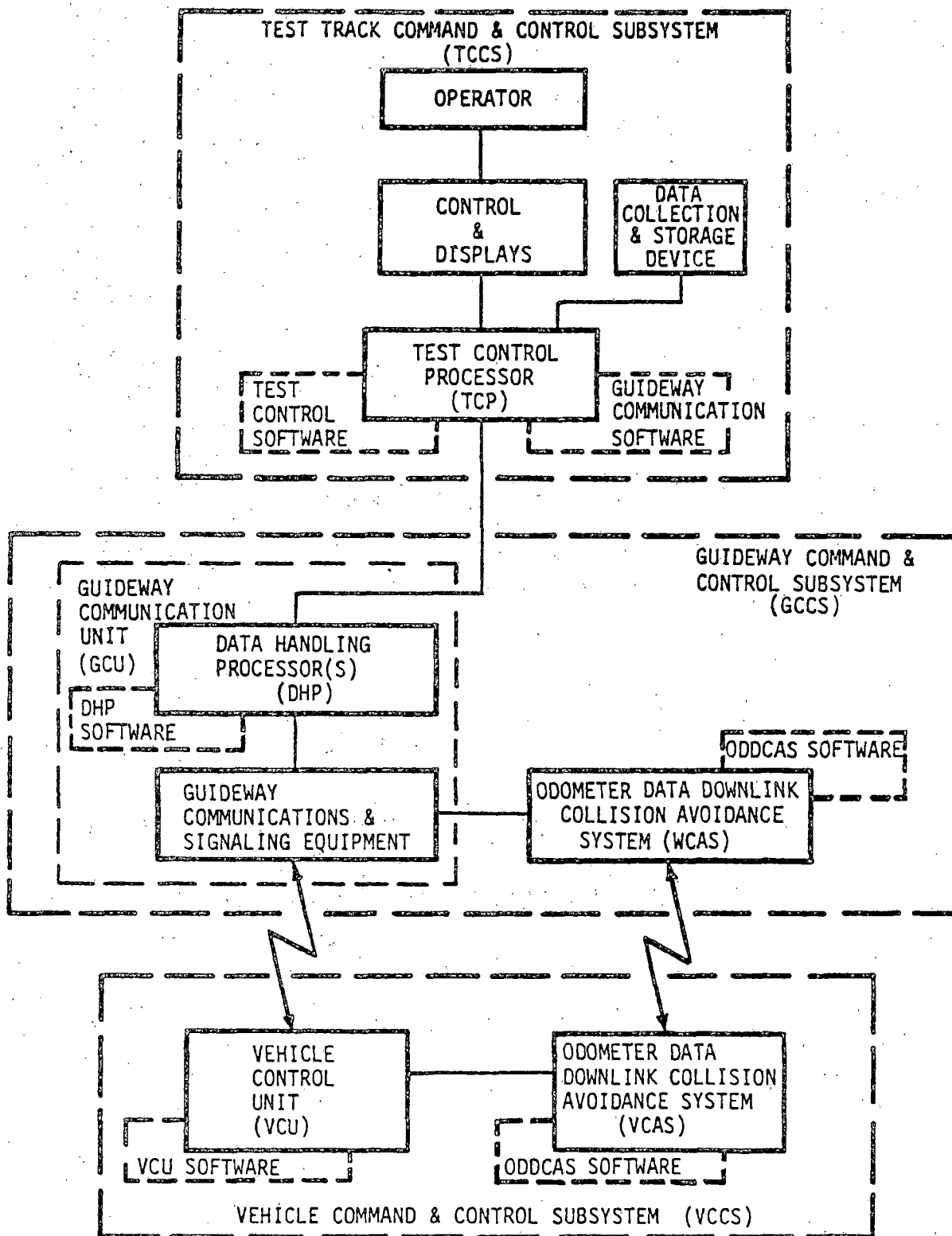


FIGURE 2.0-1: EDS COMMAND AND CONTROL HIERARCHY

sary to supervise the operation of the GCCS. The Guideway Communications Unit (GCU) serves as a communication link between the station and vehicles on the guideway and consists of communication circuits in the station and communication equipment installed in the guideway. The VCCS is a vehicle controller/sensor package located on each vehicle in the fleet; it controls each vehicle according to the commands received from the TCCS via the GCU.

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 are 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 that must 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 any guideway loop, regardless of length, results in an emergency stop of all vehicles over the affected loop. (STP removal is commanded by the Collision Avoidance System when a headway violation occurs.)

Vehicle position is established and maintained by a "point follower" position control concept using vehicle generated and wayside generated moving points.

The Vehicle Control Unit (VCU), the subject of this report, resides in the VCCS and interfaces with the Guideway Communications Unit (GCU) and the Vehicle Collision Avoidance Subsystem (VCAS).

Implementation of the critical functions of the AGRT system is achieved through use of the vehicle borne VCU; it has final responsibility for overall operation and safety of the vehicle. Vehicle operation involves implementation of wayside commands conveyed to the vehicle by inductive communication and magnetic signalling. On the basis of these commands, and in accordance with vehicle status measurements, the VCU controls longitudinal motion (jerk, acceleration, speed, and position), lateral switching, closed-loop emergency stopping, and vehicle doors. Safety assurance tasks include overspeed protection, emergency removal of tractive effort, door control, status monitoring, fault protection, and system initialization.

The development of AGRT subsystems has resulted in several innovative solutions to difficult problems faced by all control system designers. One such solution is a digital receiver, implemented with a microprocessor, capable of operating in a high impulse noise environment. (Such noise is common with vehicle chopper type propulsion systems, and can result in degraded wayside/vehicle signaling.)

In addition, a fully automated, dual channel microprocessor-based vehicle controller was developed. It employs selected hardware redundancy, associated selective dissimilar software, and disparity checking to provide protection against hardware failures and software errors. The controller hardware is adaptable to use in a "dual-duplex" configuration that would provide additional redundancy for freedom from service interruptions. Although not implemented, this concept is described further in Section 6.6.

The dual channel vehicle controller required close coupled synchronization without defeating channel independence; the resulting timing system design allows redundant systems to make sequential calculations and perform disparity checking on each other's data in a close coupled, synchronized system in a safe manner.

The microprocessor hardware and software techniques developed have also produced the capability to generate and transmit a speed limit from the wayside to a vehicle in a failsafe manner.

Any or all of these techniques could be used in other transportation industry applications; Section 6.0 contains further conclusions and explanations.

In summary, the Vehicle Command and Control Subsystem serves as the eyes, ears, and brains of an 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 Subsystem (VCAS) and the microprocessor based Vehicle Control Unit (VCU). This report describes the design, development, and testing of the VCU for the AGRT Engineering Development System.

### 3.0

### DESIGN OVERVIEW

A vehicle control concept capable of meeting the stringent performance and safety requirements of a short headway (3 second) automated transit system is described in this report. The electronic hardware built and tested provides the intelligence, the decision making elements that have the responsibility for the operation and safety of the unmanned vehicle.

The electronics developed are not based on previous designs, but on state-of-the-art microprocessor and associated software design techniques. The use of microprocessors in the design was selected as the way to satisfy the requirement to simultaneously maintain a safe vehicle separation, detect and promptly react to faults, and perform specific longitudinal speed and position control algorithms. In our judgement, only a microprocessor based system could perform within these timing and performance limits. A system built of discrete parts, such as transistors, resistors, capacitors, and inductors, to function within the timing and performance limits, would be too large to fit in the vehicle it was trying to control.

Another major point of concern during the development of the vehicle controller was safety. The AGRT Control system is required to have an ultimate operational safety goal equivalent to or better than modern rapid rail transit systems. To achieve this safety objective, failsafe design principles are applied throughout the design which will cause the system to revert to a safe state if any malfunction should occur that affects safety.

The final vehicle controller design is unique within the transit industry. A number of innovative design solutions, in both hardware and software, were developed which could be used, in part or whole, for present day transit system design solutions.

### 3.1 VCU Major Functions

The VCU major functions are the communications between the wayside and the vehicle, the control of the vehicle, and the safety assurance of the vehicle. The following sections discuss these three major functions.

#### 3.1.1 Wayside/Vehicle Communications

The vehicle, as it travels down the guideway, must keep in communications with the AGRT control hierarchy. The vehicle does this by communicating with the Guideway Communications Unit (GCU). The vehicle communication elements consist of the Inductive Communications Subsystem (ICS) and the Magnetic Communications Subsystem.

##### 3.1.1.1 Inductive Communications

The VCU communicates with the wayside via inductively coupled data links operating with carrier frequencies between 90 KHz and 150 KHz. Wires embedded in the guideway running surface are coupled inductively to the vehicle uplink and downlink loop antennas for message reception and transmission.

Each message is 40 milliseconds in length and divided into 50 equal bit times. Referring to Figure 3.1.1.1-1, the data is encoded in a bi-polar return-to-zero format and Frequency Shift Keying (FSK) is used, with the higher carrier frequency representing a logic "1" and the lower frequency representing a logic "0". During the last half of each bit period the carrier is not transmitted. This technique allows the on-board FSK receiver to extract a bit-rate clock signal, independent of the data, that is used as a safe-to-proceed (STP) tracer signal. The carrier signal is removed during two bit times for framing to indicate the start of the next message.

To provide protection against accepting false messages, the last 16 bits of the FSK message are comprised of a Cyclic Redundancy Code (CRC). A 16-bit CRC and the generator polynomial ( $x^{16} + x^{12} + x^5 + 1$ ) provides



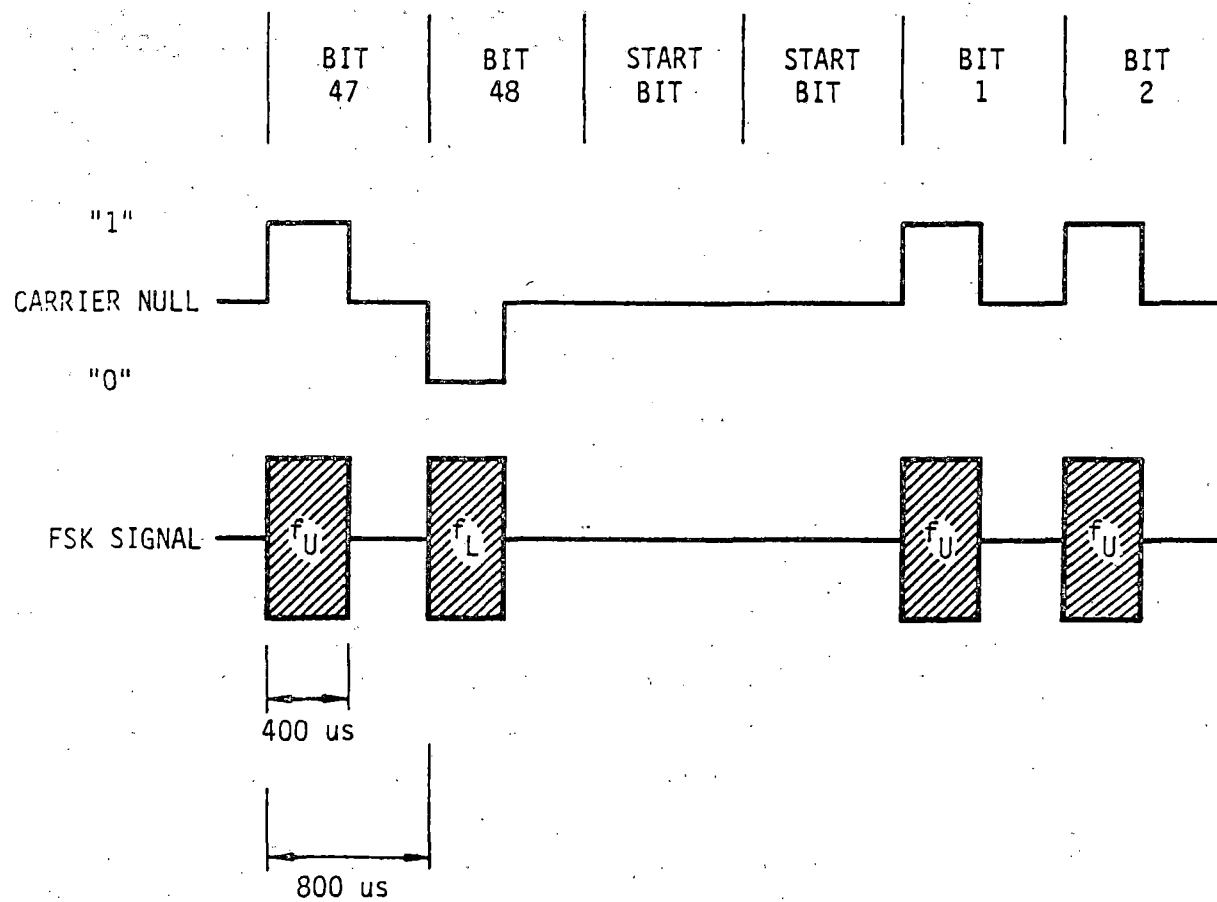


FIGURE 3.1.1.1-1: INDUCTIVE LINK MODULATION FORMAT

100% detection of single and double bit errors. Also, the CRC provides 100% detection of burst errors up to and including length 16, with burst errors of length greater than 16 having a 99.96% detection rate.

The inductive communications design is consistent with the system bit error rate (BER) goal of  $1 \times 10^{-5}$  in noise environments generated by the MPM vehicle. With the projected error rate and the protection provided by the CRC, the probability of the VCU accepting a message in error is very small. Analysis and tests confirm the excellent performance of the message structure and hardware design. (Laboratory tests indicate that the BER will be better than the stated goal; also, additional protection is provided within the message for the safety critical speed limit with a 3-bit Vertical Redundancy Check (VRC) code.)

#### 3.1.1.1.1 Uplink

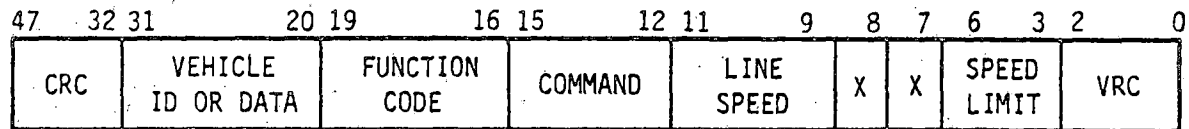
The inductive communications uplink provides speed and dispatch commands, performance levels, door commands, switch commands, position correction commands, and destination/itinerary data. The uplink message format is as shown in Figure 3.1.1.1.1-1.

The uplink FSK receivers extract the digital data and the clock or safe-to-proceed (STP) tracer signal and provide the STP to the Main Processor as a dynamic logic signal indicating STP presence. The receivers announce the loss of STP within 30 milliseconds of loss of FSK signal energy or absence of the STP. The digital data information is provided to the Communications Processor for further processing before the pertinent information is passed to the Main Processor.

#### 3.1.1.1.2 Downlink

The inductive communications downlink provides vehicle identification, fault data, routine status, requestable reports, and destination data to the wayside. The downlink message format is also shown on Figure 3.1.1.1.1-1. In the AGRT design the downlink is not considered a vital link; therefore, only a single thread downlink is provided.

### UPLINK MESSAGE FORMAT



### DOWNLINK MESSAGE FORMAT

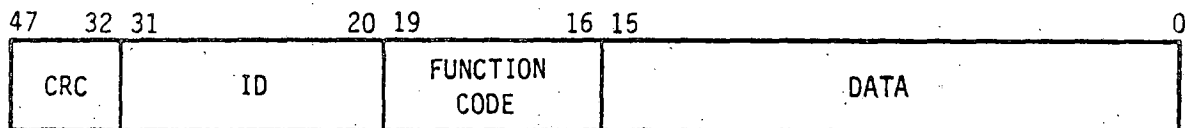


FIGURE 3.1.1.1.1-1: FSK MESSAGE FORMATS

### 3.1.1.2 Magnetic Communications

The magnetic signalling subsystem provides a second interface between the vehicle and wayside. This subsystem consists of magnets embedded in the guideway surface that perform one of three different functions dependent on the lateral guideway location. The magnets actuate vehicle mounted reed switches that initiate vehicle actions.

Also included in this subsystem are presence detectors (PD's) consisting of reed switches, buried in the guideway, that are actuated by a magnet mounted on the vehicle.

#### 3.1.1.2.1 Reed Switches

The chassis-mounted reedswitches are actuated by a longitudinal magnetic flux created by permanent magnets at various guideway locations. Three quad-redundant reedswitch assemblies are provided to detect three separate functions; these functions are switch initiate, station stop initiate, and position correction/calibration (PC/CAL) request.

Upon closure of the switch initiate reed switch, the VCU commands the vehicle steering mechanism to guide from the left or right guide rail per a previously stored FSK uplink command message.

Closure of the station stop initiate reedswitch causes the VCU to initiate an irrevocable station stop maneuver by following a predetermined speed vs. distance profile. The commanded speed at any point of the curve will be a function of the distance traveled from reed switch closure validation.

Upon closure of the position correction/calibration request reedswitch, the VCU, unless disabled by a prior calibration enable uplink message, will open a communication window of 0.48 seconds during which time position update messages from the wayside will be accepted. If this is the first validated position correction/calibration request reedswitch closure after a calibration enable uplink message, the VCU will also

initiate the odometer calibration function. This calibration function will be terminated at the next position correction/calibration request reedswitch closure. The calibration function assumes a  $(N \times 100)$  foot spacing between reedswitch closures, where  $N$  is a integer greater than 5 but less than or equal to 10. This allows for an FSK loop length of from 500 to 1000 feet (in 100 foot increments).

#### 3.1.1.2.2 Presence Detector Magnet

A permanent magnet mounted on the vehicle guide axle above the running surface activates presence detectors mounted along the guideway. These guideway mounted detectors will: announce the arrival of the vehicle into a new loop in order to initiate the position correction sequence; confirm the accurate stop of a vehicle in the station berths; verify the proper execution of a vehicle dispatch. The vehicle magnet will activate the wayside reedswitches when the magnet and reedswitch assembly centerlines are within 5.0 inches plus or minus 5.0 inches of each other.

### 3.1.2 Vehicle Control

#### 3.1.2.1 Vehicle Longitudinal Control System

The vehicle longitudinal control system (VLCS) computes the motor torque and braking torque commands necessary to implement the wayside commanded vehicle speed and position correction commands during normal operation. It is also responsible for providing the controls necessary to implement closed-loop emergency stopping in response to an emergency stop command. Functionally, the control system is partitioned into four parts: namely the Command Module Function, the Speed and Position Controller Function, the Odometer Data Processor Function, and the Signal Conditioning Function.

A simplified block diagram of the VLCS is given in Figure 3.1.2.1-1. The Command Module Function accepts input signals, principally derived from the FSK uplink messages, and issues profiled acceleration, speed,

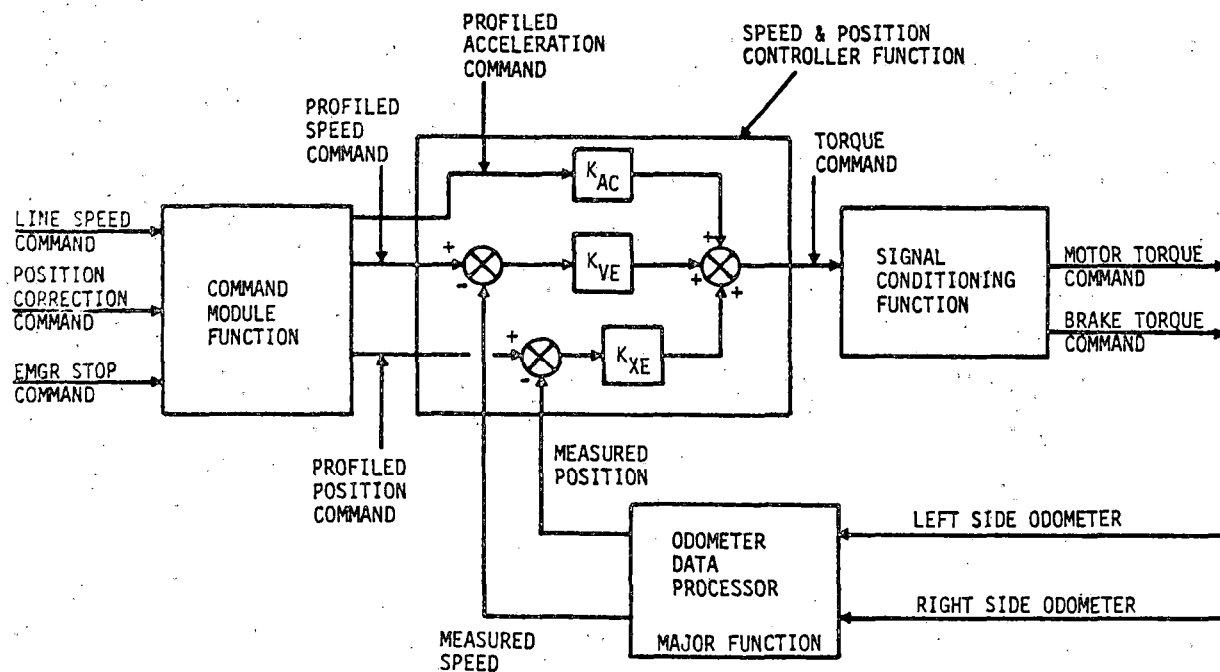


FIGURE 3.1.2.1-1: VCU VLCS REQUIREMENTS



and position commands to the Speed and Position Controller Function. Measured position and measured speed from the Odometer Data Processor Function close the feedback loop to the controller. The single resulting torque command is rate limited and split into separate output signals by the Signal Conditioning Function for delivery to the brake and motor interfaces.

The basic functions implemented in the four control system modules follows.

The longitudinal control algorithms and requirements described in this document were derived from system level longitudinal requirements via a series of design and error analyses. Compliance with these system requirements is a joint responsibility involving the VCU, propulsion system, brake system, vehicle system and wayside C&CS elements. To give the reader a better understanding of the control system algorithms a brief summary of key longitudinal control system-level requirements follows.

1. Position (Headway) Regulation:  $\pm 0.18$  second 0.997 probability limits per vehicle per 1000 feet of travel at constant 22 feet per second, requirement varies with speed.
2. Station Stop Accuracy: Within  $\pm 6$  inches of designated stop point.
3. Emergency Stopping Distance: 53.3 foot worst case upper limit for stops from a measured speed of 22 feet per second, requirement varies with speed.
4. Position Measurement: Maximum long term errors in the sum of incremental position measurements shall be limited, in the absence of failures, to  $\pm 0.7$  percent for measured speeds of 20 feet per second or greater and to  $\pm 3.3$  percent below 20 feet per second. Worst case errors, given the presence of any undetected single noncorrelated failure shall be limited to +2.1 percent, -0.7 percent (+9.9, -3.3 percent below 20 feet per second) where a negative sign indicates a measurement value which is lower than the actual position.

5. Speed Regulation:  $\pm 2.0$  feet per second 0.997 probability limits on error between profiled speed command and onboard measured speed value.
6. Speed Measurement: Maximum error in the measurement relative to true speed in guideway centerline coordinates shall be limited to  $\pm 0.5$  feet per second in the absence of failures. Worst case errors for any condition involving a single undetected non-correlated failure shall be limited to  $\pm 1.5$ ,  $-0.5$  feet per second where a negative sign indicates the measured value is less than the true speed.
7. Acceleration Limits:  $\pm 8.05 \text{ fps}^2$  maximum limits during normal maneuvering,  $14.8 \text{ fps}^2$  0.997 probability limit on deceleration (exclusive of driveline oscillations) during closed-loop emergency stops.
8. Jerk Limits:  $\pm 6.4 \text{ fps}^3$  (normal mode) and  $\pm 32.2 \text{ fps}^3$  (closed-loop emergency mode) 0.997 probability limits on average jerk over time interval of 0.7 second or greater, limits vary with duration of transient and are higher for shorter time intervals.

#### 3.1.2.1.1 Command Module

The Command Module performs the following functions:

1. Generates an internal line speed value based on GCCS line speed and position correction commands. In constant speed regions, any required change in the onboard point is accomplished by increasing or decreasing the line speed value by the commanded amount for the commanded duration. In speed transition areas, the GCCS commanded delay time (relative to PC/CAL magnet detection) is used to establish when the change in internal line speed value is to occur.
2. Controls synchronization of the commands in the redundant VCU channels.

3. Generates a position correction command uplink window based on PC/CAL magnet detection times. Position correction commands received outside this window are ignored.
4. Generates a zero or reduced performance level multiplier, in response to input commands or specified operating conditions, and reduces the internal line speed command accordingly.
5. Limits the internal line speed to specified values during berth moveup and pushing maneuvers.
6. Delays the start of the jerk and acceleration limited command profiles, when starting from rest, by a specified amount to insure proper VCU-motor-brake phasing.
7. Selects a command profile acceleration/deceleration limit based on the current profiled speed command value and the mode of operation in effect.
8. Generates jerk and acceleration limited acceleration and speed command profiles for use during normal operation based on the internal line speed command value after processing by the position update performance level, startup timer, and station stop functions.
9. In response to an emergency stop command, generate jerk and deceleration limited acceleration and speed command profiles for control of closed-loop emergency stopping, starting from the measured speed value in effect at the time of the emergency stop command.
10. Generates an incremental profiled position command during each sampling interval in both normal and emergency modes of operation which is equal to the integral of the jerk and acceleration limited speed command over the sampling interval.

11. Generates a station stop mode disable window based on FSK "Ignore Next Stop Magnet" uplink commands and measured position. Detection of a station stop magnet is ignored whenever the vehicle is within this window, i.e., less than 10 feet  $\pm$  1 foot downstream of the point where it received an "Ignore Next Stop Magnet" uplink command.
12. Computes, following receipt of a station stop command, a position-dependent speed to be used in conjunction with the time dependent command profiles to control station stopping. A unique speed-position profile is used in the event a single berth moveup message is received prior to the station stop command.
13. Generates, when stopped, a negative speed command value with magnitude sufficient to hold the vehicle in place and profile the transition to this negative value (Forced Brake Mode) such that sudden transients in vehicle motion are minimized.
14. Generates a motor on/off command in accordance with specified logic.

#### 3.1.2.1.2 Speed and Position Controller Module

1. Computes speed and position errors based on command and measurement inputs.
2. Generates a single brake/motor torque command which is a weighted sum of the acceleration command and measured speed and position errors.
3. Monitors speed error and generates a fault signal if its magnitude exceeds 2.0 feet per second.
4. Initializes the speed and position errors at the beginning of an emergency stop in accordance with specified logic.

#### 3.1.2.1.3 Odometer Data Processor

The Odometer Data Processor module performs the following functions:

1. Generates an accurate measure of the magnitude of vehicle centerline speed.
2. Generates an accurate measure of vehicle centerline displacement or position.
3. Measures the error in the odometer input signals and generates an accurate calibration factor.
4. Controls the voting of redundant inputs such that safe vehicle operation is ensured and both redundant processors operate on the same values of measured speed and position.
5. Monitors for faults; if a fault is detected, takes the safest reaction.

#### 3.1.2.1.4 Signal Conditioning

The Signal Conditioning Module performs the following functions:

1. Filters the input torque command from the Speed and Position Controller Function and limits the rate of change of the filtered command.
2. Generates scaled motor and brake torque commands from the single point limited torque command and provides biasing and command shaping as required to compensate for motor or brake nonlinearities.
3. Bypasses the torque command rate limiting function if an emergency stop command is in effect.

### 3.1.2.2 Emergency Stop Control

Emergency stopping involves two modes: a closed-loop mode and an open-loop mode. Open-loop emergency stopping is employed only if the safety of the closed-loop mode cannot be assured.

Closed-loop emergency stopping is controlled by the vehicle longitudinal control system and uses the service brake system. Emergency stopping differs from normal operation principally in that commanded brake torque is not rate limited and both jerk and deceleration rates are much higher. Closed-loop control, utilizing fed back measured speed and position, allows application of only the required percentage of available braking force necessary to maintain the commanded deceleration level; this minimizes the possibility of passenger injury due to high deceleration rates.

Upon detection of a condition requiring a closed-loop emergency stop the vehicle longitudinal control system begins a closed-loop mode command sequence within 20 milliseconds. This sequence commands the propulsion system off and initializes generation of the jerk and acceleration limited stopping command profile (starting at the measured speed value in effect when the stop command is received).

If measured speed or position exceeds the commanded value by more than an allowed error margin the vehicle longitudinal control system invokes an open-loop emergency stop. Allowed error margins as a function of time are given in Figure 3.1.2.2-1. The time delay from violation of a closed-loop emergency stop speed or position error threshold to the time an open-loop emergency stop command is actually sent to the brake system will not exceed 0.05 seconds.

In the EDS design, open-loop emergency stops will use the service brake system. The open-loop mode will be jerk and deceleration limited and under control of brake amplifiers which are independent of the VCU. VCU responsibility will be limited to initiating open-loop stops, when required, by interrupting the "Emergency Brake Hold-Off" signal.

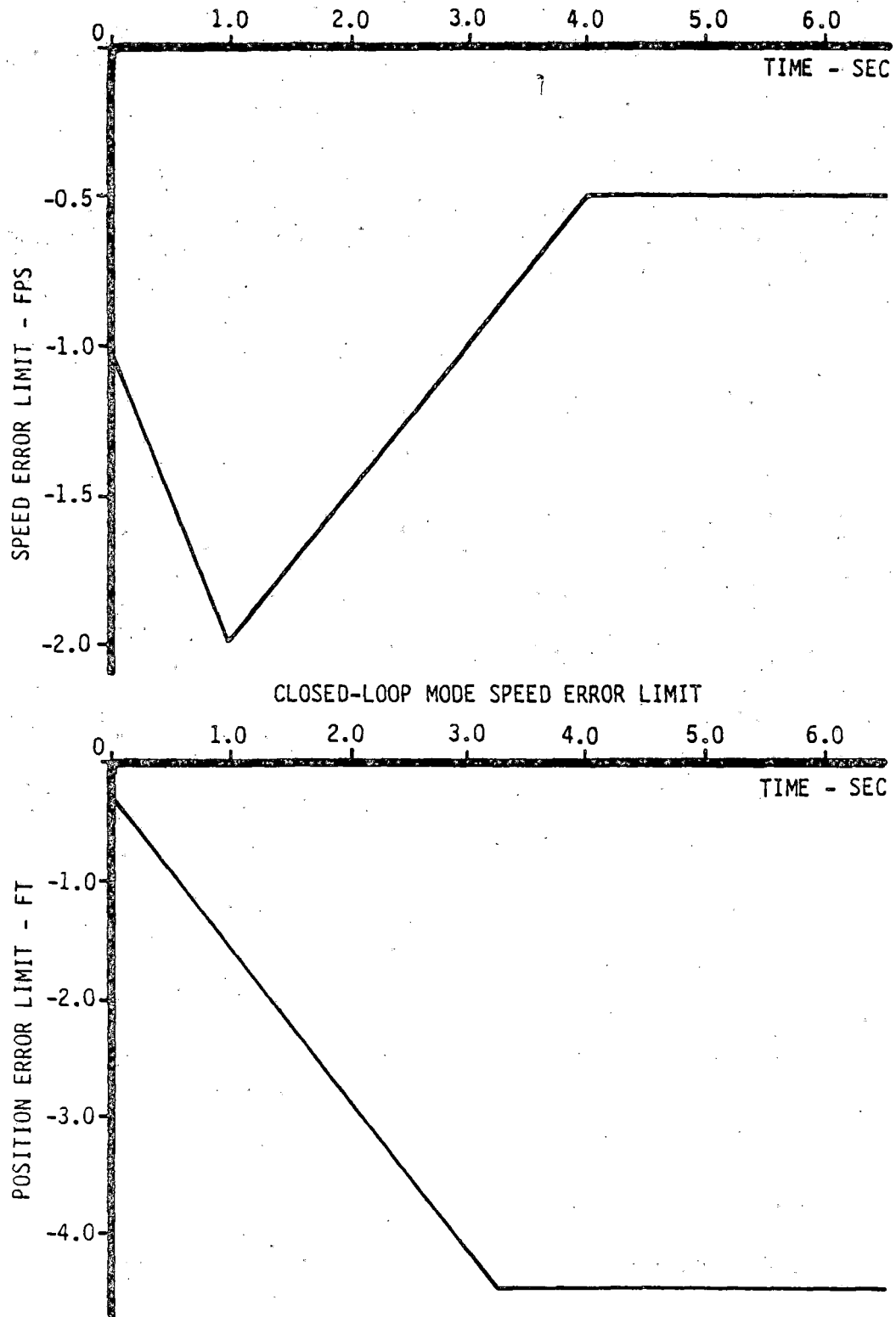


FIGURE 3.1.2.2-1: CLOSED-LOOP MODE EMERGENCY STOP ERROR LIMITS



#### 3.1.2.3 Lateral Control

The EDS vehicle utilizes the same steering subsystem as used on the Morgantown People Mover system and will have a switchable onboard collision avoidance element. The VCU stores a switch direction command (right/left) received via an ID-tagged uplink message or within a 0.5 second window upon entering the FSK loop containing the merge/diverge; this command is transmitted to the steering subsystem upon closure of the "Switch Initiate" reed switch if the profiled speed limit value is less than or equal to 24.5 feet per second. The VCU will not simultaneously command "Switch Left" and "Switch Right" should an internal VCU discrepancy be detected; instead, the last command will be retained. In addition, the VCU will retain the switch direction last commanded during removal of VCU power.

Two signals from the steering subsystem provide status data to the VCU for safety interlocking; the VCU logic performs an "Exclusive-OR" check on these status signals. Only one input must be high at all times to avoid an emergency stop, except that a 1.28 second interval of verification loss will be allowed after the VCU issues a change in the switch direction. The vehicle steering subsystem must complete the switching cycle within this window to preclude an emergency stop.

The vehicle bias direction is transmitted to the Collision Avoidance Subsystem interface after switch verification.

#### 3.1.2.4 Vehicle Exits

The emergency exit is monitored with a single status signal. If the vehicle were moving and the VCU interpreted the status signal as an "exit not closed" an irrevocable normal rate stop is started and a fault message to the wayside via the FSK downlink is initiated.

Three signal lines from each of the left and right service doors provide door status data for safety interlocks and for status downlinks. One control line to each door controller provides control capability.

### 3.1.3 Safety Assurance Tasks

Safety assurance is that portion of the VCU operation that is directly involved with the safety of passengers and the vehicle. The principal safety assurance tasks are collision avoidance, overspeed protection, loss of safe-to-proceed detection, disparity checking, and vehicle status monitoring.

Failure of a particular safety assurance test inevitably leads to shut down of the propulsion system and stopping of the vehicle. Four stopping modes are available to the VCU; Reversible Normal Rate Stop, Irrevocable Normal Rate Stop, Closed-Loop Emergency Stop, and Open-Loop Emergency Stop.

Detected safety violations or the presence of unsafe vehicle conditions will normally lead to either an irrevocable normal rate stop or a closed-loop emergency stop. Open-loop emergency stopping is invoked only upon failure of an element that could prevent successful application of closed-loop braking.

#### 3.1.3.1 Vehicle Collision Avoidance

The VCU furnishes calibrated odometer data and vehicle steering bias direction data to the Odometer Data Downlink Collision Avoidance System (ODDCAS) onboard electronics. This data is carried on two identical channels utilizing physically separate connectors and cables.

#### 3.1.3.2 Wayside/Vehicle Safe To Proceed Signal

The uplink FSK data clock constitutes a "Safe-to-Proceed" signal to the VCU. Loss of this FSK signal energy for more than 0.030 seconds will be interpreted as "loss of safe-to-proceed" and will initiate an irrevocable closed-loop emergency stop within 0.050 seconds of the initial loss of the FSK signal energy.

#### 3.1.3.3 Overspeed Protection

Vehicle overspeed protection is accomplished by comparing the measured speed with a wayside derived speed limit. Violation of the speed limit results in a closed-loop emergency stop.

Each FSK loop continuously transmits a speed limit command as well as a line speed command. The speed limit command is hardwired in the guideway communications equipment and represents the maximum safe speed under worst case conditions at a particular loop location. Commanded line speed will vary depending upon system demands; the highest line speed in any loop will be 2.5 feet per second lower than the speed limit.

In a transition to a loop with a higher speed limit, the new limit is enacted immediately after the first valid FSK message received by the forward receive antenna. In contrast, after entering a loop with a lower speed limit the old speed limit is maintained a fixed time interval, depending only upon the new and old commanded speed limit values. Transition to the new speed limit occurs with the same acceleration limit imposed on the jerk and acceleration limited line speed command. These two speed limit transition modes are illustrated in Figure 3.1.3.3-1.

#### 3.1.3.4 Master Clock Supervision

The Main Processors of both VCU channels utilize 10 millisecond interrupt pulses generated by a single master clock and divider chain. The master clock frequency is maintained within  $\pm 0.0054\%$ , 0.997 probability, of nominal. A master clock frequency error of greater than  $\pm 0.02\%$  will result in open loop emergency stopping.

#### 3.1.3.5 Status Monitoring

The VCU monitors vehicle operations to detect equipment failure and notifies the Guideway Command and Control Subsystem (GCCS) of a failure via FSK downlinks. Failures that threaten the safety of the vehicle or passengers result in an emergency stop.

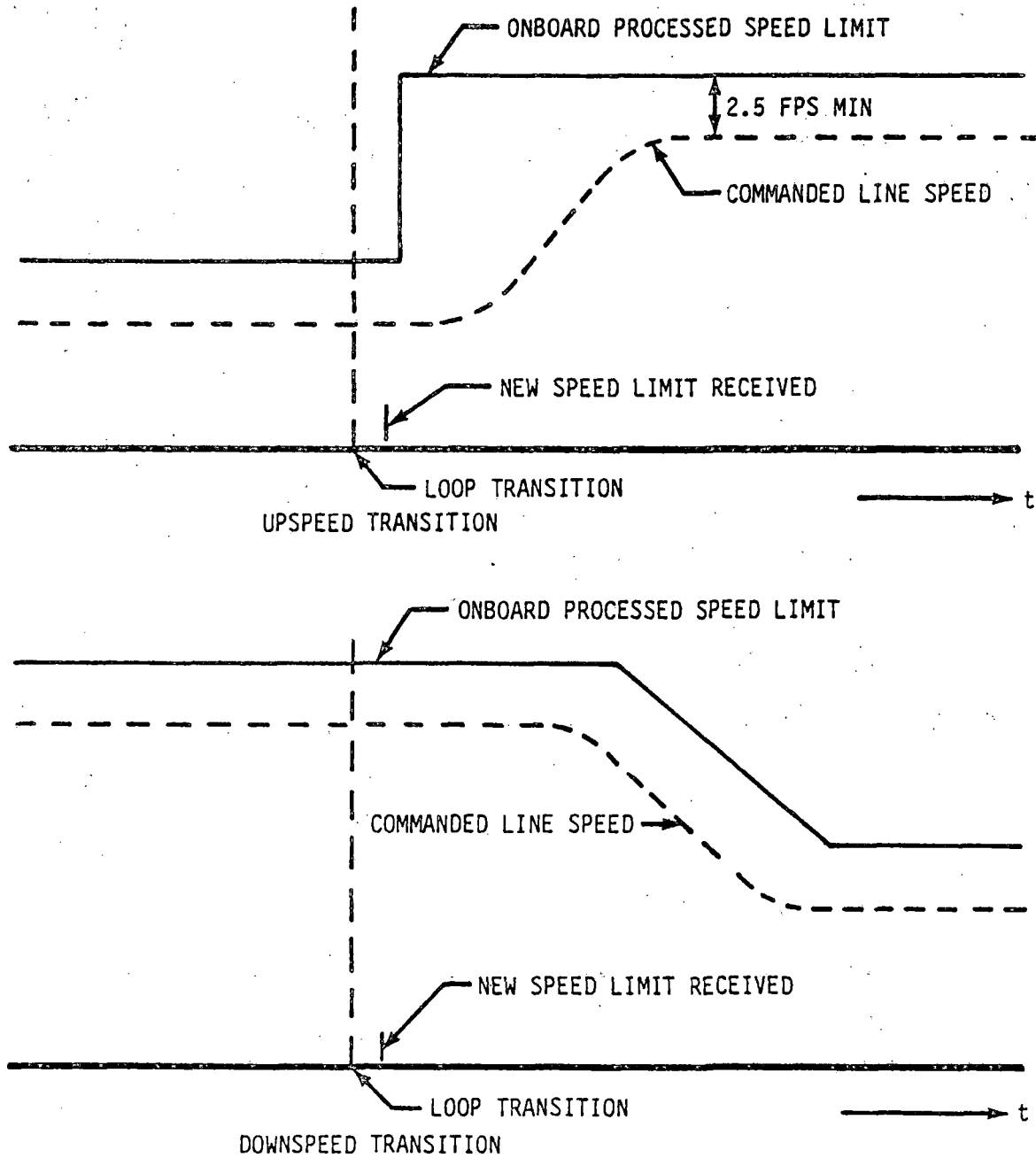


FIGURE 3.1.3.3-1: VEHICLE SPEED LIMIT PROFILES

The following vehicle systems are monitored by the VCU:

#### Brake System

The hydraulic pressure of the brake calipers downstream of both servo valves is monitored with pressure transducers in order to estimate applied braking torque. This measured value is transmitted to the VCU in analog form where the VCU converts it to a digital word with eight bits of resolution.

Switches associated with each hydraulic accumulator provide a discrete signal warning of a pending loss of brake (and switching) capability.

A thermal switch located at the hydraulic line between the reservoir and the pump indicates excessive hydraulic fluid temperature.

One brake pad has a temperature activated switch to warn of overheating and possible brake fading.

#### Propulsion System

The propulsion system provides the VCU, at the Propulsion Torque Command and Data Conversion Unit (PTCDCU), an analog measurement of propulsion torque. This value is converted to a digital word of eight bits resolution which is transmitted to the VCU along with other propulsion discrete status signals.

#### Vehicle Electronics Power

The battery/battery charger voltage is converted to a digital word with eight bits resolution and monitored by the Main Processor to detect over/under charging conditions.

## Suspension System

The vehicle pneumatic suspension system incorporates a pair of series connected, normally-closed pressure actuated switches. These switches (one forward and one aft) open when the suspension system, attempting to maintain a preset floor height, develops a pressure which exceeds a threshold based upon maximum allowable passenger loading. The VCU monitors this discrete to detect a vehicle overload condition.

### 3.2 VCU Safety Considerations

#### 3.2.1 Safety Design Philosophy

The AGRT control hierarchy allocates command and 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 "fail-safe" electro-mechanical vital elements due to inherent limitations of such devices. Instead, the VCU design solution relies heavily on microelectronics to achieve the required reliable performance within reasonable volume, weight, and power limitations. The use of microprocessor hardware (and associated software) was mandated by the developmental nature of the program and the need to further reduce parts count over a discrete (SSI, MSI) logic implementation.

Use of these high technology devices raised several important issues in the areas of safety design specification and evaluation. Whereas the traditional safety approach using "fail-safe" vital elements relies

heavily upon historical precedent, simplicity, and a few physical properties, high technology devices have neither a legacy nor the simplicity required to permit exhaustive analysis.

### 3.2.2 Safety Design Approach

The approach to Vehicle Control Unit safety began with the processes normally applied to aircraft and military systems development within the aerospace industry. This approach considers hazard identification, safety item reviews, and quantitative analyses to provide safety requirements and assessments during the design, development, test, and evaluation phases of the program. Specific tools are used, including Failure Modes and Effects Analyses, Worst Case Analyses, Fault Tree Analyses, Sneak Circuit Analyses, etc.

It became obvious early in the design phase that the accepted aerospace approach to safety was somewhat different than normal rail transit practices. Subsequent discussions between Boeing project personnel and the UMTA Protect Team established the basic design and evaluation criteria. Although this approach recognized the use of checked redundancy, the evaluation criterion was tied to traditional vital elements: any device or element performing a safety critical function must be as safe as a vital relay. The final design would be rated in terms of the safety of an equivalent vital relay design.

Such a qualitative criterion was considered inappropriate, however, and it was decided to apply the quantitative aerospace evaluation methods to certain safety critical portions of the design. Recognizing that eventually there would be a need to correlate the two evaluation methods, a search was initiated for vital relay failure data. After much discussion with UMTA, consultants, and the transit industry, it was concluded that the Mean Time Between Unsafe Failure (MTBUF) of an Association of American Railroads (AAR) vital relay is thought to be on the order of one million years. Although solid state devices are extremely reliable, not even a simple semiconductor diode can boast a million year MTBF. It was obvious that single thread micro-



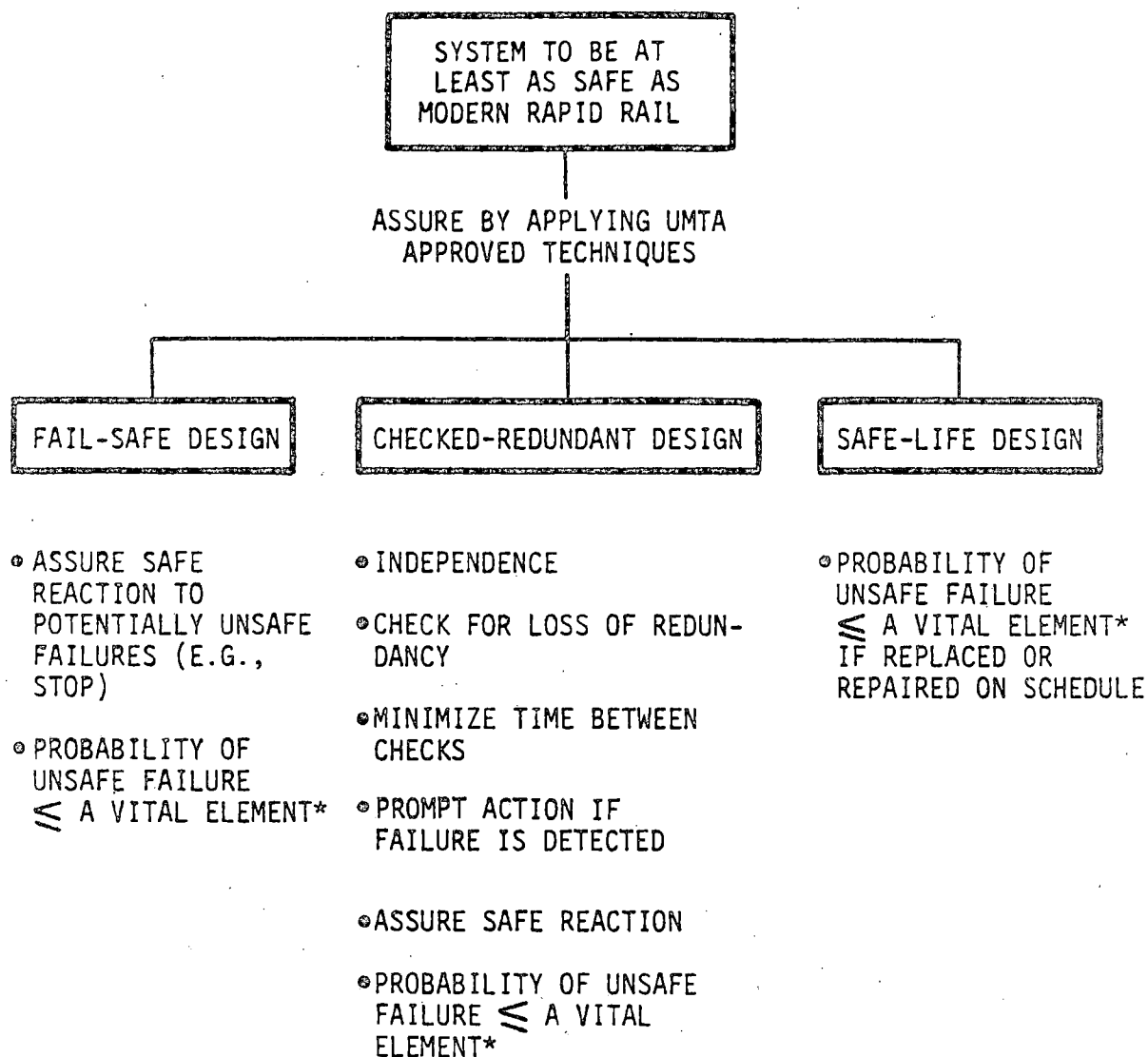
electronic implementations were simply not acceptable under AGRT program ground-rules.

### 3.2.3 Safety Principles

Further discussions with The UMTA Project Team resulted in three basic safety principles as shown in Figure 3.2.3-1: Fail-Safe, Checked Redundant, and Safe Life. In essence, these principles were the three options available for the VCU design.

Fail-safe components consist of a class of vital elements that rely on physical properties such that failure modes can be absolutely analyzed; at least one failure mode is thought to be so improbable that it is considered for practical purposes to be zero. Typical of the physical principles are: brass cannot become magnetic, pressure cannot become a vacuum, gravity is always present, etc. The Association of American Railroads "safety relay" (vital relay) is a fail-safe device; remove the coil's electrical excitation and the force generated by gravitational acceleration will always release the armature and open the front contact. If the relay has been correctly applied in the overall system, any plausible failure of the device will result in a condition known to be safe. (Of course, the relay must be installed and operated in the correct physical orientation, the case must be kept free of foreign objects and insects, the contacts must be maintained in adjustment, and the pivots must be kept lubricated. Finally, inadvertent opening of the front contact-the high probability failure-must result in a safe condition.)

Checked Redundant designs use combinations of elements having "high probability" failure modes such that the overall probability of an unsafe condition is reduced to an acceptable value. In this manner, two channels, each having a low MTBF, can be combined to achieve a high MTBF. The two channels must be independent, however, and malfunctions must be detected and corrected promptly. In a dual redundant implementation, any malfunction effectively reduces the controller to a single channel; unless each channel is itself failsafe, the fault



\* ONE OF "A SET OF ELEMENTS WHICH HAVE AT LEAST ONE MODE OF FAILURE WHOSE PROBABILITY OF OCCURRENCE IS SO SMALL THAT FOR PRACTICAL PURPOSES IT IS CONSIDERED TO BE ZERO." THE AAR SAFETY RELAY IS AN EXAMPLE OF A VITAL ELEMENT, AND IT IS BELIEVED THAT ITS MTBUF IS ABOUT  $10^6$  YEARS.

THE BOEING GOAL FOR A VITAL ELEMENT IS:

A VITAL ELEMENT PERFORMING A SAFETY CRITICAL FUNCTION SHALL HAVE AN MTBUF OF NO LESS THAN  $10^6$  YEARS WHEN THE ELEMENT IS OPERATED IN A SPECIFIC MANNER IN A SPECIFIC OPERATING ENVIRONMENT.

FIGURE 3.2.3-1: SAFETY DESIGN PRINCIPLES EVOLVED DURING AGRT PROGRAM

reaction required by the design should be to a state known to be safe - such as the application of emergency brakes.

Safe Life designs typically deal with structures. The designer considers the loads encountered during worst-case operation and sizes the various structural members to accommodate the operating stress and number of stress cycles over the design lifetime. The application remains safe if the member is replaced or repaired on a predetermined schedule.

#### 3.2.4 VCU Safety Implementation

As noted earlier, a microprocessor based implementation was chosen for a variety of reasons. A review of available design options indicated that a checked redundant configuration was the correct decision. Micro-electronic devices are neither fail-safe nor safe life.

The final Vehicle Control Unit design is checked redundant in both the hardware and the software. The two hardware channels are basically identical, while the software design employs dissimilar algorithms to detect hardware failures and embedded software errors. Figure 3.2.4-1 illustrates the hardware redundancy, while Figure 3.2.4-2 shows the dissimilar software structure.

Although the VCU performs many complex functions, its basic architecture was kept deliberately simple. In the main processor, for example, all applications algorithms are called by a cyclic executive. A hardware clock provides basic time-keeping for the executive. This simple architecture is easily understood and eases proof-of-correctness analyses.

Internal checks provide integrity for hardware and software processes. Redundant watch-dog timers monitor clock accuracy and provide protection against processor insanity or program looping. Initialization checks, background checks, traps, and emergency code exercisers provide protection against subtle processor or memory failures. Other checks provide protection against invalid data, register overflow, and truncation

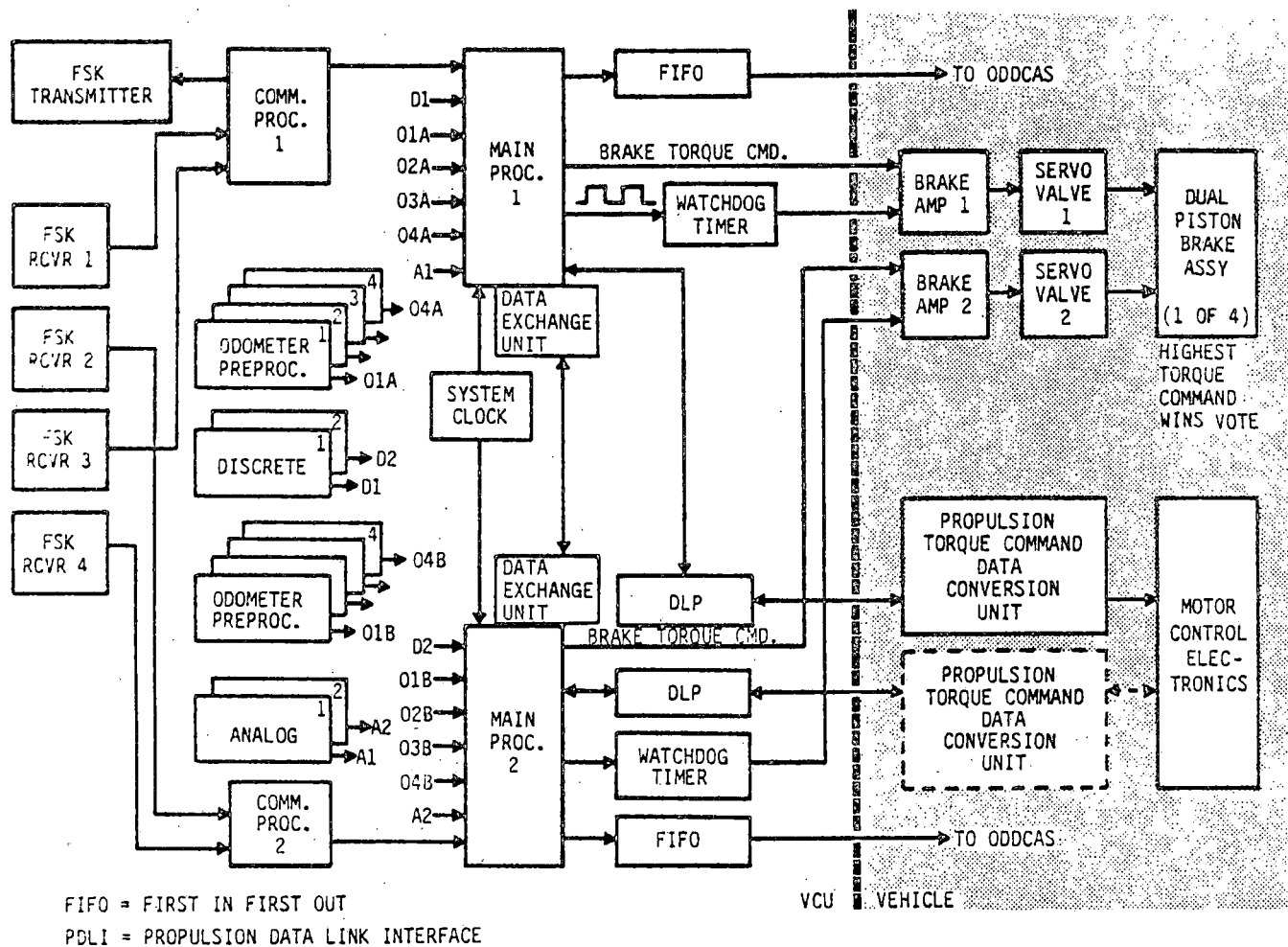


FIGURE 3.2.4-1: CHECKED DUAL REDUNDANT VCU

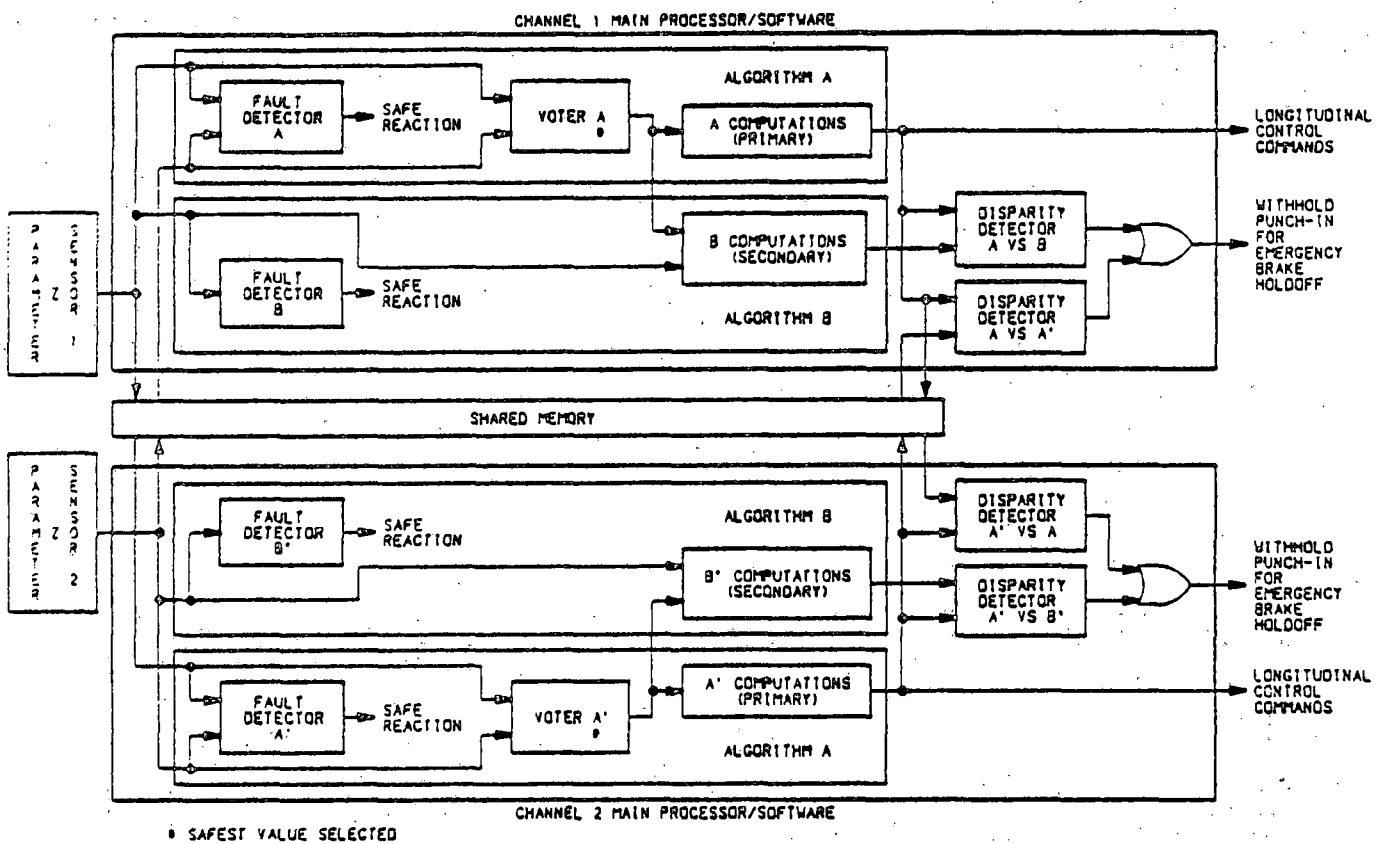


FIGURE 3.2.4-2: SYMMETRICAL DUAL-DISSIMILAR SOFTWARE WITH REDUNDANT SOFTWARE DISPARITY CHECK LOGIC

error. Data consistency checks compare data from sample to sample and sensor data to command data. An intricate punch-in key is used to ensure a safe reaction for various combinations of processor failure.

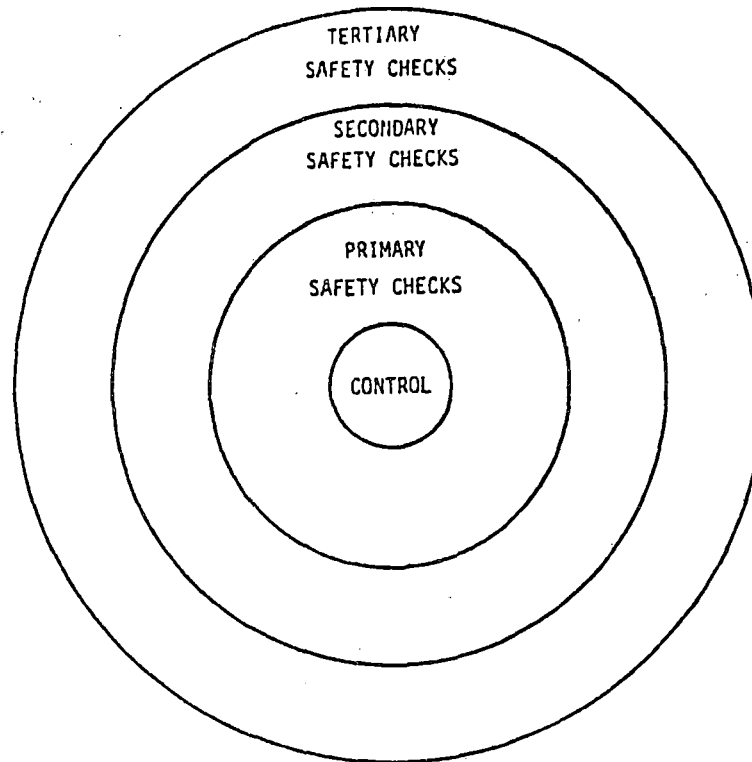
All of these techniques are aimed at detecting malfunctions (failures or errors) that could adversely affect the execution of the basic control and safety algorithms. The design provides three layers of protection to these basic algorithms; this is referred to as the "Onion Skin" approach to safety. Each layer provides safety checks that are themselves checked by the next outer layer. Figure 3.2.4-3 illustrates the "Onion Skin" safety hierarchy with examples of the primary, secondary, and tertiary checks.

Throughout the hardware and software design process, state-of-the-art tools and techniques were used to assure a high quality product. Modular design practices minimized the interaction (coupling) of unrelated functions. Top-down design assured a cohesive, consistent architecture. The use of a Program Design Language provided consistency checks and allowed project personnel without strong software backgrounds to participate in peer code reviews. The use of a Higher Order Language (HOL) minimized coding errors and provided additional consistency checks.

The use of hardware breadboards and a software simulator provided checks of hardware subassemblies and individual software modules. Initially, a single channel of hardware was integrated with the primary software algorithms. After a series of closed-loop test runs using a vehicle simulator, the redundant hardware channel and dissimilar software were integrated, and the test series was repeated. Although an abbreviated test program cannot be construed as a qualification or type approval test, it did provide a high degree of confidence in the design.

### 3.2.5 Safety Trades

The approach used assures that safety is implemented in a design in the same manner as performance, reliability, maintainability, quality, or



THE "ONION SKIN" APPROACH

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

<ul style="list-style-type: none"> <li>(S/W: data format anomaly control)</li> <li>invalid data control</li> <li>register overflow checks</li> <li>truncation error control</li> <li>range checks</li> </ul>	<ul style="list-style-type: none"> <li>(H/W: vehicle status anomaly checks)</li> <li>brake pressure checks</li> <li>motor torque checks</li> <li>hydraulic pressure checks</li> <li>voltage checks</li> <li>X-channel sensor disparity control</li> </ul>
--	---
- o SECONDARY SAFETY CHECKS:
 

<ul style="list-style-type: none"> <li>(S/W: data consistency checks)</li> <li>odometer cross checks</li> <li>data rate of change checks</li> <li>motion profile control</li> <li>cumulative error control</li> </ul>	<ul style="list-style-type: none"> <li>(H/W: microprocessor checks)</li> <li>control flags check</li> <li>CPU registers check</li> <li>RAM and Rom checks</li> <li>dynamic exercising of emergency code</li> </ul>
---	--
- o TERTIARY SAFETY CHECKS:
 

<ul style="list-style-type: none"> <li>(S/W: redundant software)</li> <li>A-B algorithm checks</li> </ul>	<ul style="list-style-type: none"> <li>(H/W: redundant hardware)</li> <li>A-A algorithm checks "punch-in" key</li> </ul>
---	--

FIGURE 3.2.4-3: SAFETY HEIRARCHY

any other system characteristic. Safety is not an added feature achieved with a few special components; in fact, it often interacts with other system characteristics. For example, safety and availability requirements actually drive the design in opposite directions. Safety features also heavily influence deployment and life cycle costs.

In the case of the VCU, operational safety was always a prime consideration in design decisions. Elsewhere in this report, various VCU safety features are described in detail concluding that the final design is technically sound in addition to meeting the AGRT ground-rules.

In reviewing this report, the reader should consider that extraordinary circumstances terminated efforts on reliability enhancement and anomaly management early in the program to reduce development costs. The design could differ somewhat if safety had been more extensively traded against availability, reliability, cost, and system performance.

Section 6.2 of this report contains specific conclusions regarding the safety design process and efforts, and offers recommendations for future transit control electronics.

### 3.3 Hardware Architecture

#### 3.3.1 General Description

Figure 3.3.1-1 is a block diagram of the Vehicle Command and Control Subsystem (VCCS). The VCCS is the electronics package carried onboard an Advanced Group Rapid Transit (AGRT) vehicle which performs the command and control function. The VCCS is made up of two distinct parts: the onboard portion of the Odometer Data Downlink Collision Avoidance System (ODDCAS) and the Vehicle Control Unit (VCU). The VCU includes the Vehicle Control Electronics (VCE), the inductive communications loop antennas and feedlines, the reed switch assemblies and the presence detection magnet.



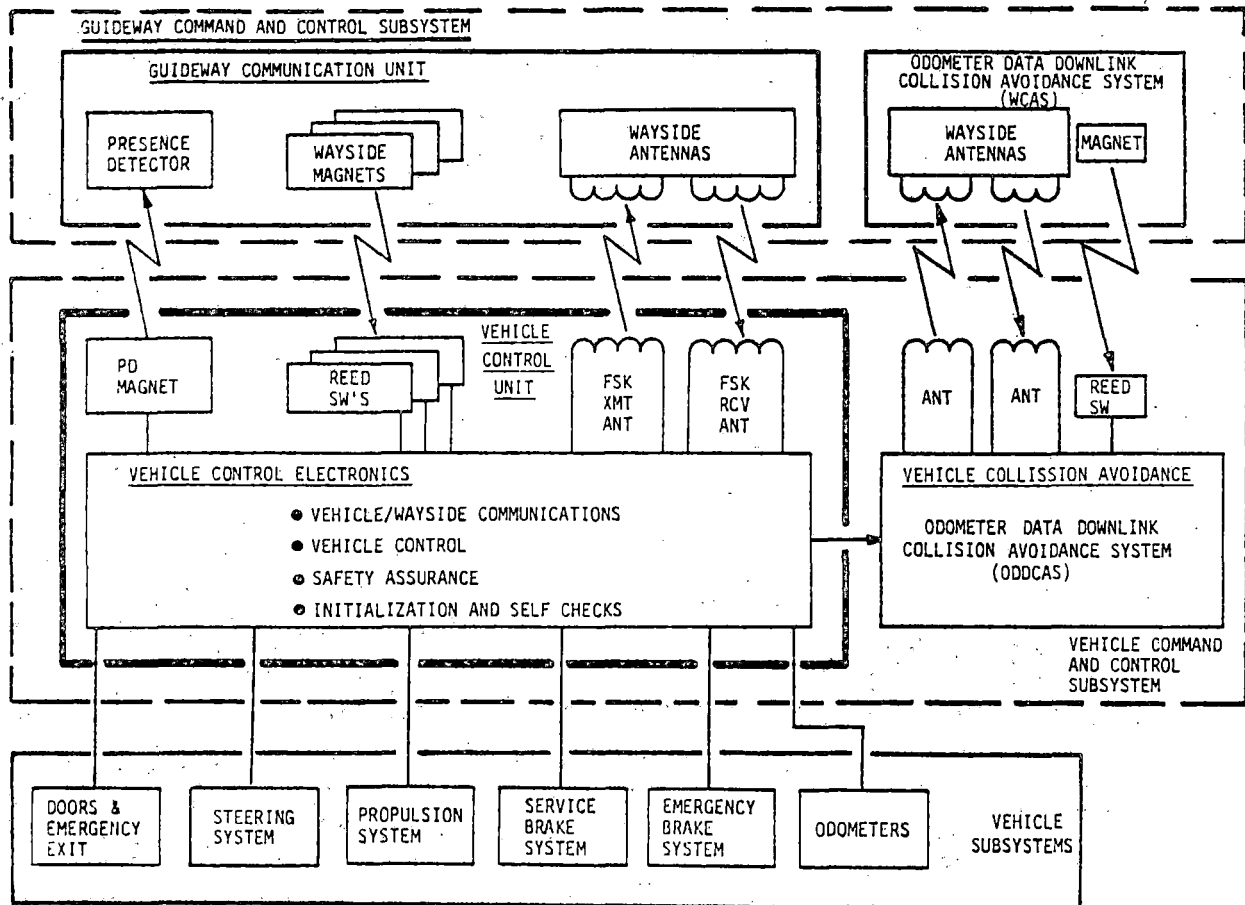


FIGURE 3.3.1-1: VEHICLE COMMAND AND CONTROL BLOCK DIAGRAM

The VCU is responsible for the operation and safety of the vehicle. Vehicle operation involves implementation of wayside commands conveyed to the VCU by inductive communications and magnetic signalling. On the basis of these commands, and in accordance with vehicle status measurements, the VCU controls longitudinal motion (jerk, acceleration, speed and position), switching, closed-loop emergency stopping, and vehicle doors. Safety assurance tasks include odometer data output, overspeed protection, emergency removal of tractive effort, door control, status monitoring, fault protection, and system initialization. The VCU provides conditioned odometer data to the ODDCAS Onboard unit. This data, consisting of measured vehicle speed and incremental position, is then downlinked via the ODDCAS Onboard Unit to an ODDCAS Wayside Unit which implements a variable length, moving block collision avoidance system.

Still referring to Figure 3.3.1-1 the VCU includes the Vehicle Control Electronics (VCE), the inductive communications loop antennas and feed-lines, the reed switch assemblies and the presence detection magnet. The VCE includes the processors with their associated support circuits and the FSK transmitter and receivers.

The VCE contains the intelligence of the VCU. Processors, utilizing instructions stored in Read Only Memory (ROM), analyze data sent from sensors and circuits throughout the vehicle and make decisions; resulting control commands are then transmitted to appropriate vehicle control elements.

The principal interfaces for the VCE are shown in Figure 3.3.1-2 . Discrete signals include the on/off levels produced by various relay contacts and limit switches, the magnetic communications reed switch closures and output control relay contact closures. The commanded brake caliper pressure signal, measured brake caliper pressure, and the prime power voltage level are analog signals. Pulse train signals include the wheel mounted odometer pulses and the FSK antenna signals.

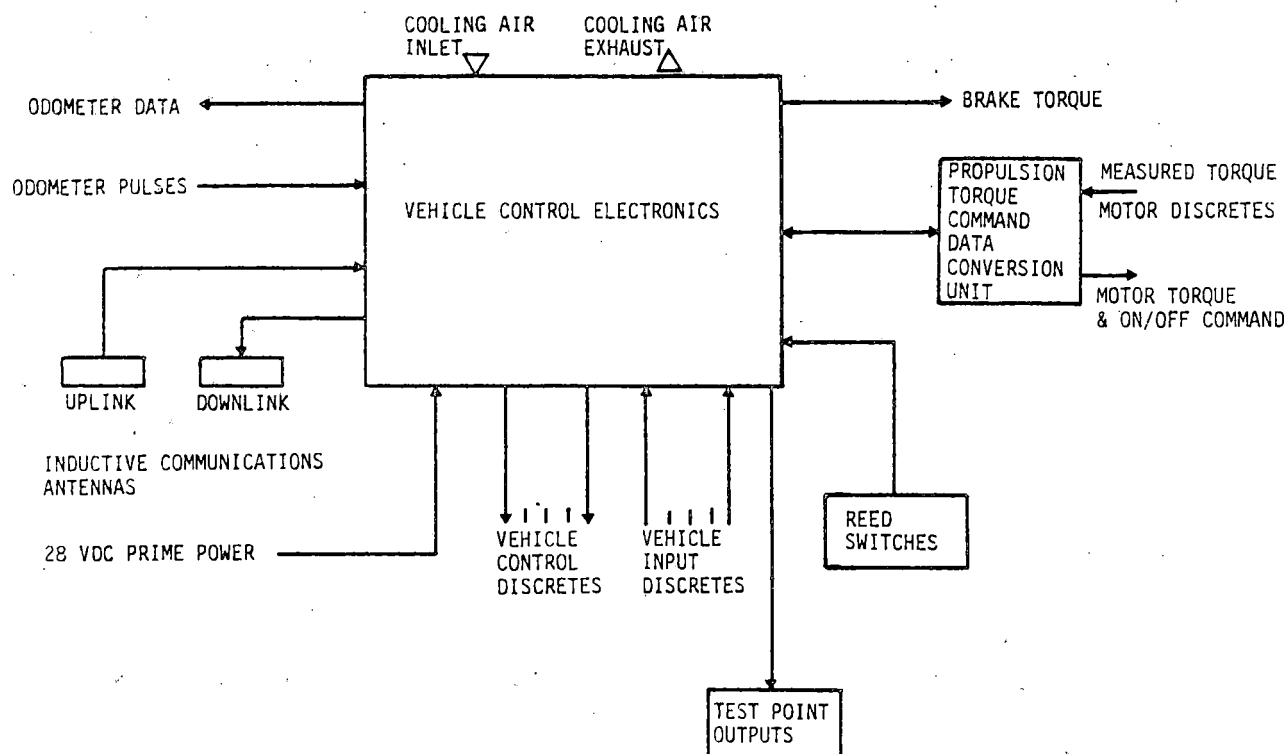


FIGURE 3.3.1-2: VEHICLE CONTROL ELECTRONICS INTERFACES

Signals involving the propulsion unit are carried between the VCE and a separate interface unit, the Propulsion Torque Command and Data Conversion Unit (PTCDCU), in asynchronous serial format over a fiber optic cable. The PTCDCU circuitry delivers an analog torque command signal and an on/off command to the propulsion subsystem and processes the analog measured torque and discrete propulsion status signals for transmission back to the VCE processor.

### 3.3.2 Hardware Safety Implementation

As previously stated, a major requirement in the design of the VCU is safety. The AGRT system is required to have an ultimate operational safety goal equivalent to or better than modern rapid rail systems. To achieve this safety goal, failsafe design principles are applied throughout the design. Failsafe design guarantees that any malfunction affecting safety will cause the system to revert to a safe state. To achieve this failsafe design, "fail-safe" (as differentiated from "failsafe") and checked redundant implementations are used. These implementations are defined below.

**Fail-Safe:** A single thread implementation which takes advantage of intrinsic physical properties of its elements or of failure modes where probabilities of occurrence are so small that they are considered to be negligible. In the AGRT program "negligible probability" has been taken as "one in a million years".

**Checked Redundancy:** An implementation which makes use of two or more independent paths having no common mode or correlated failures for performing the same function. Each independent path may individually exhibit high-probability, unsafe failure modes. However, each path is checked, either continuously or periodically, such that the probability of undetected unsafe failures of the checked combination is negligible.

Appropriate use of these design techniques enables the VCU to meet the AGRT safety goal.

### 3.3.3 Internal Configuration

The processing functions the VCU must perform are divided into two categories. The first is the handling of the received uplink and transmitted downlink FSK messages. The second is the control function of the VCU. Each type of function is handled by a separate 16-bit microprocessor system. Referring to Figure 3.3.3-1, the FSK functions are handled by a processor named the Communications Processor; it performs the formatting, error checking, and serial/parallel data conversion of the uplink and downlink FSK messages. The remaining control functions are handled by a second 16-bit processor named the Main Processor. The Main Processor is cyclic in operation, and performs its functions at regular intervals, regardless of the occurrence of external events. In contrast, the Communications Processor is event driven, since it must respond to FSK transmissions from the wayside and provide FSK transmission to the wayside when told to do so.

Data is passed back and forth between the Main Processor and the Communications Processor via a shared random access memory (RAM). 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. Memory access arbitration logic and a system of status flags allow conflict-free data transfer between the two mutually asynchronous systems. The size of this shared RAM is 1024 16-bit words. (In computer language a piece of data that is 16-bits wide is referred to as a word, 8-bits wide is called a byte, and 4-bits wide is called a nibble.)

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.

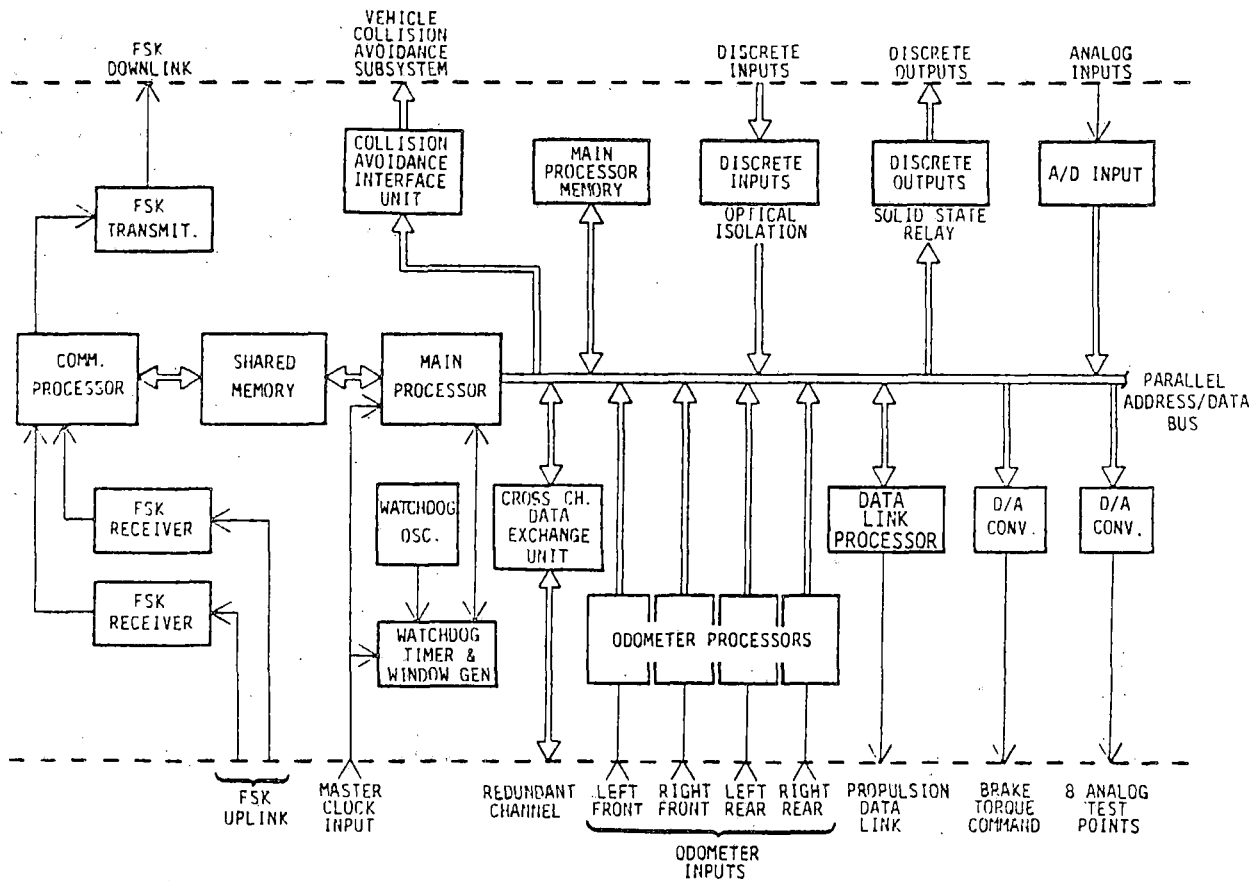


FIGURE 3.3.3-1: SIMPLIFIED BLOCK DIAGRAM OF VCU ELECTRONICS

In order to reduce the conduction of common mode electromagnetic noise into the VCE enclosure, most I/O lines are isolated either optically or magnetically. Discrete and pulse train inputs are coupled to input data latches through opto-isolator units. Output control discretes are relay closures and isolation is achieved via solid state relays using optical or magnetic means. Signals both to and from the propulsion subsystem are carried over fiber optic cable, a dielectric. This provides essentially infinite common mode signal rejection. Filtered connectors and internal packaging of I/O circuitry away from processing logic provide additional isolation for metallic interfaces.

Timing for the system is provided by a single master clock which is continually being checked by a watchdog clock. Any failure of either the master or watchdog clock will cause the system to react in a safe manner.

Protection against failures that might lead to unintended software halts or loops is provided by the hardware watchdog timers associated with the main processor. Correct operation of the software program provides for periodic issuing of a pulse that must be within a window generated by the watchdog circuit. If the pulse is absent or falls outside the window, the transmission of a hold-off signal to the emergency brake circuit is withheld. To meet the safety goals previously discussed, the complete VCE contains two identical channels (see Figure 3.3.3-2) with the exception that a single FSK transmitter and a single master clock circuit are used for both channels. Communication between the two channels occurs via a unique channel to channel Data Exchange Unit (DEU). Additional discussion of this unit is available in section 3.3.3.2 and a detailed discussion in section 4.2.1.2.

It should be noted here that in the past the channel to channel DEU has been referred to as a cross channel shared memory. The name cross channel shared memory is a term that very often causes undue concern when discussed. The name is not a proper description of the electrical processes being performed, therefore, for clarity a more accurate descriptive name is being used in this document.

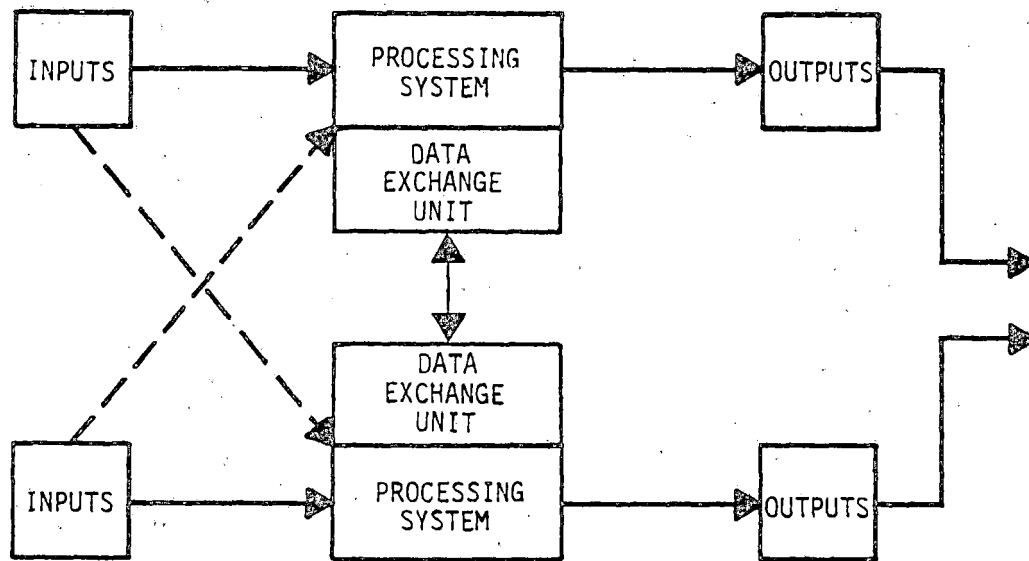


FIGURE 3.3.3-2: BASIC VEHICLE CONTROL UNIT CONFIGURATION



#### 3.3.3.1 Dual Redundancy Configuration

The Vehicle Control Electronics are configured in a dually redundant fashion as shown in Figure 3.3.3.1-1. The philosophy from which the dually redundant design evolved is contained in section 3.2, VCU Safety Considerations.

The hardware is configured as two identical channels. The electronic cards are directly interchangeable between channels. The only electrical difference is a single backplane connection in each channel that designates which channel is prime.

Referring to Figure 3.3.3.1-1, The FSK uplink signals are recovered as serial digital data and input to the Communication Processors. Each Main Processor independently processes the various sensor input data and generates appropriate control commands. Certain computations in each channel are monitored by the other channel in order to detect disparities between the two channels.

#### 3.3.3.2 Channel to Channel Data Exchange Unit

Communication between the two Main Processors, necessary for the cross checking of computations, signal checking, and mutual sanity checking, is provided by a channel to channel Data Exchange Unit (DEU). Each channel's DEU has a 1k word memory circuit that can be read from and written into by its own Main Processor when the proper conditions are met.

The DEU's memory circuit is configured as a dual ported memory in which one port is connected to its local Main Processor's data bus through isolation amplifiers and the other port is connected across to the redundant channel with isolation amplifiers on each side of the interface. In this manner the other Main Processor is only allowed to read data from the cross channel DEU when the proper conditions have been met. In other words, data may travel only one way from the memory of a DEU

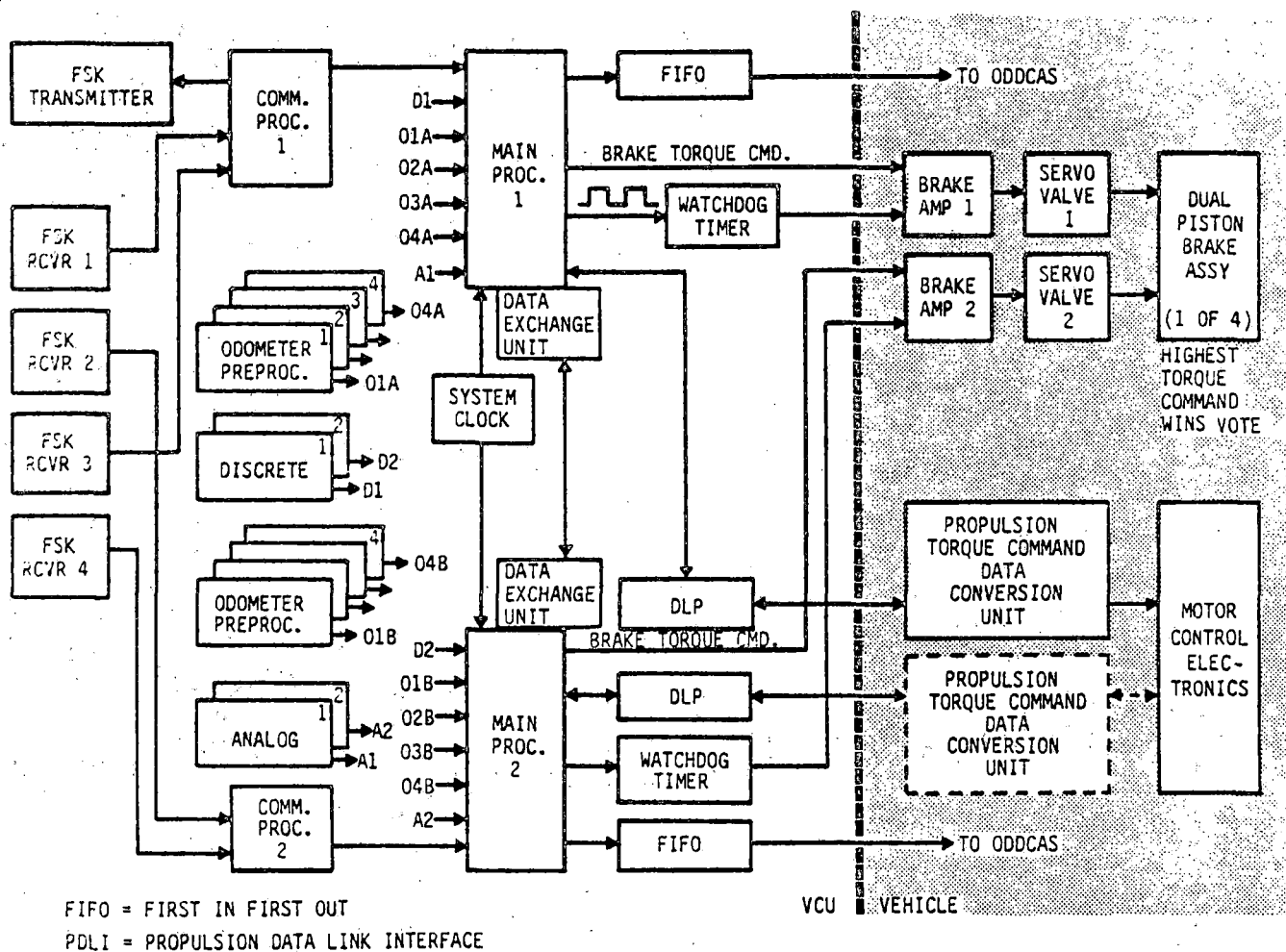


FIGURE 3.3.3.1-1: CHECKED DUAL REDUNDANT VCU

across to the Main Processor of the other channel. Arbitration logic in each DEU reconciles any conflicts between the two units. This method employed in exchanging data between the two channels solves a somewhat difficult problem in a fast, efficient, and safe manner. A Failure Modes and Effects Analysis (FMEA) was performed, and the analysis showed that all failures were detected promptly and result in a safe reaction.

#### 3.3.3.3 System Clock

In order to maintain the AGRT short headway system the cross checked functions must be checked at precise time intervals so the VCU design requires a synchronous operation between the Main Processors. This design allows the redundant systems to make sequential calculations and perform disparity checking on each other's data in a close coupled, synchronized manner. Also, the integrity of certain calculations using sensor input data requires the clock frequency to be maintained within a close tolerance of its specified frequency. The system provides inputs from a single clock to each channel, detects frequency out-of-tolerance conditions and hardware failures in the timing and checking circuits, and initiates safe responses when such a condition occurs.

There are three accepted ways of achieving synchronization in redundant systems - independent accurate clocks, a common external reference, and mutual feedback. The use of a common external reference is currently the most widely used technique but suffers from vulnerability to common point failures. The method chosen for the VCU is the common external reference technique, which is applicable in systems where a common point failure is tolerable if the failure is detected and responded to in a fail-safe manner.

Figure 3.3.3.3-1 is a simplified block diagram of the timing system used in the VCU. Two signals are provided to each channel from the master oscillator circuit. The signals are a 4 MHz clock signal that stimulates the Main Processor and a 100 Hz signal that provides an interrupt to each Main Processor every 10 milliseconds.

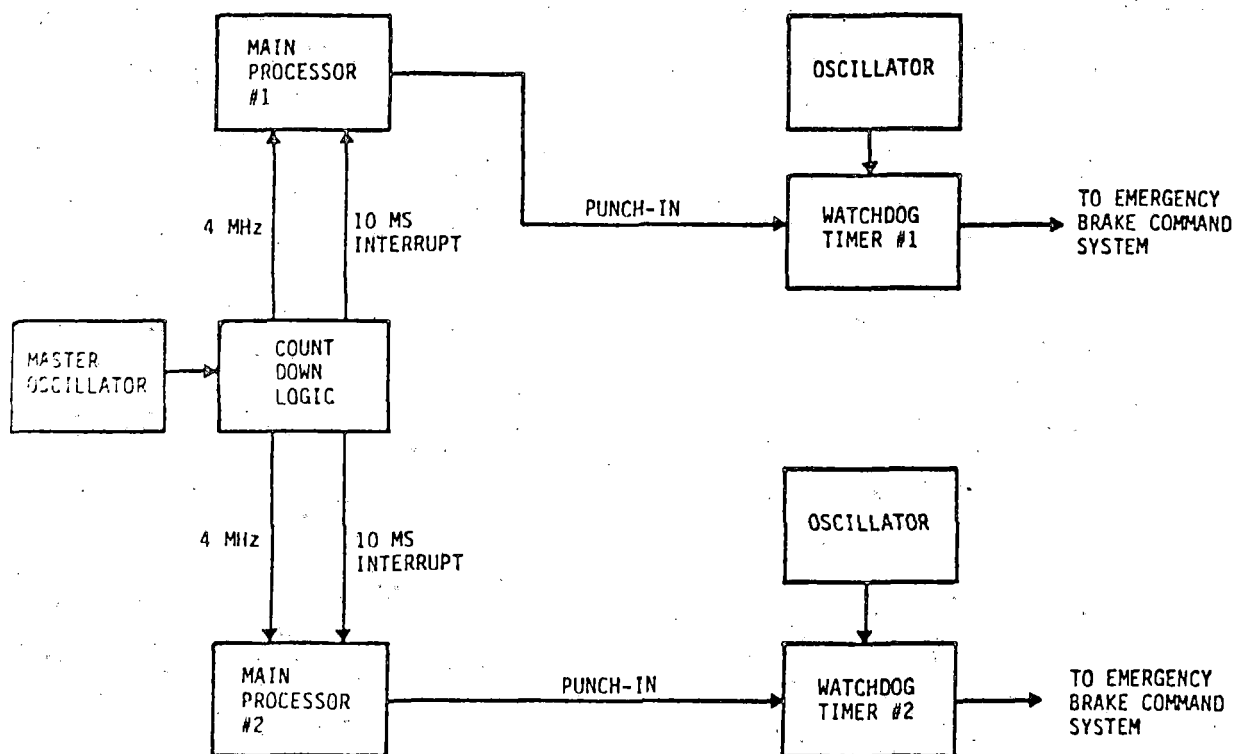


FIGURE 3.3.3.3-1: TIMING BLOCK DIAGRAM

Each channel has an oscillator of the same accuracy as the master oscillator; from this, each channel generates a narrow window every 40 milliseconds. Now each Main Processor must provide a pulse within this window every 40 milliseconds or the system is declared in error and an emergency stop is initiated. This pulse is called the Punch-In pulse. In this manner either Main Processor can initiate an emergency stop by withholding Punch-In pulses; likewise, an emergency stop is initiated if any oscillator drifts out-of-tolerance such that Punch-In pulses fall outside the window.

Figure 3.3.3.3-2 is a diagram of the 4 MHz clock distribution to the microprocessors in the dual channel VCU. As shown on the diagram, a 4 MHz clock signal is used by Main Processor 1 and the 4 MHz inverted (complemented) is used by Communications Processor 1. The Main Processor in channel 2 uses the inverted clock and the Communications Processor uses the non-inverted clock. The use of an inverted and non-inverted clock simplifies the design of the arbitration logic for data exchanges between the Main and Communications Processors and between the two Main Processors. In this manner, when processors are exchanging data, one processor is always leading the other by 125 nanoseconds. In the execution of instructions, the lead or lag of 125 nanoseconds is of no consequence.

#### 3.3.4 External Interfaces

Referring to a figure from a previous section, Figure 3.3.1-1, the Vehicle Command and Control System Block Diagram shows the VCU interfaces. As shown on the diagram the VCU interfaces with the Guideway Communications Unit (GCU), the vehicle portion of the Collision Avoidance Subsystem (CAS), and the Vehicle Subsystem. Table 3.3.4-1 is a tabulation of the VCU electrical interfaces.

Interfacing with the GCU is accomplished via inductive FSK transmissions and magnetic signalling. Interfacing with the CAS is a parallel transfer of 8-bit bytes of digital information on hard wired lines; however, these lines are electrically isolated by the use of optical couplers.

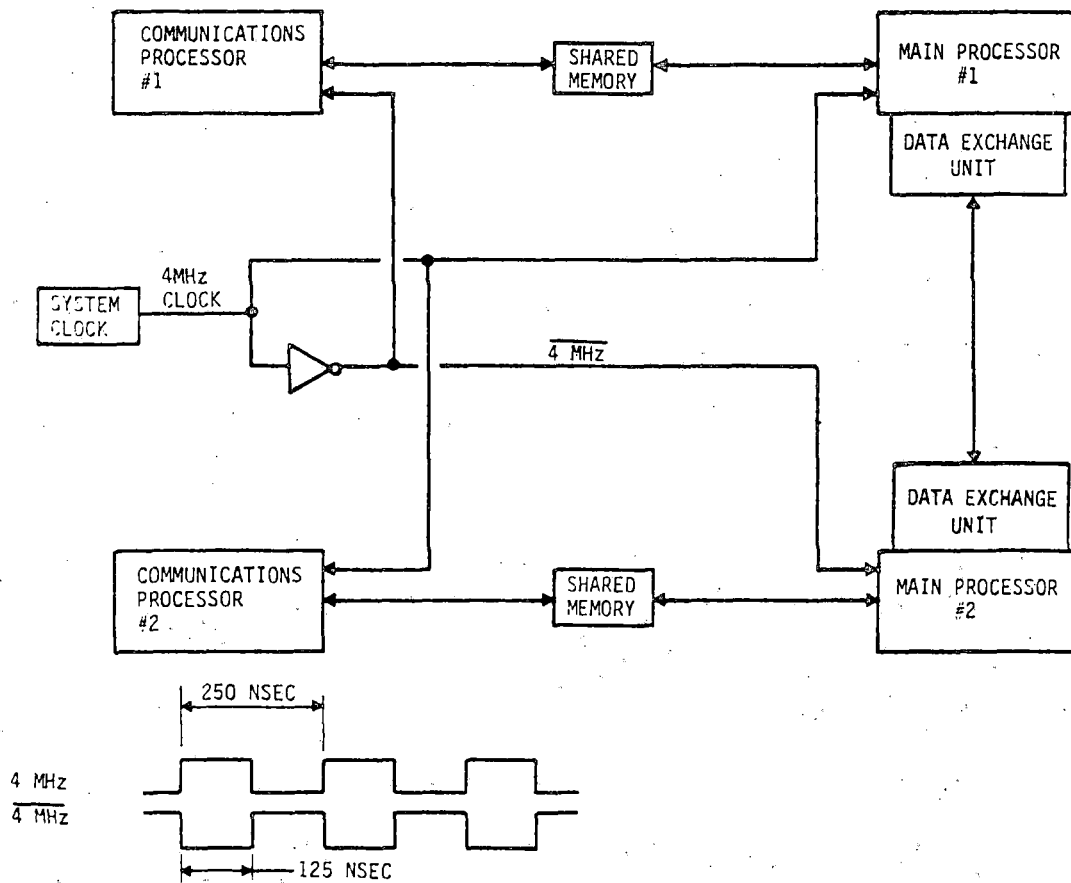


FIGURE 3.3.3.3-2: SYSTEM CLOCK DISTRIBUTION

TABLE 3.3.4-1  
VCU ELECTRICAL INTERFACES

INPUTS				Source/Sensor
	Analog	Discrete	Pulse Train	
Signal				
FSK Uplink Data			X	Loop Antenna
Position Correction/Calibration Request		X		Reedswitch (Dual)
Switch Initiate		X		"
Station Stop Initiate		X		"
Propulsion Torque, Measured	X			Motor Controller
Propulsion Contactor Open		X		" "
Instantaneous Loss of Power		X		" "
Overtemperature Shutdown		X		" "
Overtemperature Warning		X		" "
Overcurrent/Overspeed Shutdown		X		" "
Loss of Battery Charger		X		" "
Caliper Pressure Full Range Sys. (A)	X			Hydraulic Pressure Transducer
Caliper Pressure Lim. Range Sys. (A)	X			" " "
Caliper Pressure Full Range Sys. (B)	X			" " "
Caliper Pressure Lim. Range Sys. (B)	X			" " "
Brake Pad Overtemperature		X		Thermally Actuated Switch
Hydraulic Fluid Temperature		X		Thermally Actuated Switch
Hydraulic Accumulator A		X		Pressure Actuated Switch
Hydraulic Accumulator B		X		" " "
LR Wheel Angular Displacement			X	Hall Effect Pickup
LF Wheel Angular Displacement			X	" " "
RR Wheel Angular Displacement			X	" " "
RF Wheel Angular Displacement			X	" " "
Switch Left Verification		X		Microswitch
Switch Right Verification		X		"
Calibration Factor Command		X		Push-Button Switch

TABLE 3.3.4-1 (Continued)  
VCU ELECTRICAL INTERFACES

INPUTS Signal				Source/Sensor
	Analog	Discrete	Pulse Train	
Emergency Exit Closed		X		Reedswitch on Lock
Left Service Door Fully Closed		X		Microswitch
Left Service Door Fully Open		X		"
Left Service Door Obstructed		X		"
Right Service Door Fully Closed		X		"
Right Service Door Fully Open		X		"
Right Service Door Obstructed		X		"
Power Monitor	X			Battery Buss
Vehicle Overload		X		Switch Pneumatic Pressure
Main Processor Monitor Data Input			X	EIA RS232C Line
Comm. Processor Monitor Data Input			X	" " "
Test Point Output Select		X		Thumbwheel Switches
Pneumatic Pressure Low		X		
OUTPUTS Signal				Destination/Receptor
ODDCAS Speed, Position		X		ODDCAS Input
ODDCAS Push Mode		X		" "
ODDCAS Bias Direction		X		" "
ODDCAS Handshake		X		" "
FSK Downlink Data			X	Guideway Loop Antenna
Propulsion Torque Command A & B	X			Motor Controller
Propulsion Enable		X		" "
Brake Torque Command A & B	X			Brake Amplifier
Suspend Emergency Brake A & B			X	" "
Switch Left Command		X		Relay Coil
Switch Right Command		X		" "
Open/Close Left Service Door		X		Relay Coil
Open/Close Right Service Door		X		" "
Unlock Service Doors		X		Solenoid Coil
Analog Test Point Outputs (16 Total)	X			Meter Jack
Main Processor Bus		X		Test Jack
Comm. Processor Bus		X		" "
Vehicle Presence		X		Wayside Presence Detector
Main Processor Monitor Data Output			X	Terminal
Comm. Processor Monitor Data Output			X	"
Calibration Factor Acknowledge		X		Lamp



The vehicle interface involves a variety of signals; analog, digital discrete, and pulse train. The analog signals are the Propulsion Torque Command, the Brake Servo Command, the Measured Propulsion Torque, the Brake Caliper Pressure, and the Prime Power Voltage. The discrete signals are the Steering Subsystem Commands, the Door Subsystem Commands, the Steering Subsystem Verification, and the Door Subsystem Status. The pulse train type signals come from the wheel mounted odometers and the FSK uplink/downlink messages. The majority of these lines are electrically isolated by the use of optical isolation techniques and solid state relays.

The vehicle has sensors monitoring certain functions such as door status. Certain of these sensors are in a dual configuration and each signal is assigned to its respective Main Processor Channel. Other monitor points have a single sensor with its output routed to both Main Processors. An example is the wheel odometer pickup; one sensor is placed on each wheel but each sensor's data is input to both Main Processors. However, in both cases the sensor data one channel sees is passed through the Data Exchange Unit to the other channel for checking and/or voting.

Output control discrettes such as steering or door commands are configured as series contact closures where signals from both Main Processors must agree in order to complete the circuit. The brake and motor torque command signals have special requirements that will be discussed in detail in the following pages.

#### 3.3.4.1 Inductive Communication Signals

##### 3.3.4.1.1 FSK Receiver Signals

The vehicle is equipped with two antennas for receiving FSK data; a forward antenna and a rear antenna. The received uplink signal path to the Main Processors is shown in Figure 3.3.4.1.1-1. The data from each antenna is fed into two FSK receivers. (One receiver per antenna per

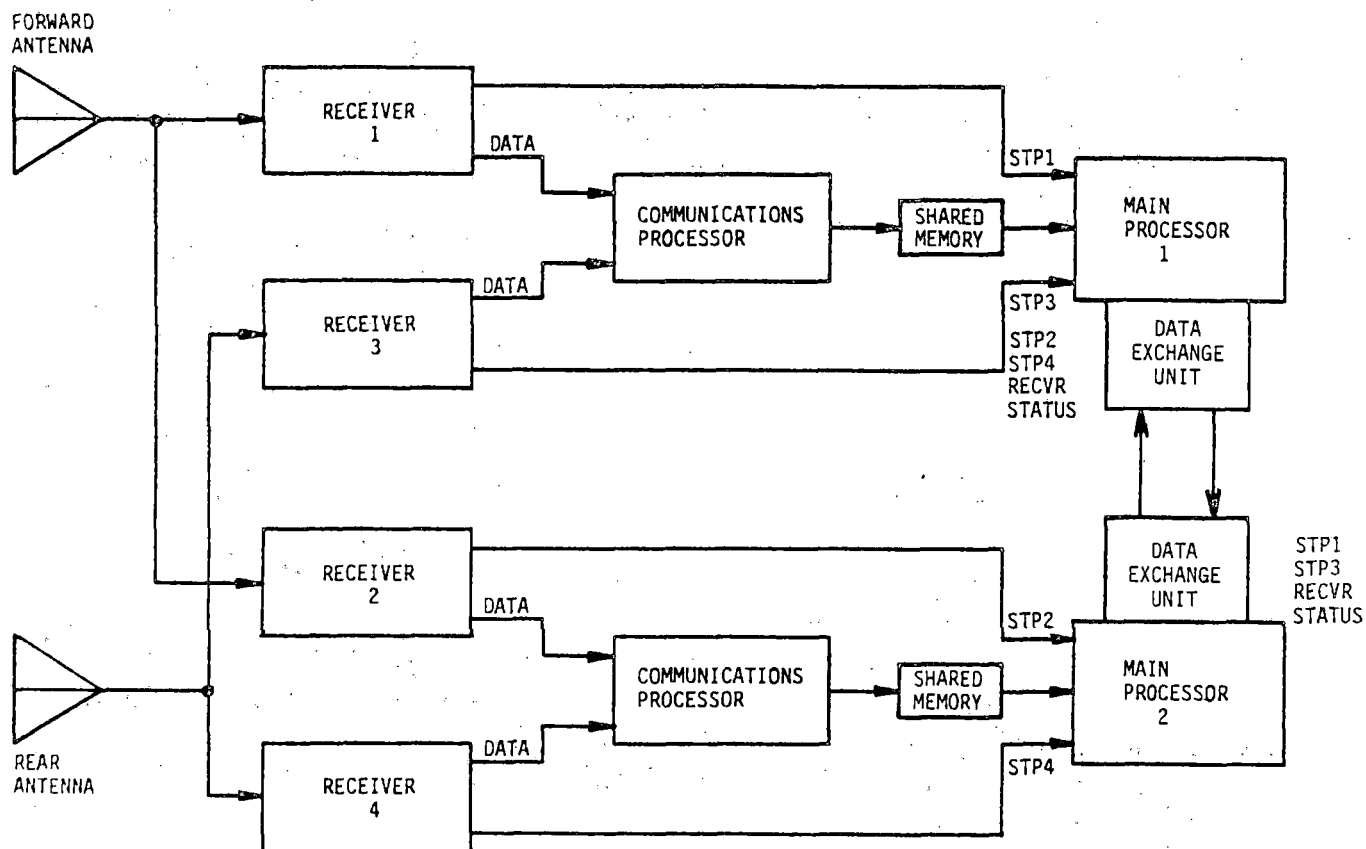


FIGURE 3.3.4.1.1-1: FSK RECEIVER SIGNAL PATHS

channel or two receivers in each channel.) The receivers use the FSK modulated signal to extract a clock pulse and data. The clock pulse is used as the clock signal by the Communications Processor to input the serial data message from the receiver. This clock pulse is also used as the Safe-to-Proceed (STP) signal to the Main Processor. The STP signal from the receivers is a dynamic signal that must continually set a latched input logic device to the Main Processor. The Main Processor, at a rate slower than the dynamic STP signal, samples the latch then resets it. If the latch is not set between samples a loss of STP is declared.

Referring to the same figure, the receivers labeled 1 and 3 input their STP signal to latched inputs of Main Processor 1 and their data to Communications Processor 1. Receivers 2 and 4 are connected to Main Processor 2 and Communications Processor 2 in the same manner. Each Main Processor always utilizes data from the forward antenna's receiver for control purposes. The rear antenna receivers are to provide a communication backup in anomaly situations and to ensure a continuous STP signal at FSK wayside loop boundaries.

Each Main Processor inputs and stores the two latched STP signals every 10 milliseconds. The STP information is exchanged between the two Main Processors and safe reaction is initiated when the following logic condition exists:  $(STP1 + STP2) (STP3 + STP4)$ . Stated another way, the system is allowed to operate when the logic function is  $(STP1 \cdot STP2) + (STP3 \cdot STP4)$ .

#### 3.3.4.1.2 FSK Transmitter Signal

The vehicle is equipped with one antenna for transmission of FSK data to the wayside. The transmit downlink signal path is shown in Figure 3.3.4.1.2-1.

The downlink, unlike the uplink, is not performing a safety critical function; therefore, it is implemented as a single thread configuration.

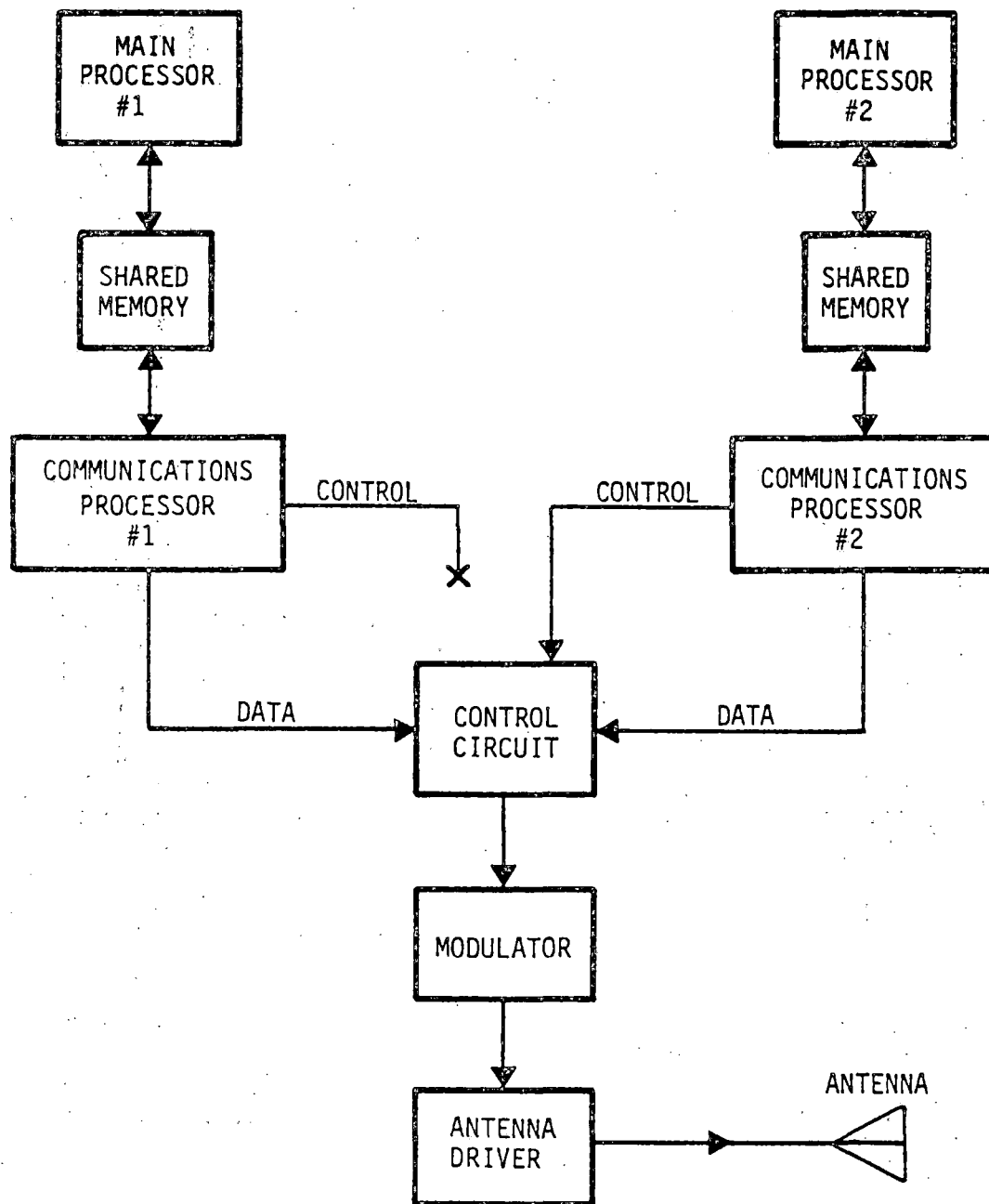


FIGURE 3.3.4.1.2-1: FSK TRANSMISSION SIGNAL PATH

Also downlink messages are not transmitted continually; messages are only downlinked when requested by an uplink command or initiated by the VCU under certain anomaly conditions.

Downlink data from each channel is fed to a gating circuit prior to the modulator. A signal from Channel 2's Main Processor controls the gating circuit that selects which Channels' data is actually transmitted. The normal selection is to use Channel 1's data. If Channel 1 appears to be experiencing a problem, Channel 2 switches to its own downlink data and reports the anomaly.

#### 3.3.4.2 Discrete Input/Output Signals

A discrete signal is defined as having two states, such as "on" or "off". They are normally the output of a switch or relay. On the vehicle, discrete inputs to the VCU report the status or condition of a vehicle element, such as a door. Most discrete outputs from the VCU provide a command function to a vehicle element, such as close a door. Following is a description of each input and output discrete.

##### 3.3.4.2.1 Discrete Input Signals

###### Switch Initiate

A dual redundant reed switch assembly mounted on the underside of the vehicle is activated whenever the switch centerline is within  $5.0 \pm 5.0$  inches of the guideway magnet centerline. Activation of this switch causes the VCU to initiate the vehicle's switching action according to a previously stored switching direction command. This signal is connected to both VCU channels.

###### Station Stop Initiate

A dual redundant reed switch assembly mounted on the underside of the vehicle is activated when the switch centerline is within  $2.0 \pm 2.0$

inches of the guideway magnet's centerline. Activation of this switch causes the VCU to initiate the station stopping profile of a previously stored station stop command. This signal is connected to both VCU channels.

#### Position Correction/Calibration Request (PC/CAL)

A dual redundant reed switch assembly mounted on the underside of the vehicle is activated when the switch centerline is within  $5.0 \pm 5.0$  inches of the guideway magnet's centerline. Activation of this switch causes the VCU to initiate the a position correction/calibration function. This signal is connected to both VCU channels.

#### Propulsion Contactor Open

A signal from the propulsion unit that indicates if power is being applied to the propulsion unit. When the Propulsion Contactor Open signal is true the power line to the propulsion unit has been physically opened. This signal goes to both VCU channels.

#### Instantaneous Loss of Power

A signal from the propulsion unit saying that it has shut down because the power (voltage) is too low to operate or has been lost completely. This signal is fed to both VCU channels.

#### Overtemperature Warning

A signal from the propulsion unit saying it is overheating. This signal is fed to both VCU channels.

#### Overcurrent/Overspeed Shutdown

A signal from the propulsion unit saying it is in an overcurrent/overspeed condition and is shutting down. This signal is fed to both VCU channels.

### Loss of Battery Charger

A signal from the propulsion unit saying the battery charger voltage is below allowable limits. This signal is fed to both VCU channels.

### Brake Pad Overtemperature

This signal comes from a thermally actuated switch that monitors the temperature of one brake pad. This signal is fed to both VCU channels.

### Hydraulic Fluid Temperature

This signal comes from a thermally actuated switch that monitors the temperature of the hydraulic fluid. The switch is actuated when the fluid temperature goes above a limit. This signal is fed to both VCU channels.

### Hydraulic Accumulator A(B)

There are two hydraulic systems that control the brake system. The hydraulic accumulator in each system is monitored for low pressure by a pressure sensitive switch. Each accumulator signal, A and B, is fed to both VCU channels.

### Switch Left Verification

This signal comes from a microswitch which is monitoring the left steering mechanism. When the vehicle steering is in a left mode a positive indication is sent to both VCU channels.

### Switch Right Verification

This signal comes from a microswitch which is monitoring the right steering mechanism. When the vehicle steering is in a switched right mode a positive indication is sent to both VCU channels.

#### Calibration Factor Command

This signal comes from a push-button switch located on the test panel of the VCU rack that an operator depresses when a condition exists that would make the stored calibration void. This signal is fed to both VCU channels.

#### Emergency Exit Closed

This signal comes from a reedswitch on the lock of the emergency exit door which monitors that the door is closed. This signal is fed to both VCU channels.

#### Left Service Door Fully Closed

This signal comes from a limit switch on the door cam. The switch closes when the door is fully closed. This signal is fed to both VCU channels.

#### Left Service Door Fully Open

This signal comes from a limit switch on the door cam. The switch closes when the door is fully open. This signal is fed to both VCU channels.

#### Left Service Door Obstructed

This signal is not implemented for EDS.

#### Right Service Door Fully Closed

(Same as Left service door.)



#### Right Service Door Fully Open

(Same as left service door.)

#### Right Service Door Obstructed

This signal is not implemented for EDS.

#### Vehicle Overload

The vehicle pneumatic suspension system incorporates a pair of series connected, normally closed pressure actuated switches. These switches (one forward and one aft) open when the suspension system develops a pressure which exceeds a threshold of loading. This signal is fed to both VCU channels.

#### Pneumatic Pressure Low

This signal is from a pressure actuated switch which opens when the pneumatic pressure falls below a certain pressure. This signal is fed to both VCU channels.

### 3.3.4.2.2 Discrete Output Signals

#### Propulsion Enable

The Main Processor provides, through the PTCDCU, the propulsion system with a command to enable propulsion. This command causes the propulsion contactor to close. When "Propulsion Enable" is removed the propulsion contactor will open. Each channel provides this signal, however, the EDS configuration has only one propulsion contactor. This signal is provided by Channel 1 only in the EDS configuration.

### Switch Left Command

The VCU provides a signal to the steering system to switch left. This command is provided by both channels through series connected solid state relays. Both channels must respond before the command is sensed by the steering system.

### Switch Right Command

(This signal is implemented the same as the "Switch Left Command.")

### Open/Close Left Service Door

The VCU provides a signal to a relay coil in the door system which opens the left service door. This command is provided by both channels through series connected solid state relays. Both channels must respond positively before the door will open.

### Open/Close Right Service Door

(This signal is implemented the same as the left service door.)

### Unlock Service Doors

(This command is not implemented in the EDS design.)

### Vehicle Presence

An output signal created by the magnetic field of an onboard permanent magnet acting upon a guideway mounted presence detector. The magnet, when mounted on the underside of the vehicle, will actuate a guideway mounted detector when the magnet centerline is  $5.0 \pm 5.0$  inches from the detector's centerline.

### Calibration Factor Acknowledge

A signal, provided by the VCU in a series fashion, which turns on an indicator light on the VCU acknowledging that both channels have received the "Calibration Factor Command". If either channel doesn't respond positively the light will not turn on.

#### 3.3.4.3 Analog Input/Output Signals

Three analog inputs are converted by A/D converters into 8-bit bytes and input to the Main Processor by means of the parallel input port. A fourth analog signal from the propulsion unit is converted to a digital byte in the PTCDCU and is transmitted to the Main Processor via the fiber optic link.

One analog output signal, the brake torque command, is converted from an 8-bit byte to an analog signal. The propulsion torque command is transmitted to the PTCDCU over the fiber optic cable and converted to an analog signal for use by the propulsion unit.

The remaining analog signals are the analog test point outputs. These are test points only, not vehicle signals, and are treated separately in Section 5.2.1.

##### 3.3.4.3.1 Analog Inputs

#### Measured Propulsion Torque

This is an analog signal, which is proportional to the generated tractive effort developed in the propulsion unit. This signal is fed to the PTCDCU via a low impedance, differential, balanced, shielded pair. The analog signal at the PTCDCU is sampled every 10 milliseconds and converted into an 8-bit natural binary byte. The PTCDCU then transmits the digital information via the fiber optic link to the Main Processor.

In the EDS configuration there is only a single thread propulsion unit electronics and a single PTCDCU. The PTCDCU interconnection is routed to both VCU channels for input signals.

#### Caliper Pressure Full Range Sys. A

This is an analog signal proportional to the hydraulic pressure applied at the brake caliper as measured by a transducer. The transducer range is 1000 P.S.I.G. and the scaling factor is 5 millivolts per P.S.I.G. The signal is sampled and converted every 40 milliseconds to an 8-bit natural binary byte. This signal is fed to Channel 1 only.

#### Caliper Pressure Limited Range Sys. A

This is an analog signal proportional to the hydraulic pressure applied at the brake caliper as measured by a transducer. The transducer's range is 200 P.S.I.G. and the scaling factor is 25 millivolts per P.S.I.G. The signal is sampled and converted every 40 milliseconds to an 8-bit natural binary byte. This signal is fed to Channel 1 only.

#### Caliper Pressure Full Range Sys. B

This signal is handled the same as (A) above, only it is fed to Channel 2 only.

#### Power Monitor

Each VCU channel has an A/D converter that samples the battery voltage every 40 milliseconds and converts the analog voltage reading to an 8-bit binary byte for processing.

#### 3.3.4.3.2 Analog Outputs

#### Propulsion Torque Command A

The Main Processor sends a 12-bit natural binary digital message over

the fiber optic link to the PTCDCU. This signal is then converted to an analog signal which is proportional to the commanded torque. The signal is connected to the propulsion unit via a low impedance, differential balanced, shielded pair.

Since in the EDS configuration there is only one PTCDCU and propulsion unit, only Channel 1's data is used.

#### Propulsion Torque Command B

This is the output of Channel 2 but is not used in the EDS configuration.

#### Brake Torque Command A

The VCU delivers an analog signal to a brake amplifier. The Main Processor sends a 12-bit natural binary message to an A/D converter where it is converted to an analog signal proportional to the commanded braking torque. The signal is transmitted to the brake amplifier via a low impedance, differential balanced, shielded pair. This signal is from Channel 1.

#### Brake Torque Command B

This signal is generated similarly to (A) above but in Channel 2 it is output to a second brake amplifier.

### 3.3.4.4 Vehicle Collision Avoidance Signals

The VCU furnishes calibrated odometer data and vehicle steering bias direction data to the Odometer Data Downlink Collision Avoidance System (ODDCAS) on-board electronics. The interface consists of 10 lines, all electrically isolated by the use of optical isolation techniques. The 10 lines include 8 lines for a parallel byte transfer and two handshake lines. Information is transferred from the VCU to the ODDCAS every 40 milliseconds.

#### 3.3.4.5 Odometer Signals

The vehicle has an incremental encoder at each wheel that produces a pulse train data signal. The four odometer pulse train data signals are routed to both channels of the VCU. The signals are electrically isolated by the use of optical isolation techniques. Nominal signal scaling is 0.0338 feet/pulse.

#### 3.3.4.6 Motor Controller Signals

Figure 3.3.4.6-1 details the signal redundancy configuration between the VCU and the propulsion subsystem. Torque command signal disparity checking and transmission are performed in the Main Processors. Each processor calculates a torque command, examines the torque command value calculated by the other Main Processor, and if equal transmits it to the propulsion system.

Within the propulsion system the two torque command signals are compared in independent over-torque detectors with locally measured torque values. The over-torque detectors provide hold-off signals to the line contactors and return status signals to the VCU to indicate a runaway motor condition.

For the EDS (Engineering Development System), a Morgantown People Mover (MPM) propulsion subsystem was to be used. Consequently the redundancy configuration for an AGRT configuration, as shown in dashed lines in the figure, was not fully implemented. The EDS configuration is given in solid lines.

#### 3.3.4.7 Vehicle Brake Signals

##### 3.3.4.7.1 Service Brakes

To apply service brakes each Main Processor commands a servo valve in a dual, independent hydraulic system. Each brake caliper assembly contains two input ports with each port connected to one of the hydraulic systems. The brake torque command, therefore, is voted mechanically at

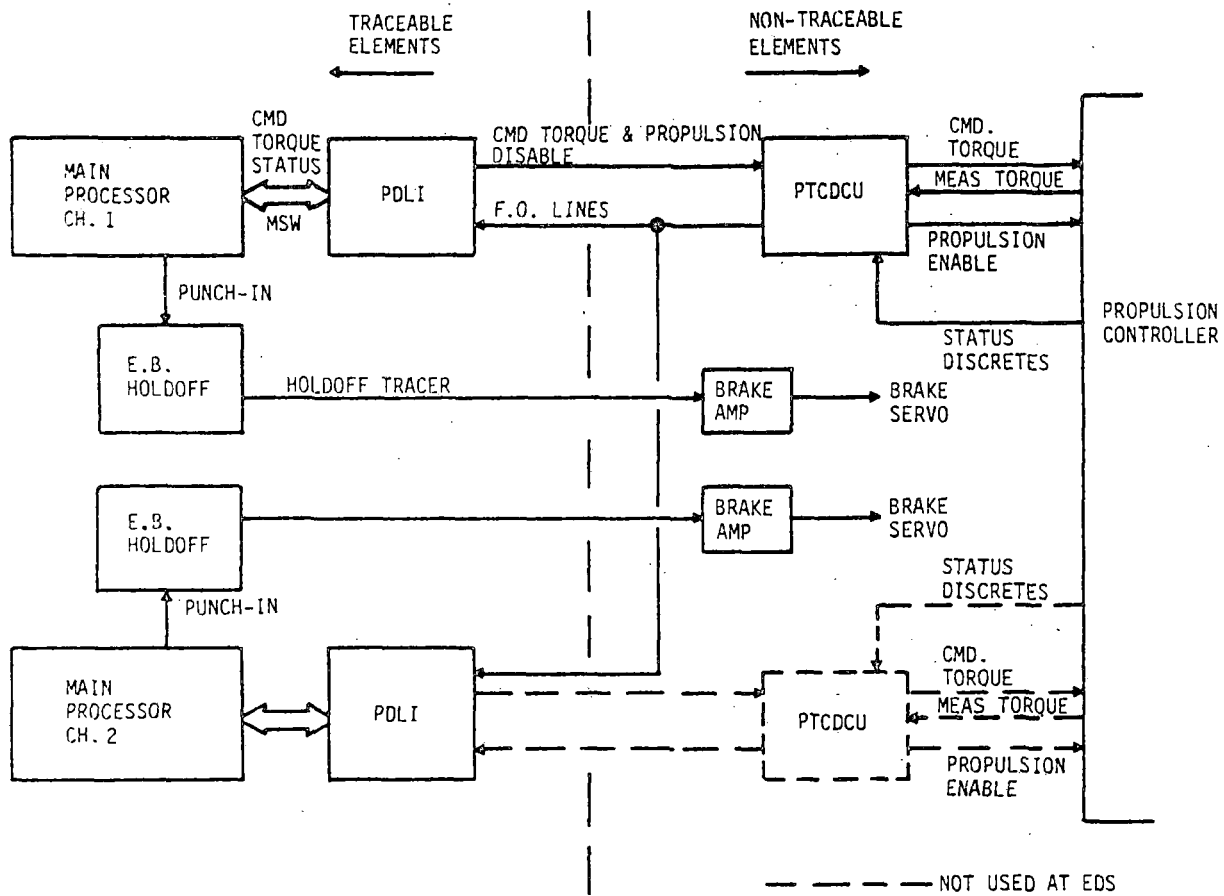


FIGURE 3.3.4.6-1: EDS PROPULSION INTERFACE

the brake caliper, with the highest torque command prevailing. Disparity checking between the two servo valve control signals is performed in software within the Main Processors. Additionally, disparity checking of hydraulic pressures is performed in software within the Main Processors.

#### 3.3.4.7.2 Emergency Brakes

The emergency brake control configuration is given in Figure 3.3.4.7.2-1. Loss of "keep alive" signals generated by either Main Processor causes drop out of the emergency brake hold-off signal, resulting in the application of open-loop emergency brakes.

The "keep alive" signal from each Main Processor is a pulse occurring every 10 milliseconds. Loss of this signal constitutes a command to deploy the emergency brake. In each channel the 10 millisecond pulses are used to generate a 50 Hz square wave tracer signal by a timer circuit clocked with an oscillator independent from the Master Clock. In this way frequency drift or failure of the Master Clock or failure of the 10 millisecond interrupt signal lead to deployment of the open-loop emergency brakes.

### 3.4 Software Architecture

#### 3.4.1 General Description

The VCU software is divided between two micro-processor systems: the Communications Processor, which handles the formatting, error checking, and serial/parallel data conversions of the FSK messages, and the Main Processor, which performs the decision and control functions of the VCU.

##### 3.4.1.1 Communication Processor Software General Description

The Communication Processor Software is an event driven design. There are three types of events to which the Communication Processor Software responds.



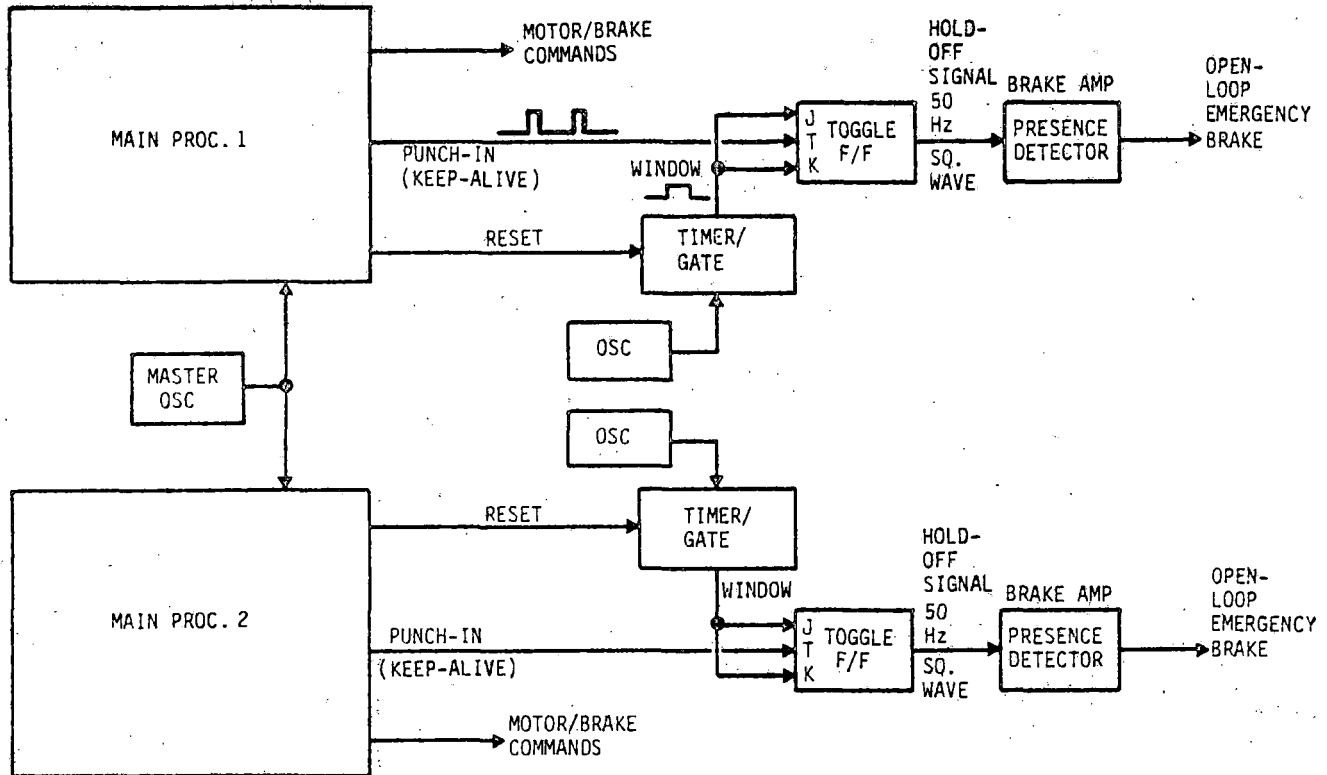


FIGURE 3.3.4.7.2-1: EMERGENCY BRAKE COMMAND SYSTEM

First, when a single binary digit of an FSK message sent to the vehicle from the wayside is detected by the receiver, it sends an interrupt to the communication processor. These bits are taken in, checked one at a time, and assembled into uplinked messages.

Second, downlink messages are loaded into the communications processor from the main processor and the transmitter is turned on in response to requests from the main processor. These requests are detected via periodic polling of the main processor.

Third, the transmitter sends interrupts to the communications processor requesting the next downlink message bit. These downlink messages are transmitted to the wayside one bit at a time.

#### 3.4.1.2 Main Processor Software General Description

The Main Processor Software has a cyclic design. In a forty millisecond cycle, as determined by an on-board clock, a series of tasks are executed. These tasks are built around the major functions: monitoring of vehicle status, processing of external input, and generation of vehicle commands.

#### 3.4.2 Software Safety Implementation

One major implementation of the failsafe design principles in the Vehicle Control Unit is checked redundancy; software is the key to this implementation. One of the requirements for achieving safety through checked redundancy is that the redundant paths have no common or correlated failure modes for performance of the same safety-related function. The failsafe requirement is satisfied if the probability of such a common or correlated failure being unsafe and undetected is negligibly small; this negligible probability is taken to be one in a million years.

The safety related redundant paths that must be free of unsafe common or correlated failures were categorized and studied; each function has a hardware and software path.

Every element of the hardware path not intrinsically fail-safe must be periodically exercised (checked for failure). The check period is determined by the statistical failure rate of the element being checked and the consequences of a failure, i.e., performance of the vehicle in the event of a failure.

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 fail 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 cells every 9 minutes. The implementation does it once every 2 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 is not 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" algorithm) then checks the results of the "A" logic. If the A/B results differ by more than a set margin, the software is assumed to be in error and a safe reaction is initiated.

#### 3.4.2.1 Redundant Input Management

The vehicle sensors and communication processors that pass information to the two channels are, in some cases, distinct devices dedicated to serving only one channel. In other cases the sensors may feed their output simultaneously to both channels. For those sensors that are tied to both channels, their signals arrive functionally at different times to the main processors that read them. The main processors have a common clock, but each is out of step with the other by one half clock cycle. (Clock pulses for one channel are inverted to simplify the task of arbitrating simultaneous access to common addresses in the Data Exchange Unit.) As a result of this difference in cycle phase between channels, even signals sent simultaneously to each redundant main channel will be read at differing times by those channels. The data used by the control laws in the two channels must be identical or resulting control commands will differ and will result in a shutdown of the system.

The software scheme for resolving differences must not affect the independence of the command paths; three methods are used in the VCU.

One method is to have the two channels exchange their respectively received input data and each independently select the safest data to use. Sometimes this results in ignoring and in other cases using signals received from the other channel. In either case the data used is common between the channels. This method resolves all internal and external discrete sensors, all FSK communicated speed limits, and some of the analog data.

A second method is to have the data exchanged across the channels and have one channel designated as prime. The prime channel's data is used by both channels for vehicle command generation. The other channel's data is used for comparison to check for unacceptable drifts between the two sets of data. Again, each channel processes full data independently. This method is used for all odometer processing.

A third method involves data that is used for status measures of devices, which if out of tolerance, result in commanded safe reactions. These status measures are processed independently by each channel and the reaction commands are exchanged on a periodic basis. Here the control commands are synchronized instead of the data. This method is used for certain device checkers like the logic that checks the Safe-to-Proceed flip-flop and the rest of the analog data.

There is an additional method for resolving differences, but it does not preserve channel independence. It therefore cannot be used for safety related vehicle control. This involves each channel receiving data and exchanging it. Only the prime channel's data is used and the non-prime channel's data is discarded. The input device for that data in the prime channel must be continually checked for operability and if it fails, the non-prime channel's device must take over the function of data input for both channels. (This method is used for FSK vehicle command messages but is not used for FSK speed limit processing.)

#### 3.4.2.2 Monitoring of Redundant Processing

Vital data used in the generation of brake torque and propulsion torque commands are exchanged between the redundant channels every forty milliseconds for the purpose of detecting any disagreement that would indicate insanity of the control system. Because the input data on which the control laws depend are made common by independent processes before the control commands are generated, no margin for disagreement is permitted in the cross channel comparison process; any disagreement in command data results in a safe shut down of the microprocessor control

system. To assure the correct operation of this disparity detection process, a second comparison of this vital data is made during the same forty millisecond cycle using a differing methodology.

#### 3.4.2.3 Monitoring of Logic Integrity

There are two aspects of assuring that logic paths required for control command generations will operate as designed. First, the code as stored in memory must not change due to any failure of the cells where it is stored or the circuitry that fetches the code. Second, once good code is fetched into the code processor hardware, it must result in computations and decisions as intended.

Assurance that the program code, as stored, is intact and can be fetched when needed is established by a periodic checksum of the entire body of stored program logic. If the checksum is not as expected, the system initiates a safe shutdown. This logic checking is done in background.

Assurance of the reliability of the code processing hardware is achieved by exercising of the safety critical code through the processing hardware. A series of self tests are called in background; each one of these self tests calls vital control code, passing to that code dynamically changed data that simulates emergency conditions. The self test then checks the output of this control code for the expected control reactions to the simulated emergency data. If the reaction is as expected, it is assumed the hardware is operating correctly and would properly process that code if circumstances required.

All safety critical logic is so exercised in background. For any detected failure of this code the reaction is to not only withhold the punch-in (emergency brake holdoff) but to immediately halt all processing by the Central Processing Unit.

#### 3.4.2.4 Monitoring the Integrity of the Software Processing Hardware

The previous section describes forms of processing hardware integrity checks. In addition to those checks, there is a need to assure that the RAM cells, accumulators, general purpose registers, and control flags of the Central Processing Unit are operating correctly.

In background each memory cell in the Data Exchange Unit and Communications Processor shared memory is checked bit for bit for operability; the same is done for each of the processing registers of the CPU.

The accumulator or computation processing part of the CPU is exercised in background in such a way as to set and clear each of the control flags on which all logic path switching is based. Any detected failure of the processing hardware results in an immediate halt of any further processing.

#### 3.4.3 Main Processor Software

The Main Processor Software is composed of three distinct elements:

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

##### 3.4.3.1 Initialization and Synchronization

On start up or reset of the main processor the software initializes and checks its associated hardware and software. The steps involved in the initialization process for each of the two main processors are outlined in the following subparagraphs:

#### 3.4.3.1.1 Loading of CPU Internal Registers

The interrupt service vector table address is loaded to the CPU. There are only two interrupts that are acceptable to the CPU during initialization: the non-maskable, and the non-vectorized.

A non-maskable interrupt results in a jump to service; this interrupt comes every ten milliseconds. The service done at this interrupt during the initialization process is to increment a clock used for timing the duration of the initialization process and to set a flag used by some initialization processes to sequence loop tasks.

The non-vectorized interrupt is serviced only during initialization. Pressing the non-vectorized interrupt button on the VCE card cage provides operator access to the special monitor program used for inspection of micro-processor memory and registers.

The flag and control register is loaded with allowance for only the two interrupt signals described. Any other interrupt signal that reaches the CPU is considered anomalous and results in a CPU halt.

#### 3.4.3.1.2 Software initialization

All non-fixed data memory is cleared to zero except the stack. Then those global variables that require non-zero values at the start of vehicle control processing are set to their required values.

The first of two steps in building the emergency brake holdoff key is taken; this holdoff key is checked every 10 milliseconds during vehicle control logic processing before punch-in.

The fault queue of software reported faults (implemented as a linked list stored in non-volatile memory) is checked for correct format. If it is not in correct format, it is cleared and a report of "garbled fault queue" is prepared for FSK downlink at the end of initialization.



Two calibration factors for combinations of the four wheel odometers are stored in non-volatile memory. If they are out of range of the nominal calfactor, or differ from those stored in the other channel, they are cleared, set to a safe default value, and a fault message is put on the fault queue.

Only one of the two redundant main processor channels is allowed to be designated as the prime channel for odometer and FSK communication processing. A discrete input (backplane wiring) designates which channel is prime.

#### 3.4.3.1.3 Processor Integrity Check During Initialization

The second step in building the emergency brake holdoff key is taken. It is done here to allow use of the key in the code and processor integrity checks. All code and processor integrity checks described in section 3.4.2.3 are executed during initialization.

#### 3.4.3.1.4 Hardware Initialization

During the hardware check portion of initialization:

1. All preprocessor devices are reset.
2. Brake command levels are dispatched to the braking system.
3. Steering bias is read and asserted.
4. Doors are commanded closed and checked.
5. Sensors are read, checked, and synchronized with the redundant channel sensors.
6. Odometers are checked for a vehicle at rest and then cleared.
7. Emergency brake system is checked end to end by checking the brake pressure under emergency brake command conditions, then under parking brakes, and again after reapplication of the emergency brake command.

#### 3.4.3.1.5 System Synchronization and Start of Vehicle Control

Thirty seconds is allowed for the initialization tests; this period permits the hydraulic system to come up to full pressure. If all initialization checks are successful within that period, a check is made of the ready flag from the communication processor. If all is ready, a flag is set in the Data Exchange Unit to indicate the main processor is ready for vehicle control. When the redundant channel's ready flag goes high, the synchronization is complete. (A special flag sequence is used here to prevent reading a non-operating channel as ready.)

On completion of synchronization the new interrupt service vector table address for vehicle control is loaded to the CPU. Vehicle control by the main processor begins with the next ten millisecond interrupt.

#### 3.4.3.2 Cyclic Executive

Every ten milliseconds an interrupt from the master clock initiates a vehicle control duty frame; these ten millisecond frames are called minor frames. The start of each frame includes a punch-in, the reading and integrating of guideway communication discretes, and the reading of the four wheel odometers. After the initial common portion of the frame is complete one of the four major functions is done. These are allocated among the minor frames as follows:

Minor Frame 1 - Processing of vehicle control data input

Minor Frame 2 - Processing of longitudinal control laws

Minor Frame 3 - Processing of safety assurance logic

Minor Frame 4 - Processing of vehicle status, lateral control laws, exit control, and dissimilar control software.

This cycle of 4 minor frames is referred to as a single major frame.

#### 3.4.3.2.1 Punch-In

Failure of any self check which indicates that the control system is not operating properly results in the clearing of the punch-in key. On each receipt of a ten millisecond interrupt signal, this key is checked. If the key is intact, a pulse is sent to the emergency brake holdoff mechanism indicating the brakes should be withheld for another ten milliseconds. Under the same conditions the motor torque command is sent to the propulsion system. If the key is not intact the holdoff pulse and motor torque are withheld. This causes the emergency brakes to be applied and the propulsion system to drop the motor torque to zero.

Failure of the self checks done in background also results in a CPU halt which prevents the processor from even acknowledging the 10 millisecond interrupts.

#### 3.4.3.2.2 Frame Common Input Processing

There are several sensors that are read every ten milliseconds:

1. Every ten milliseconds the magnetic signaling from the guideway is read and, if precision requires, time tagged.
2. The safe-to-proceed discretes are processed and shared with the redundant channel. If at least both of the forward receivers or both of the aft receivers indicate it is safe to proceed, normal vehicle processing continues. Otherwise the command to initiate a software controlled closed-loop emergency stop (CLEB) is given. When any new command to initiate a CLEB is made, the sequence of minor frames is broken and frame one is started. This resequencing accomplishes an immediate start of the controlled closed loop emergency stop.

3. If the vehicle is at rest and an onboard operator depresses the monitor request button on the VCU card cage, that action would be sensed and the control program would stop to allow use of the monitor program to search the data base.
4. All four wheel odometers are read for pulse count and last pulse time. An array is maintained that contains all of the running pulse counts from each wheel for the present minor frame and each of the past four minor frames. Associated with each pulse count is the time at which the last pulse of that count was detected. Later in frame one the array is used to calculate the number of pulses detected over the last four frames for each wheel and also to calculate exactly the span of time for that number of pulses; vehicle speed and position is derived from this data.
5. If a maintenance operator should change vehicle tires, the calibration factors stored in the system would no longer be valid. Safe default calibration factors are loaded by pressing the cal-factor request button mounted on the card cage of the vehicle electronics. This request sensor is polled every 10 milliseconds, not because of any urgency, but because it is located in the same register with the magnet and safe-to-proceed sensors.

#### 3.4.3.2.3 Frame One - Data Input

The data processed in this minor frame includes the odometer data and the FSK messages.

The number of odometer pulses accumulated over a distance of from 500 to 1000 ft is converted to a calibration factor used in the measure of vehicle speed and position. The speed and position of the vehicle is calculated using two combinations of front and rear wheel odometer measures. To assure the reliability of these vital measures, there are nine consistency and continuity tests performed on them each major frame.

The incremental position, or distance traveled by the vehicle during the last major frame, and the measured speed are passed to the moving block collision avoidance subsystem during this minor frame.

Under normal operating conditions FSK messages are uplinked continuously. It takes forty milliseconds for one message to be relayed (one major frame). If the message carrier (the safe-to-proceed signal) is present but no messages are transmitted for four hundred milliseconds (ten message periods), the vehicle will execute a normal rate stop.

FSK messages are composed of seven fields:

1. Speed Limit Command
2. Vertical Redundancy Check (VRC) (Check of the integrity of the speed limit)
3. Line Speed Command (The speed at which the vehicle should regulate when dispatched.)
4. ID/Data (For messages with commands intended for a particular vehicle, the vehicle ID number is present; messages with data intended for a particular vehicle are processed by that vehicle only if the vehicle has been previously notified that the data is to be expected.)
5. Function Code (Command category)
6. Command
7. Cyclic Redundancy Check (CRC) (Check of integrity of entire message)

Each of the two redundant channels accepts and unpacks messages from its respective communication processor. Each loads its own speed limit, but compares and uses the lower of the two speed limits if the speed limits

in the two channels differ. (They could differ if one channel did not receive a message.)

The rest of the message fields are shared cross channel via the Data Exchange Unit; only those received by the prime channel are used.

The data and commands received from the FSK messages are loaded into the data base as flags and variable values are used later in the execution of the vehicle control laws.

Included in this data input frame is the reading of the non-latched discrete sensors which are processed later.

#### 3.4.3.2.4 Frame Two - Longitudinal Control

The interpreting of the FSK message commands, vehicle speed and position data, and guideway sensor data via the vehicle control laws enables the generation of brake and motor torque signals for the longitudinal control of the vehicle. Frame two is composed of the Command Module, Speed and Position Controller, and the Signal Conditioning function.

##### 3.4.3.2.4.1 Command Module Function

The command module function performs the following tasks:

1. Calculate the jerk and acceleration limited position, speed and acceleration commanded profiles.
2. Calculate the speed and incremental position commands during normal operation, station stopping, and emergency stopping modes of operation.
3. Generate position dependent station stop speed commands, forced brake signal, and motor on/off commands.

4. Maintain longitudinal vehicle motion within specified performance limits.

#### 3.4.3.2.4.2 Speed and Position Controller Function

The Speed and Position Controller Function performs the following functions:

1. Compute speed and position errors based on command and measurement inputs.
2. Monitor speed error and generate a fault signal if its magnitude exceeds 2.0 fps.
3. Generate a single brake/motor torque command that is a weighted sum of the computed speed and position errors and the jerk and acceleration limited acceleration command.

#### 3.4.3.2.4.3 Signal Conditioning Function

The Signal Conditioning Function performs the following tasks:

1. Filter the input torque command and limit the rate of change of the filtered command.
2. Generate scaled motor and brake torque commands from the single point limited torque command and provide biasing and command shaping as required to compensate for motor and brake nonlinearities.

#### 3.4.3.2.5 Frame Three - Safety Assurance

In this frame the following tasks are performed:

1. overspeed detection
2. predispatch checks

3. additional odometer checks
4. closed-loop emergency stop profile check
5. cross channel disparity check of vehicle control command data

#### 3.4.3.2.5.1 Overspeed Detection

The overspeed detection function compares the measured speed to the FSK commanded speed limit. This comparison allows for a profiled transition from a higher speed limit when a new lower speed limit is commanded. A violation of the speed limit results in a command to start a closed-loop emergency stop.

#### 3.4.3.2.5.2 Predispatch Checks

The Predispatch test at present is limited to a check of the Safe-to-Proceed devices from end-to-end. In event of failure, commands to dispatch are ignored.

#### 3.4.3.2.5.3 Missing and Extra Pulse Checks

The odometer preprocessors contain logic intended to detect missing and extra pulses in the pulse train coming from the sensor on the wheels. Information relating to these anomalies is passed to the main controllers at this point for processing.

#### 3.4.3.2.5.4 Closed-Loop Emergency Stop Profile Check

Under certain emergency conditions the vehicle is brought to a stop under the control of the software. This emergency software is designed to profile the vehicle speed and position for stopping within a safe distance while minimizing the hazards of excessive jerk and deceleration rates. While such an emergency stop is under way, logic within the safety assurance minor frame monitors the stopping profile of both the speed and position. If at any time the speed or position of the vehicle fall outside the profile required for stopping within the required



distance, the software control of the emergency stop is abandoned and an open-loop emergency stop is initiated.

#### 3.4.3.2.5.5 Cross Channel Disparity Check of Vehicle Control Command Data

The monitoring of redundant processing referred to in section 3.4.2.2 is implemented in software as a bit by bit comparison of the vital data exchanged cross channel in frame three.

#### 3.4.3.2.6 Frame Four

During Frame 4, the following tasks are executed:

1. Steering commands and steering status are processed.
2. Door commands and door status are processed.
3. Brake, motor and propulsion link status is monitored.
4. Internal status discretes are read and processed.
5. Detected faults are reported.
6. Downlinking of non-fault FSK messages to the wayside is managed.
7. Test point communication is managed. As an aid for control system study, the main processor has the capability to output to special ports up to eight variable values every major frame.
8. The rate of background testing is monitored.
9. The mechanisms for detecting spurious punch-ins are read and tested.
10. All of the redundant logic for safety critical vehicle control code is run to check the correct operation of the primary control logic. (A-B checks)

#### 3.4.3.2.6.1 Fault Reporting

Related to safety assurance is the process of reporting anomalies. Faults detected on board are categorized according to the response of the control systems. The highest, category 6, is restricted to exits.

not closed. If any vehicle door is open when it should be closed, the door fault is immediately downlinked in a fault summary message three times to alert the wayside operator of the potential of passengers exiting to the guideway. If the doors are opened while the vehicle is moving, the reaction also commands the vehicle to immediately initiate a normal rate stop.

The next category of faults, category 5, indicates the control system is unable to safely control the vehicle. Any detected loss of vital sensor data or failure of processing hardware would require an open-loop emergency stop. This is achieved by clearing the "punch-in key" which results in a withholding of the punch-in required to hold off the emergency brakes.

Category 4 faults are those that require a closed-loop emergency stop and refusal to accept further dispatch commands. These faults do not indicate insanity of the control system, but do indicate a potentially unsafe vehicle status such as low hydraulic or brake pressure, certain single odometer faults, or steering anomalies. One special category 4 fault is the loss of safe-to-proceed. If the FSK communication link with the wayside is broken, the vehicle does a closed-loop emergency stop. However, if a subsequent dispatch message is received after the vehicle is stopped, it will be accepted. (The vehicle will not restart unless the fault has cleared.)

Category 3 faults cause normal rate stops that result in a full stop. These faults are not considered potentially unsafe, but could lead to unsafe conditions. These would include brake overtemperature, motor overtorque, excessive invalid messages, and motor signal processing anomalies.

Category 2 faults initiate normal rate stops that need not go to completion if the detected fault disappears. These include a temporary loss of power through the vehicle power collector and a wheel spin.

The last category of faults, 1, are those which indicate a need for vehicle maintenance. These faults are recorded and reported, but do not cause any change in vehicle control.

Each individual fault reported is entered only once on the fault queue. If the category of the detected fault is higher than any category of fault already on the stored fault queue, a fault summary message of all existing fault categories in the list is down loaded to the wayside operator. If the operator wants to know what the specific faults are, he can request the transmission of the entire fault queue. When the fault queue is downlinked to the wayside, the fault titles are sent in the order in which the faults were detected.

#### 3.4.3.2.6.2 Downlinking of FSK Messages

There are five messages that are managed differently from fault queue messages:

1. Fault summary messages, which contain only the fault category
2. Destination reports, which includes a vehicle load indicator

NOTE: The vehicle load indicator tells whether a vehicle is traveling with a load of passengers or simply is in transit to balance fleet distribution. This indicator is determined by a message sent to the vehicle from the wayside.

3. Odometer report: position within a guideway FSK loop boundary
4. Door status: open/closed, right/left
5. Control status: stopped/moving, predispach checked

These messages are pushed onto a downlink queue for dispatching to the communication processor as the mail box to the communications processor is available. Fault queue content messages are managed separately at a lower priority, i.e., if the mail box to the communications processor is not being used for one of the five messages above, a fault queue message is passed as required.

Only one of the two communication processors is connected to the transmitter; the processor selection is determined by the non-prime main processor. Normally the communication processor associated with the prime main processor has the transmitter. However, if the prime main processor or its associated communication processor fails the non prime main processor switches the transmitter to its own associated communication processor.

#### 3.4.3.2.7 Duty Cycle Monitoring

The tasks assigned to each of the minor frames of the major frame cycle must complete within ten milliseconds. The tasks described in the paragraphs above have been measured and found to require the following times:

Frame 1 - Runs in 5 to 7 milliseconds depending on FSK messages to be processed, magnetic signaling to process, and whether the vehicle is calibrating its odometers.

Frame 2 - Runs in 2 to 2.3 milliseconds

Frame 3 - 1.4 to 1.6 milliseconds

Frame 4 - 3.8 milliseconds

Hence, all the tasks assigned a major frame take from 12.2 to 14.7 milliseconds out of an available 40 milliseconds. This leaves 25.3 milliseconds for executive overhead and background self testing. Any minor frame that might not complete its assigned task in ten milliseconds would be interrupted. A nesting of tasks is not permitted. A failure to complete would be detected and result in a category 5 fault and the shutdown of the control system.

### 3.4.3.3 Background Self Checking

The checking of the processing hardware described in section 3.4.2.4 is done during the time between the end of one minor frame set of tasks and the start of another. This time is referred to as background time, but is not completely unstructured.

The requirements for punch-in are restricting; the time from which an interrupt occurs to the time the software must send a pulse to the emergency brake holdoff is 28 microseconds + or - 2 microseconds. When the interrupt is received, any instruction being processed must be completed. Because the timing requirements are so tight, no long instructions could be completed in time to allow punch-in within that narrow time window. As a result, no background test is allowed to be done near the time an interrupt is expected.

The background tests are broken up into thirty tests. Each of the tests is design to run in one millisecond or less. Before any one of these tests is called, a check is made of a flag that indicates an interrupt is expected within the next one millisecond. If that flag is true, no further background testing is done in that minor frame; the processor merely waits for the interrupt. If the flag is false, however, another one of the self tests is called.

Tests indicate the average time required to do one background test is 0.42 milliseconds. This allows each of the self tests to be called approximately twice every major frame. At that rate the complete random access memory (RAM) is checked every 2 seconds and the complete read only memory (ROM) is checked every 9.1 seconds.

The data used in several of the background self tests affects data used in other background self tests. For this reason certain tests cannot be conducted in both redundant channels at the same time. The indices that track which test is next to run in background in the two channels are deliberately maintained roughly fifteen tests apart.

#### 3.4.4 Communication Processor Software

Unlike the main processor, which executes tasks on a scheduled forty millisecond cycle, the communication processor mainly responds to externally initiated interrupts. There are self checks and polling/posting tasks that are done on a continuing basis while waiting for interrupts.

The self tests are the same ones done by the main processor for checking the RAM and ROM hardware and the CPU register and flags. The polling tasks are a periodic check of the memory shared with the main processor for messages to transmit to the wayside. There are two posting tasks. One is a periodic setting of a flag in the shared memory to tell the main processor that the communication processor is still working. The other is a periodic check and reload of the vehicle's identification number from a set of rocker switches on the circuit board.

Interrupts can come from two sources:

1. One of the two receivers (only the forward receiver is serviced normally, the aft receiver interrupts are ignored)
2. The transmitter

The receiver sends an interrupt every time it gets a confirmed bit signal from the wayside FSK transmitter. These come every 800 microseconds as long as messages are sent. The service logic for that interrupt reads the bit from the receiver. The bit comes with an additional flag to indicate whether it is the first bit of a message.

The first 32 bits are message content that is passed to the main processor. The last 16 bits form a cyclic redundancy check (CRC) used by the communication processor to determine if the first 32 bits were received without error. From receipt of the first bit of a message to the last bit of the CRC, the communication processor tracks the 48 consecutive interrupts. If the count and CRC check are correct, the message content is then checked for type. If the command field of the

message contains a command that requires a vehicle ID match to determine whether the vehicle should accept the command, the communication processor compares the number in the data field with the vehicle ID and raises a flag in the shared memory to tell the main processor it has specific mail.

All messages that pass the bit count and CRC requirement are posted to the shared memory and a flag is raised to indicate the availability of the messages.

If the main processor posts a message for downlinking, the communication processor moves the message to its downlink buffer, adds the vehicle ID, and turns on the transmitter. The transmitter in turn sends interrupts every 800 microseconds to the communications processor. The interrupts are serviced by posting to the transmitter one bit of the message to downlink. As with the uplink messages, the downlink messages have a 32 bit content format with a 16 bit CRC. After the last bit of the message is sent, the downlink buffer is checked for further messages. If none are indicated, the transmitter is turned off.

### 3.5 Considerations in the Design of the Software

The constraints on the software that drove the selection of software implementation techniques can be categorized as follows:

- 1) Safety
- 2) Performance
- 3) Operability
- 4) Testability
- 5) Maintainability

cause of the research nature of the project and the need to demonstrate the safety of the system. Maintainability is intended to facilitate adjustments to the software that are identifiable in scope of effect and simple to achieve. These considerations will be addressed in a dis-

cussion of the rationale for selection of each of the following elements:

- 1) The Executive
- 2) Fixed Point Computation
- 3) Language Selection
- 4) Dissimilar Software
- 5) Code Exercisers
- 6) Process Monitoring: Test Points and Fault Reporting
- 7) Single Thread FSK Command Processing

#### 3.5.1 The Executive

The tasks required for the operation of the vehicle are either responses to events or iteration steps in the execution of control laws.

The events requiring action include:

- 1) Reception of FSK messages
- 2) Detection of guideway magnets
- 3) Loss of safe-to-proceed
- 4) Detection of changes of vehicle status

Cyclic tasks requiring accurate time scheduling:

- 1) Speed and position measurement update
- 2) Speed and position command update
- 3) Brake and motor torque command update
- 4) Exchange of data between redundant processes and processors

Cyclic tasks that do not require high priority scheduling are self tests, unrelated to real time control.

To schedule tasks that must be synchronized with tasks done in a redundant processor requires an executive that contains a protocol to coordi-



nate that scheduling with the other processor. The simplest approach is to have these tasks scheduled in response to an external interrupt sent to both channels from an external clock.

The remaining events then would have to be scheduled on a lower priority. These, however, must also be synchronized cross channel to allow coordination of input used in the execution of the cyclic control laws.

The cycle time required for the control laws is 40 milliseconds. The response to an event that would occur during execution of control logic would be delayed until the control logic was completed. It was found that for accuracy reasons in the case of guideway magnet detection, and for safety reasons in the case of loss of safe-to-proceed, delays should not exceed ten milliseconds.

A multitasking executive with complex scheduling priority schemes and a table of event vectors would do the job; however, it would be expensive to build and very expensive to demonstrate as safe. Analysis showed that a forty millisecond cycle allowed ample time to poll all event sensors and respond as required. For those events requiring minimum delays of less than forty milliseconds, their respective sensors could be polled every ten milliseconds. We therefore chose a cyclic executive. An interrupt every ten milliseconds results in:

- 1) A reassertion of the emergency brake hold-off and motor enable command if the "punch-in" key is intact
- 2) A reading of each wheel odometer and latched event discrete
- 3) Execution of one of four major control or safety tasks

The time between the completion of the tasks listed above and the next interrupt is referred to as background time. During this background time a series of low priority self tests are executed.

The simplicity of this approach allowed full analysis of failure modes, detection schemes, and reactions to such failure modes.

The drawback to such a scheme was that events with low priority were scheduled with the same polling frequency as all other forty millisecond tasks. Care was required to make sure any task initiated during any ten millisecond frame was completed before the next ten millisecond interrupt occurred.

The simplicity of the selected executive reduced the number of tests required to verify the safety of the executive.

Maintenance considerations included care to balance the loading of the ten millisecond frames.

### 3.5.2 Fixed Point Computation

The driving force in the selection of fixed point computation in the software design was speed of execution and the need to control the accuracy of results.

Fixed point computation requires great care in the selection of the number of significant digits; accuracy must be considered as well as range. The control and coordination of the scaling factors adds to design overhead. The range of values for variables is more restricted. The main advantage of fixed point over floating point is constant knowledge of the accuracy of results.

Testing was made simpler because data base reading in fixed point is easier. Maintenance of the software is made more complex because of the need to constantly consider scaling issues in code design.

### 3.5.3 Coding Language Selection

Under conditions where time and space efficiency is important, assembler language is often used. The problem with assembler is that it requires management of code overhead, whereas High Order Language (HOL) compilers do this automatically. These overhead considerations are often sources of error in code written in assembler. HOL code is easier to read, analyze, and maintain.

On the other hand, Vehicle Control code often requires manipulations that are harder to write in a high order language. Unless the language supports a symbolic debugger, code testing must be done using the assembler produced by the compiler; this adds an extra phase of code analysis.

The driving force in the choice between assembler and HOL for the main processor code was ease of analysis. Safety required verifiability. This is easier in a high order language. The language selected was "C". "C" is considered among high order languages to be fairly low order. It is a loosely typed language that provides many features to allow bit level manipulations.

#### 3.5.4 Dissimilar Software

The most common implementation of dissimilar software is as two alternate logic paths used to generate the same output. The logic in the separate paths is supposed to be dissimilar enough to contain no common mode errors. If both paths produce the same output, the output is assumed correct and therefore safe. If they differ by a sufficient margin, one or both of the paths is assumed to be defective. There are many schemes which respond to detection of defective output. If the response is to initiate recovery in an attempt to continue operation, the restrictions on the coding are great. The use of dissimilar software in the AGRT applications is solely to detect errors. The response to errors is to declare insanity and stop processing control laws, i.e., stop on open-loop brakes.

The design in the AGRT application emphasized dissimilarity. The first of two alternate paths, the "A" algorithm, was designed to satisfy the accuracy requirement of the control laws. The second path, the "B" algorithm, generated only an approximate value used to check the sanity of the "A" algorithm's output. Freedom from strict accuracy requirements allowed the "B" algorithm to use alternate input data or to use the same input in a different manner to generate a window into which the

"A" algorithm output had to fall to be considered correct. Using this approach to distinct code generation obviated the need to use different languages for the two logic paths. There would be no advantage to different languages, save avoiding the possibility of common mode compiler errors. (Module testing checked for compiler errors.) The forcing of great differences in the two logic paths required the same teams to produce both. The one disadvantage to this is the possibility that any erroneous biases in the interpretations of the specification might be found in both paths.

In the AGRT application the "B" logic is executed widely separated in time from the execution of the primary logic. This separation diminishes the probability that any transient effect could disturb both operations.

The disparity detector for the results of the two dissimilar algorithms is part of the "B" algorithm code module. The response to detected disparities is destruction of the punch-in key.

We recognize that the value of dissimilar software is often debated. There is not a procedural way to generate dissimilar software; almost every case is ad hoc and expensive in terms of the analysis required to make it both effective and reliable. There is no way to prove that there are no common mode failures possible in the two logic paths. There is a non-negligible probability of the secondary logic false alarming the systems and degrading reliability. Testing the secondary logic is difficult because the code is designed to not allow disparities between the two paths. Maintenance is complicated because a disturbance to the primary logic more than likely requires an adjustment to the secondary logic. But dissimilar software provides the assurance needed to minimize the probability of undetected errors.

#### 3.5.5 Code Exercisers

The mechanics of implementing emergency code exercisers introduce more cross coupling of code. Any changes made to safety critical code, which

is exercised in background, require that the code exerciser be checked and modified. In addition, any change to variables used in safety critical code in the redundant channel must be coordinated with the code exercising sequence to prevent false alarms caused by mismeshed readings of variable values in flux. Both primary and secondary paths of dissimilar software are exercised in background. The resulting four dimensional maintenance considerations are real problems that, from software engineering principles, could prevent the wide use of code exercisers in this type of software.

The testing of exercisers cannot be done in the final code configuration because their failure is dependent on failure of code processing hardware. The failures the exercisers were intended to detect were simulated by a special driver, and the code was tested in isolation from the target system.

A failure of any background self test results in a cessation of punch-in. Rather than just reset the punch-in key in software when a failure is detected, a different technique was used. Because it is the code processing hardware itself which is under test, the response to the failure results in halting of the processor itself. Only a reset of the system initiated by an FSK message received by the redundant processor, or pressing of the reset button on the card cage, or a power recycle will bring the halted processor back up. Upon reset all of the background tests are executed. If the failure occurs again, the processor halts again.

The source of the failure can be found by asserting the monitor request button and hitting reset again. Non-volatile RAM is loaded with the test number before a test is executed and cleared only after successful completion. The monitor program in the failed channel can be used to examine the failed test indicator, thus displaying the number of the failed test.

The design of the code exercisers requires that safety critical variables be skewed to indicate an unsafe state. This skewing is done by modifying real data, which is changing dynamically under process control use, in such a way as to make it indicate an unsafe condition. Calculation of this amount by which to skew must consider worst case margins. Poor analysis in the establishment of these margins could result in reduced reliability of the system due to false alarming.

#### 3.5.6 Process Monitoring: Test Points and Fault Reporting

There are 87 different faults that can be reported to the wayside about conditions within the main processor. Three of them are generated by the communications processor and relate to unresponsiveness of the main processor. One from the main processor relates to the state of the fault queue. The remaining 83 are stored on the fault queue for transmission to the wayside on request; this design was invaluable in testing and was found to be very reliable.

For analysis of the internal dynamics of the control system, the current value of each of a set of eight different variables (within each channel) is passed to an external port. Hence, a stream of 16 variable values, output every 40 milliseconds, is available externally. Variable sets to be output are switch selectable from up to 100 combinations. Chart recordings and decimal lists of these values with associated time tags provided data for analysis and confident test evaluation.

#### 3.5.7 Single Thread FSK Command Processing

The command portion of messages received by the acting primary channel is processed by both channels. A failure of the prime channel's communication processor would result in loss of communications. Because this method of redundant input management reduces the input to single string, a fault recovery mechanism was introduced to keep communication open. (This represents the only fault recovery code in the system.)

Each channel monitors the keep alive signal from the other channel's communication processor. If it fails, the channel with the surviving communication channel takes over the role of prime channel message posting and message transmitting. Because the FSK transmitted speed limit is safety critical, any increase in the speed limit received by the vehicle running under a single communication processor is ignored. Any decrease in speed limit is accepted and enforced by both channels.

In the event of a failure that causes the vehicle to stop open-loop, the two channels are separated and each channel processes its own FSK up-linked commands.

### 3.5.8 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 affect 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.

## 4.0

## DETAILED HARDWARE DESIGN DESCRIPTION

Having completed the design overview, a more detailed description of the VCU hardware elements follows. This includes the vehicle communications and the VCU hardware.

### 4.1 Wayside/Vehicle Communications Elements

The vehicle, as it travels down the guideway, must remain in contact with the AGRT control hierarchy. The vehicle does this by communicating with the Guideway Communications Unit (GCU). As shown in Figure 4.1-1, the vehicle communication elements consist of the Inductive Communication Subsystem (ICS) and the Magnetic Communications Subsystem.

Much of the AGRT inductive communications and magnetic communications design is based on the experience gained from the MPM design. Documentation on the MPM design is available in an NTIS Report, number UMTA-MA-06-0048-78-6, titled "Morgantown People Mover Inductive Communications System Design Summary."

Detailed documentation of the AGRT GCU design is available in NTIS Report, number UMTA-WA-06-011-84-1, titled "Advanced Group Rapid Transit Guideway Communication Unit Design Summary."

#### 4.1.1 Inductive Communications

The ICS uses the inductively coupled link between the guideway and the vehicle over 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 which couple inductively with rectangular coil antennas mounted to the underside of the vehicle. The loops and antennas provide both the uplink (station to vehicle) and the downlink (vehicle to station) communications. Each guideway segment, which can be as long as 1000 feet in length, contains a pair of these inductive loops. One loop is located in the right half of the guideway for uplinks; a similar loop is located in the left half for downlinks.



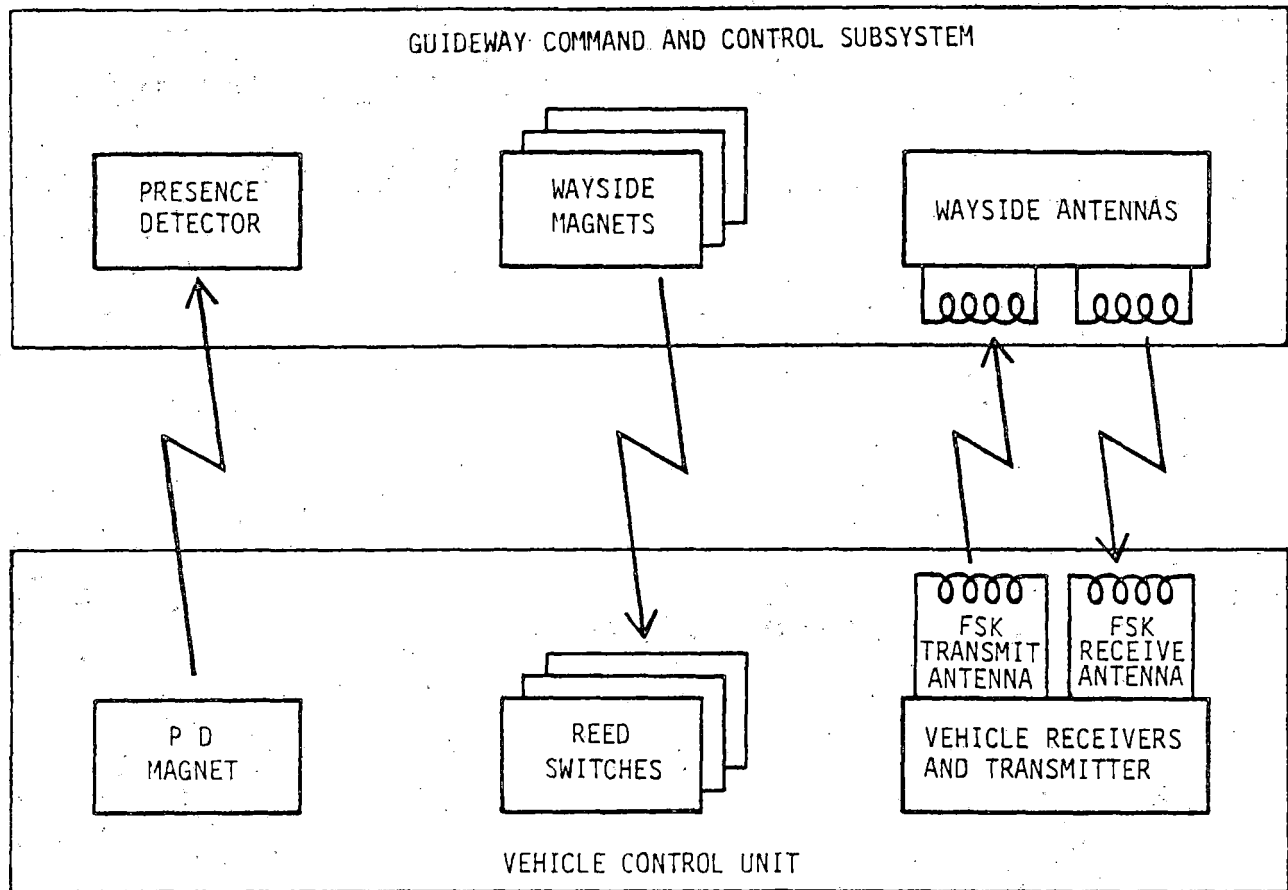


FIGURE 4.1-1: WAYSIDE/VEHICLE COMMUNICATIONS ELEMENTS

Susceptibility of the loops and antennas to vehicle generated noise was a concern in the design of a reliable communication link. Past data taken on the Morgantown People Mover System and the Seattle Metro Trolley show sinusoidal interference and Gaussian noise to be negligible; however, impulse noise, from 1) the chopper controlled propulsion unit on board the vehicle and 2) the contact bounce of the power collectors, is very severe. Cases were even observed where the signal to noise ratio fell as low as 0 dB. Due to the importance of meeting the bit error rate requirement of  $10^{-5}$  errors/bit in such an environment, much time and effort was spent in the development of a suitable receiver. From these efforts emerged the design of a digital receiver, implemented with a microprocessor, capable of operation in a high impulse noise environment.

The uplink and downlink modulation method is binary Frequency Shift Keying (FSK). The four frequencies used are near 100 KHz. The uplink message is 50 bits in length and encoded in a bi-polar return to zero format (see Figure 3.1.1.1-1). The upper FSK carrier frequency ( $f_u = 110.34$  KHz) represents data "1" and the lower ( $f_l = 108.84$  KHz) represents data "0". During the second half of each bit time, the carrier frequency is shut off. In addition, the FSK carrier is interrupted during the first two bit times to mark the beginning of each message.

The AGRT system has a message transmission rate of one message every 40 milliseconds. A complete message is 48 bits in length with two missing bits to mark the start; thus, a message is 50 bits total. This establishes a bit length of 800 microseconds, and a bit rate of 1250 bits per second.

Early in the program a complete end-to-end inductive communications link was assembled and tested in the laboratory, demonstrating a viable design approach to the vehicle/wayside communications. Included in the demonstration was the transmission and recovery of a safe-to-proceed clock signal, a speed limit command, and a field of variable data.

The primary purpose of the demonstration was to test the ability of the link, particularly the digital receiver, to perform in the presence of noise. To this end, the link was subjected to impulse noise modeled from data collected at Morgantown, the Surface Transportation Test Facility (STTF), and the Seattle Metro installation. The layout for the Inductive Communications Demonstration is shown in Figure 4.1.1-1.

Referring to the figure, the FSK message originates in the Z8002 Development Module. (The Development Module is a general purpose hardware/software development tool consisting of a Z8002 microprocessor, memory, prestored monitor program, and I/O ports.) A CRT terminal allows an operator to enter a message for transmission; this message is then passed to the Communications Processor. The complete message is clocked out serially to the modulator. Timing pulses necessary for the serial data transfer and recognition of the beginning of new messages are provided by the data clock and frame clock signals from the Clock Module. The data clock toggles the modulator "carrier enable" input, producing the safe-to-proceed clock. The FSK modulator output is amplified in the Loop Driver and applied to the Guideway Loop. The transmitted signal is inductively coupled into the Receive Antenna and applied to the Digital Receiver for detection.

A second loop antenna couples the noise signal from the Impulse Noise Generator into the receiver. Results of this testing indicate that the Digital FSK Receiver, using the digital discrimination technique, is highly insensitive to the noise environment created for the test. The test disclosed, as predicted, that the Digital Receiver is not sensitive to the amplitude of the impulse noise, but is more sensitive to the number of impulses that occur per bit time.

We know from the demodulation scheme used that the receiver will not perform as well in an environment where significant sinusoidal interference is present. Tests were run to determine the ability of the receiver to operate in the presence of an interfering sinusoid. The Digital Receiver threshold (the level at which the receiver can accurately decode FSK signals) was adjusted to -50 dBV RMS (3 dB below the

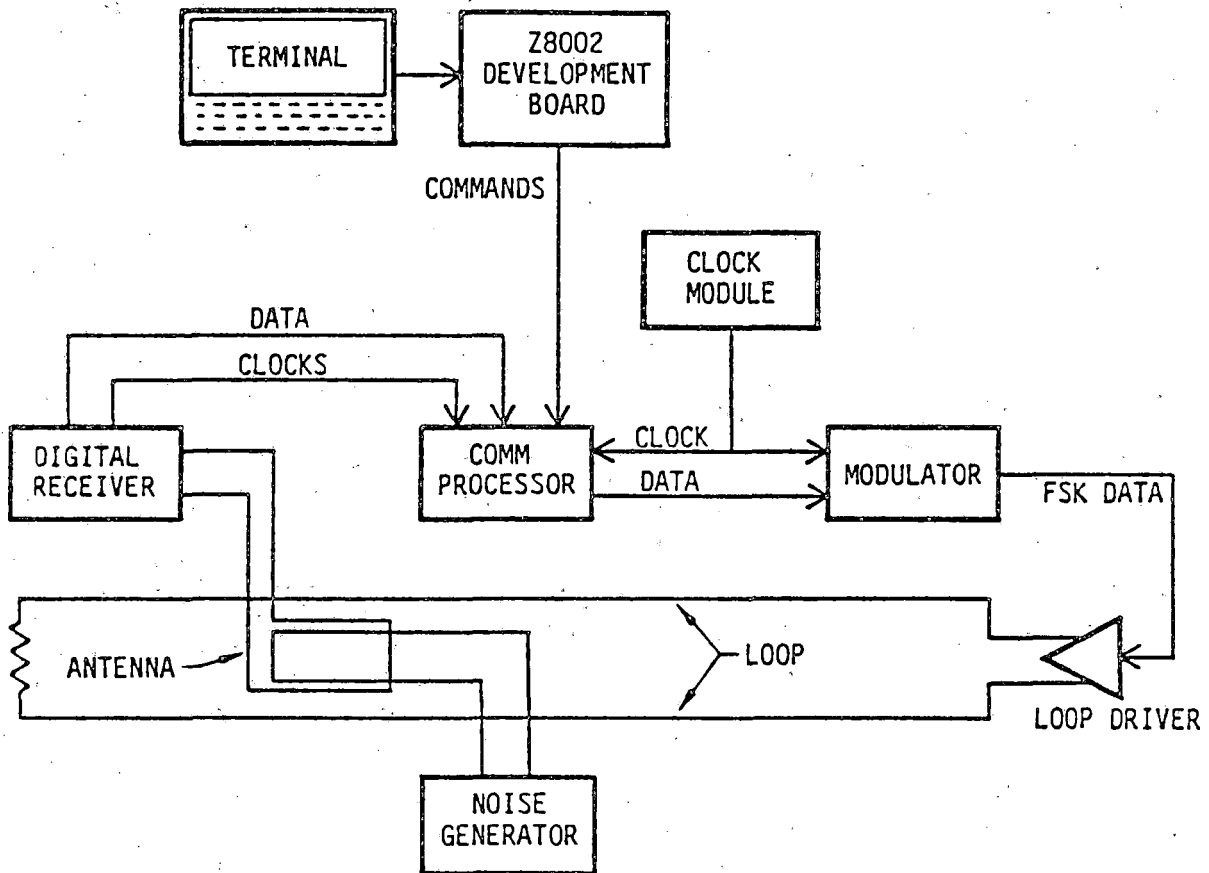


FIGURE 4.1.1-1: INDUCTIVE COMMUNICATIONS DEMONSTRATION CONFIGURATION

operating level, -47 dBV RMS) and a steady tone was coupled into the receive antenna using a summing amplifier to sum the FSK carrier and the interfering sinusoid. The level of the interfering signal was increased until a threshold was reached where errors began to occur. The results of these tests are shown in Figure 4.1.1-2. It can be seen from this graph that the Digital FSK Receiver has a rather wide interference bandwidth for sinusoids. However, high level sinusoids, other than 60 Hz, are not expected. If it should be required, a 60 Hz notch filter can easily be included in the design.

#### 4.1.1.1 Uplink

The FSK uplink consists of the two antennas, mounted on the underside of the vehicle, each connected to a Digital Receiver. The antennas are called the forward antenna and the rear antenna. The vehicle electronics always utilizes data which is received on the forward antenna for control purposes. The information received on the rear antenna provides a communications backup in anomaly situations, but more importantly it ensures a continuous STP signal at FSK wayside loop boundaries. The uplink vehicle antenna is based on the MPM design which is 22 turns of wire on a rectangular bobbin.

##### 4.1.1.1.1 FSK Digital Receiver

Previous FSK receiver designs have utilized analog bandpass filters to detect spectral energy within FSK passbands in order to demodulate FSK signals. Such designs have an inherent problem in severe impulse noise environments because impulses are composed of an infinite number of spectral components. An analog bandpass filter designed to detect FSK frequencies would detect spectral energy within its passband even when the only input to the filter is a series of pulses with Pulse Repetition Frequencies (PRF) lower than the FSK frequencies. With several impulse noise sources, all with their own pulse widths and PRF's, the spectral makeup of the signal can become quite complex. The Digital FSK Receiver minimizes the effect of this because of its unique method of frequency demodulation. As shown in Figure 4.1.1.1-1, the Digital Receiver

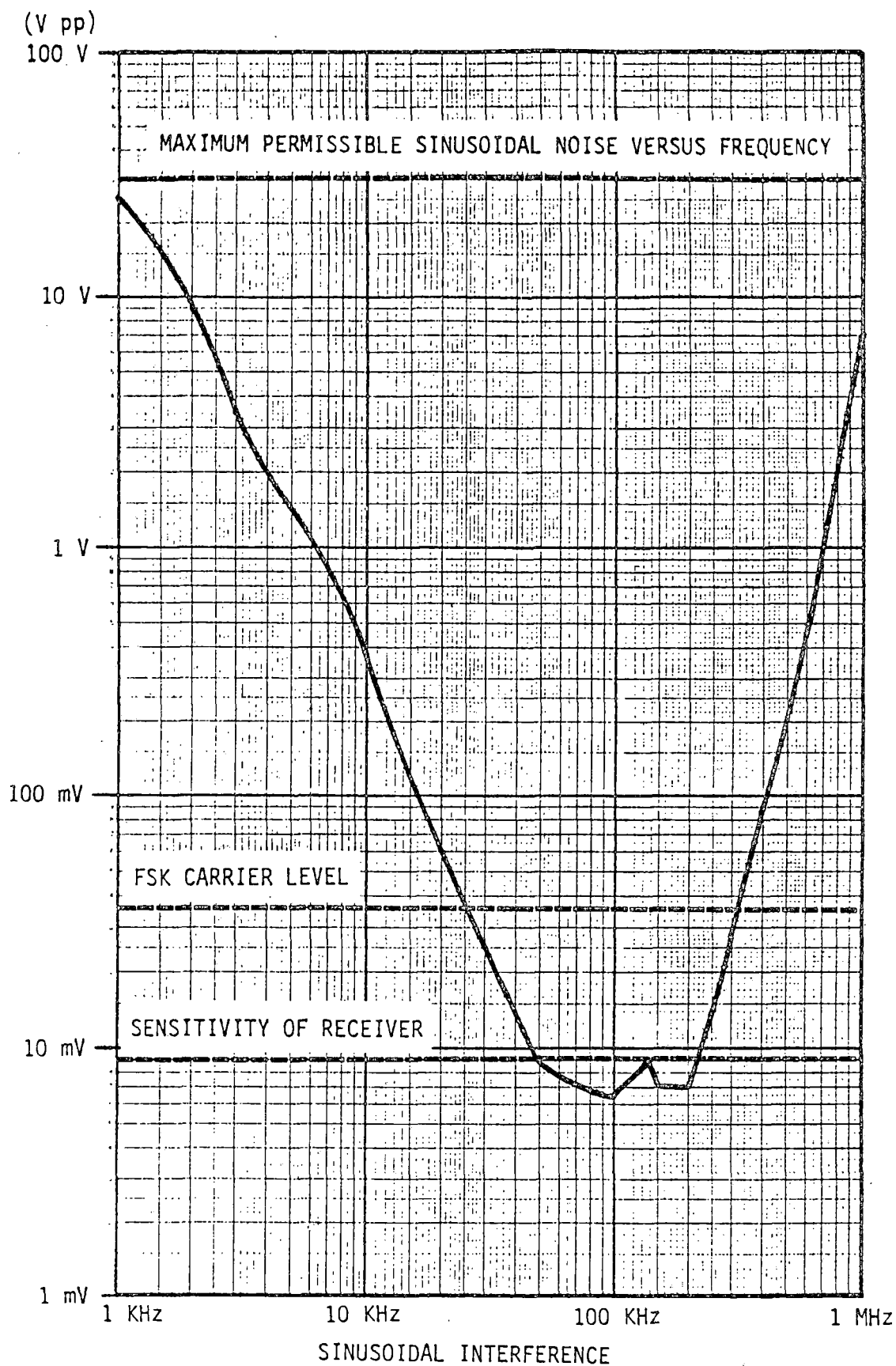
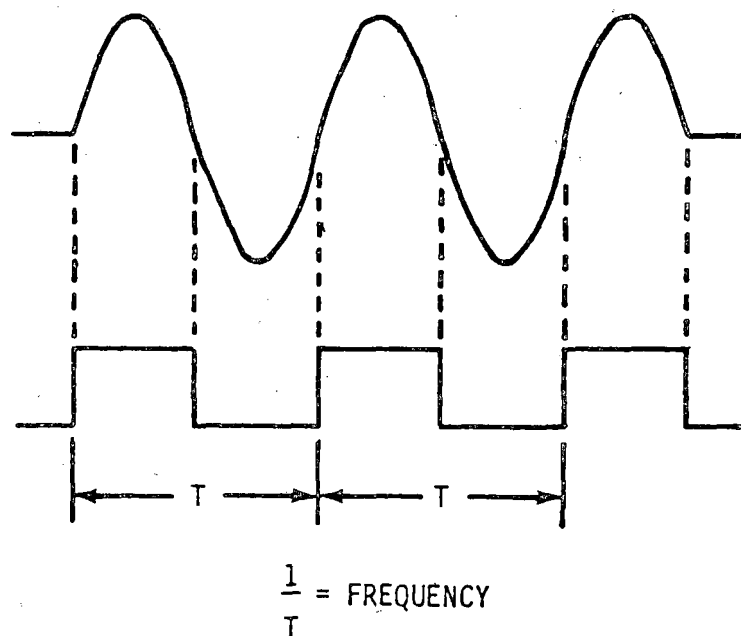


FIGURE 4.1.1-2: PLOT OF RECEIVER SENSITIVITY TO SINUSOIDALS VERSUS FREQUENCY



- After converting sinusoid to TTL square wave, the discriminator measures the period of the cycle last received. The frequency is determined based on the time measures.
- The receiver integrates the total number of frequency decisions made during each data bit transmission. The result of the integration is dumped and the data bit is set at the output at the end of the data bit transmission.

FIGURE 4.1.1.1.1-1: METHOD OF FREQUENCY DEMODULATION

measures the period of each cycle of the received uplink signal and determines the frequency of the sinusoid based on the time measured. In addition to determining frequency at the end of each cycle of received signal, the receiver digitally integrates the results of the decisions made after each cycle. This technique results in a very accurate decoding of the FSK data because the time duration of each interfering noise element is very short relative to the bit transmission time. The noise impulses are short (20 microseconds) compared to the energy portion of the bit time (400 microseconds). Since the Pulse Repetition Frequency (PRF) of the noise sources is less than 1 KHz, each source can contribute only one pulse per data bit time. Even when impulses from all four noise sources appear in one bit time, there is sufficient time for the receiver to make an accurate decision.

The purpose of the digital receiver is to decode FSK analog inputs and produce the corresponding digital code with the correct timing. The receiver consists of two sections: an analog front end and a digital demodulator. Block diagrams of these two sections are shown in Figures 4.1.1.1.1-2 and -3. The analog front end amplifies and bandpass filters low level input signals. A limiter removes amplitude variations and a threshold detector passes signals above 0.4 volts.

The digital section consists of an up counter that counts between signal zero crossings, a Programmable Array Logic (PAL) decoder that maps counter outputs to convenient jump addresses, and a microcomputer that chooses the PAL code that occurs most often and strobes out the corresponding code. Figure 4.1.1.1.1-4 is a picture of an assembled Digital Receiver Card.

#### 4.1.1.1.2 The Front End Circuit

The Front End Circuit is the interface between the analog signal received from the FSK antenna and the digital demodulator. It accepts the signals from the antenna through an instrumentation amplifier. The buffered signal is subjected to a broad preselection filter and then a hard limiter before being converted to TTL levels by a comparator at its out-



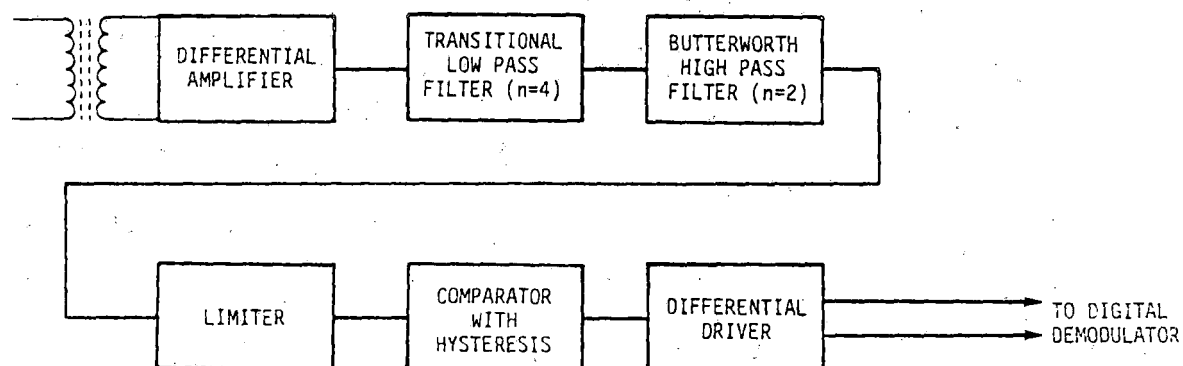


FIGURE 4.1.1.1.1-2: ANALOG FRONT END BLOCK DIAGRAM

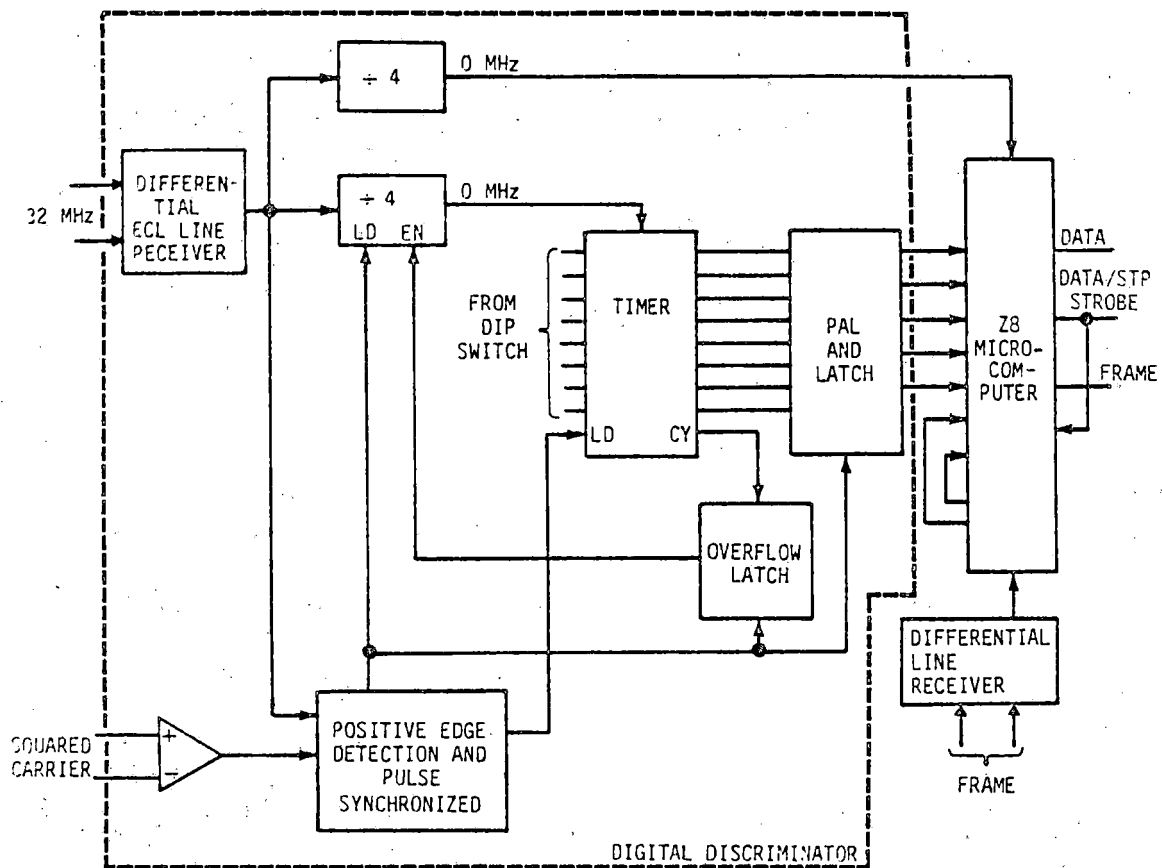


FIGURE 4.1.1.1.1-3: DIGITAL DEMODULATOR BLOCK DIAGRAM

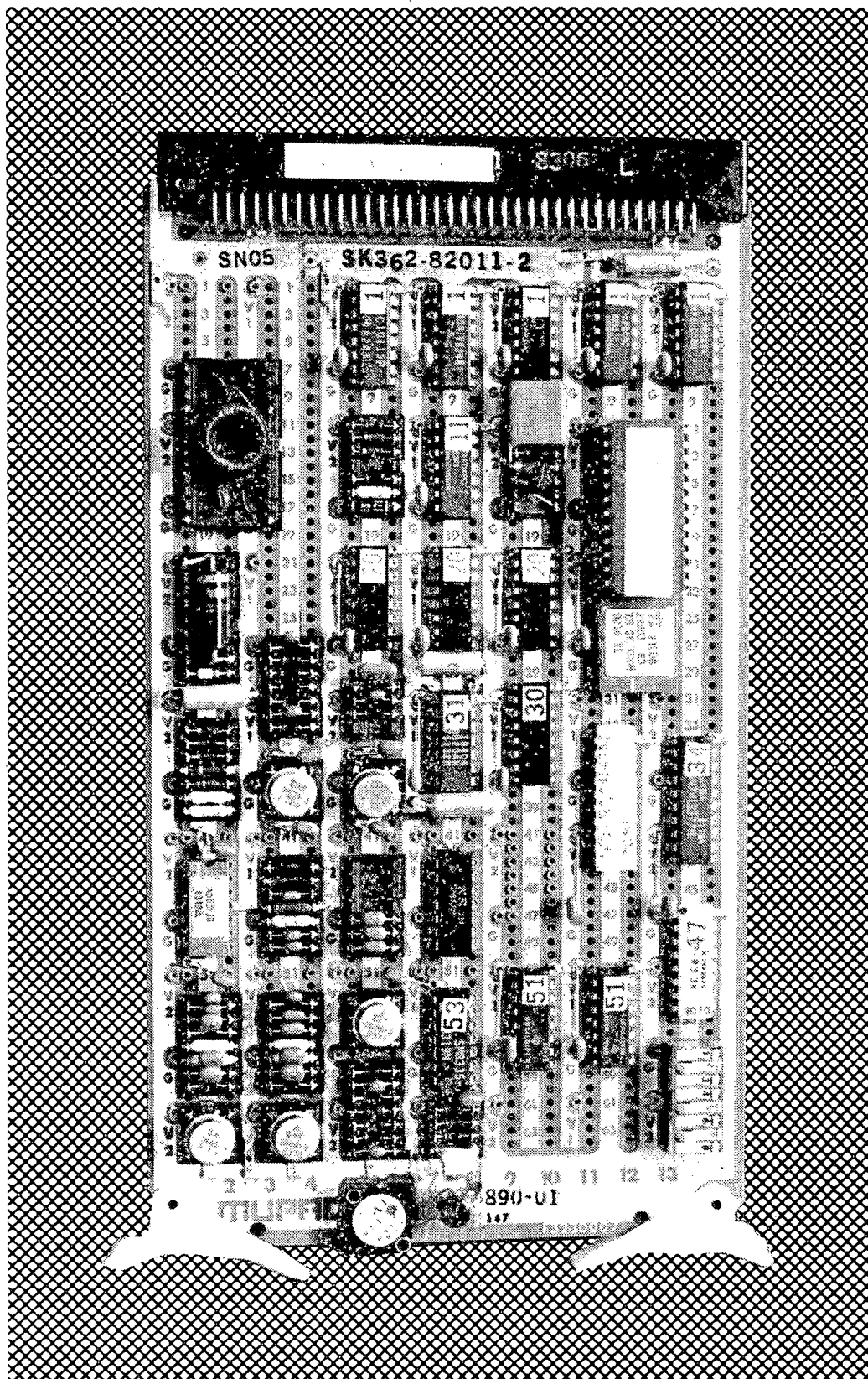


FIGURE 4.1.1.1-4: FSK DIGITAL RECEIVER CARD

put stage. The TTL compatible square wave output is delivered to the Frequency Discriminator and the Carrier Start Detector.

The design of the preselection filter required careful consideration. Due to the nature of the demodulation concept used, a problem results when one tries to filter the signal received to any great extent. To understand the problem, let us examine why the digital demodulation technique is so attractive for our application.

This concept was conceived because it was known from past experience that the major type of interference expected in our application would be very sharp impulse spikes occurring at relatively low repetition rates. Gaussian noise is expected to be negligible and sinusoidal interference is expected to be very low. In such an environment the Digital Discriminator is ideal because the major type of interference is present only during the very sharp spikes and does not interfere with the reception during an entire bit time. It is important to note here that interference, which is present during the entire bit time, such as a continuous high level sinusoid, could deteriorate the receiver performance. Power line 60 Hz interference for instance, would make the receiver inoperable if it were not somehow filtered out. (Figure 4.1.1.1.2-1 shows the effects of both types of noise.)

We know from the Fourier Theorem that any impulse is actually a sum of an infinite number of sinusoids. Subjecting such an impulse to a bandpass filter can alter the phase and amplitude relationships of these sinusoidal components and thus alter the shape of the impulse spike.

Consider then what happens when we subject such an impulse spike to a bandpass filter. As we begin eliminating spectral components by progressively making the passband narrower, rise and fall times suffer. The waveform becomes "stretched out" until eventually the filter allows but one spectral component through, a steady sinusoid. Also, even with a very broad passband, if the phase relationships between the spectral components are altered, we will experience a degradation on the settling time of the response. This too will result in extending the duration of

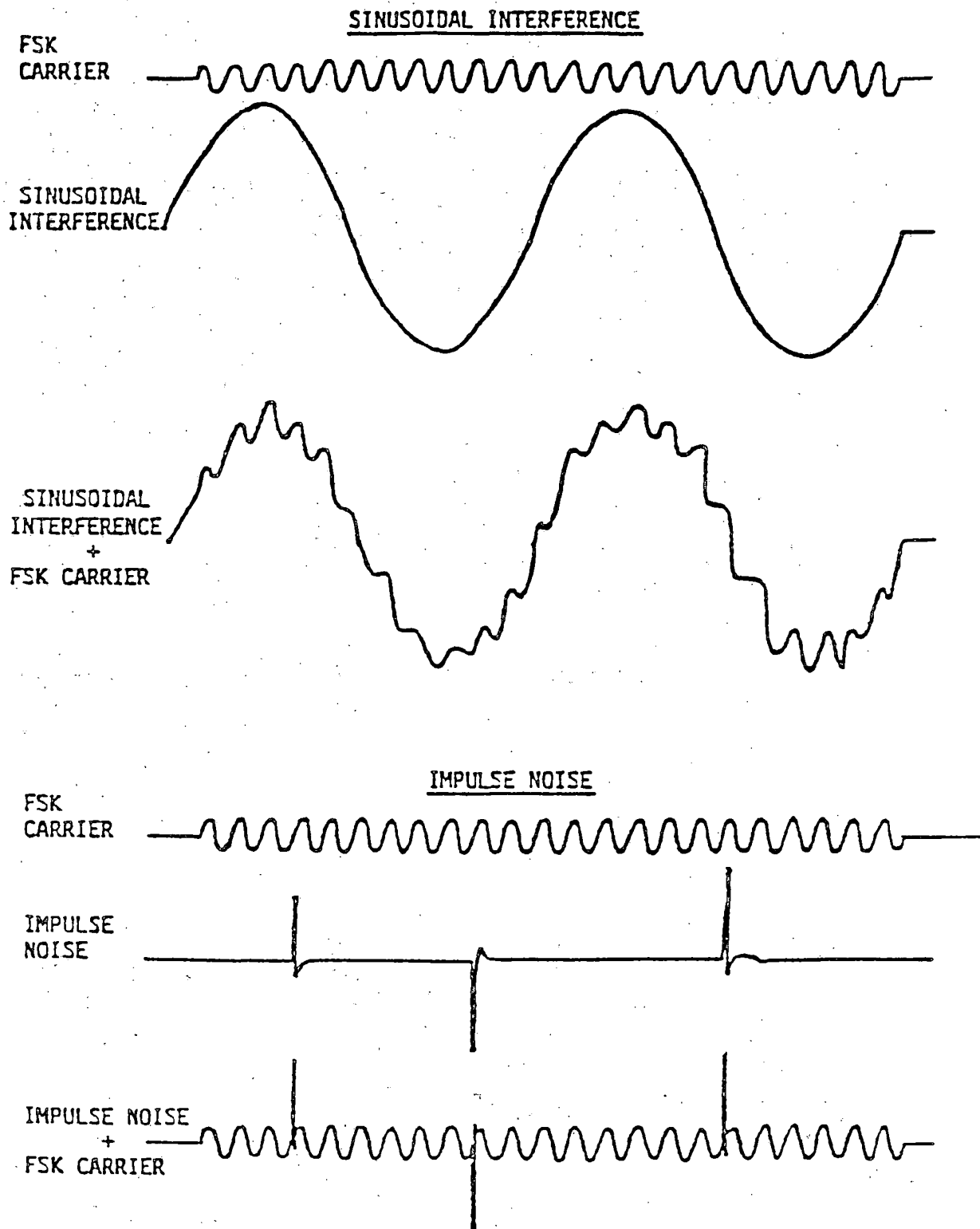


FIGURE 4.1.1.1.2-1: EFFECTS OF SINUSOIDAL INTERFERENCE AND IMPULSE NOISE

the interference caused by the impulse spike. Both phenomena pose a problem for the Digital Receiver, because the interference ceases to be a short spike which interferes with the reception for only a small fraction of the bit time.

Now the dilemma can be seen. On one hand, no band limiting is desired so that all impulse spikes can be received without stretching their short time duration. On the other hand, it would be desirable to make the passband as narrow as possible around the FSK frequencies in order to eliminate any interference from sinusoidal noise sources. This trade must be performed in order to optimize the receiver to the environment expected.

The AGRT vehicle is expected to utilize a propulsion unit similar to the unit used on the Seattle Metro electric trolley system. Tests on the Seattle Metro vehicle show that up to four independent sources contribute to the impulse noise interference. Each source generates noise at relatively low PRF's (less than 800 Hz) but due to the fact that they are not synchronous, it is possible for all of them to occur during any single bit time. It was determined from this that the filter should not be allowed to "stretch" a spike more than two FSK cycle times (about 20 microseconds).

In order to meet the above requirement, a very broad filter with maximally linear phase delay is required. This was implemented by cascading two 3-pole low pass Bessel filters with 3 dB frequencies at around 150 KHz and a differentiator with unity gain at 100 KHz.

#### 4.1.1.1.3 The Digital Discriminator

The Digital Discriminator is the heart of the Digital FSK Receiver (refer to Figure 4.1.1.1.3). The discriminator times every cycle of carrier received at the squared carrier input and determines if the period corresponded to one of the two valid frequencies. Its function is therefore to select a code which corresponds to the frequency which occurs most often. A diagram of the receiver software structure is shown in Figure 4.1.1.1.3-1.

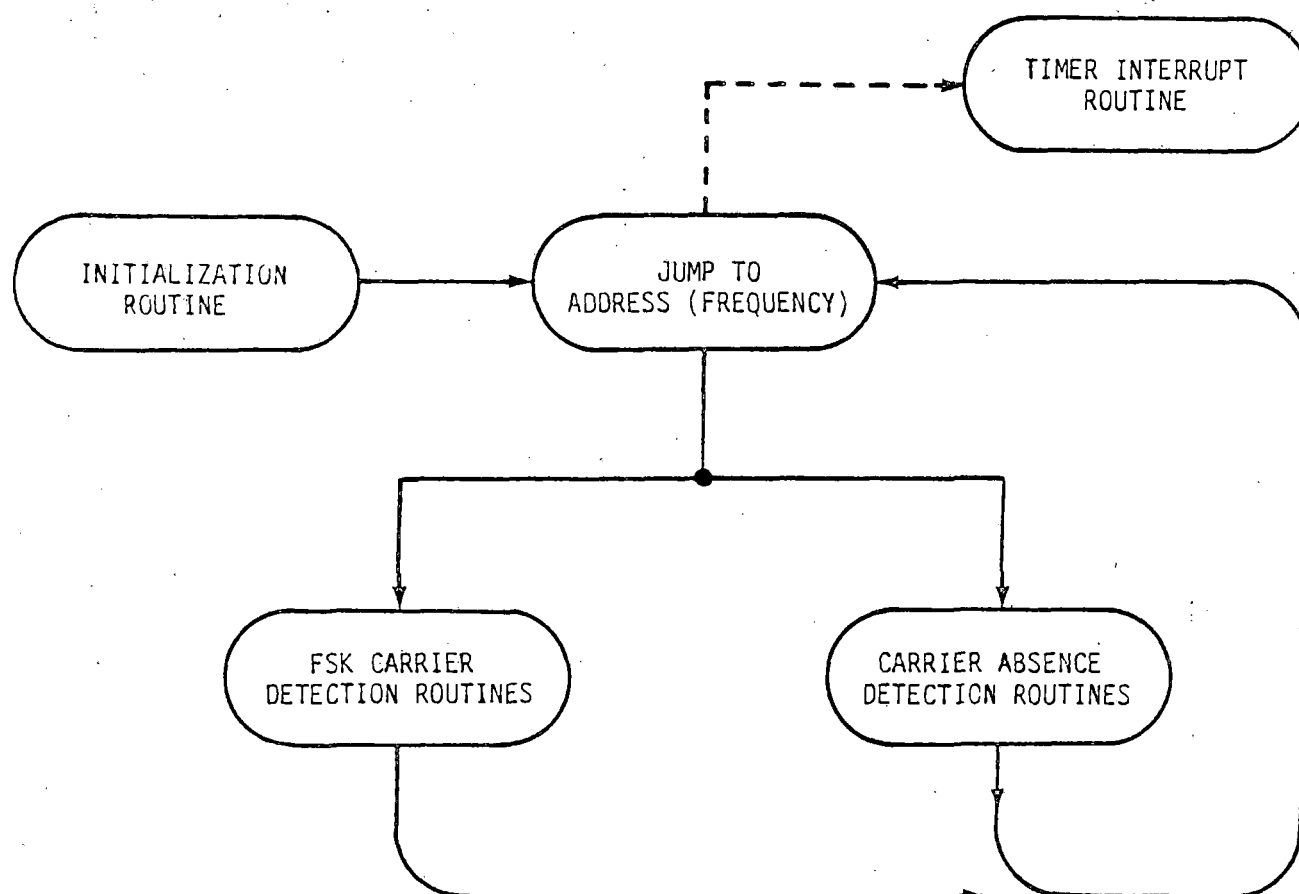


FIGURE 4.1.1.1.3-1: RECEIVER SOFTWARE STRUCTURE

#### 4.1.1.2 Downlink

The FSK downlink is as shown in Figure 4.1.1.2-1. It consists of an FSK Modulator, Antenna Driver, and a Transmitting Antenna.

##### 4.1.1.2.1 FSK Modulator

Figure 4.1.1.2.1-1 is a block diagram of the FSK Modulator. The Communications Processor provides binary data, data clock, and frame information to the Modulator. The Frequency Generation block uses the binary data and data clock to down convert a 32 MHz primary clock input into a FSK square wave frequency of 113.48 KHz for a logic "0" and 115.11 KHz for a logic "1". This square wave signal is then passed through the Digital-To-Sine-Wave Converter section where the signal becomes an analog FSK signal; the circuitry of this section is a series of low pass filters. The last block is an output amplifier circuit with adjustable gain. The nominal output is 1 volt RMS. Figure 4.1.1.2.1-2 is a picture of the FSK Modulator Card.

##### 4.1.1.2.2 Antenna Driver/Antenna

The Antenna Driver is again taken from the MPM design. The circuitry (as shown in Figure 4.1.1.2.2-1) is made up of an input buffer amplifier, a low-pass filter, a differential amplifier for gain control purposes, and an output power amplifier. The output amplifier is monitored by a bi-metallic switch that causes the entire circuit to shut down if it overheats. The antenna is also taken from the MPM design and is similar to the receiver antennas.

#### 4.1.2 Magnetic Communications

Mounted to the underside of the vehicle are three sets of reed switch assemblies and a pair of permanent magnets. The Magnetic Communications Subsystem provides location specific information transfer between the wayside and the vehicle that cannot be provided on the Inductive Communications link; this subsystem consists of permanent magnets embedded



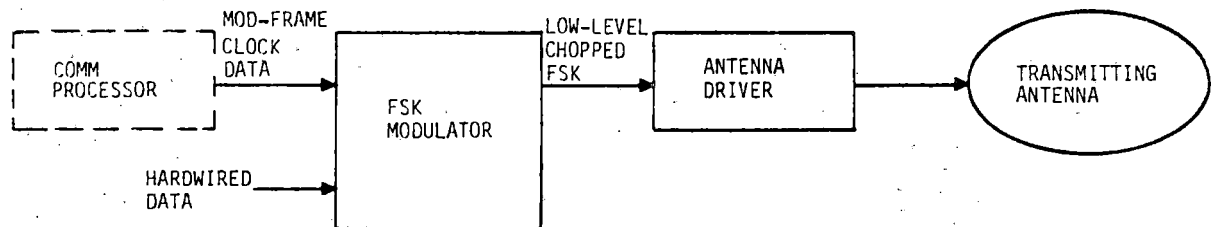


FIGURE 4.1.1.2-1: FSK DOWNLINK

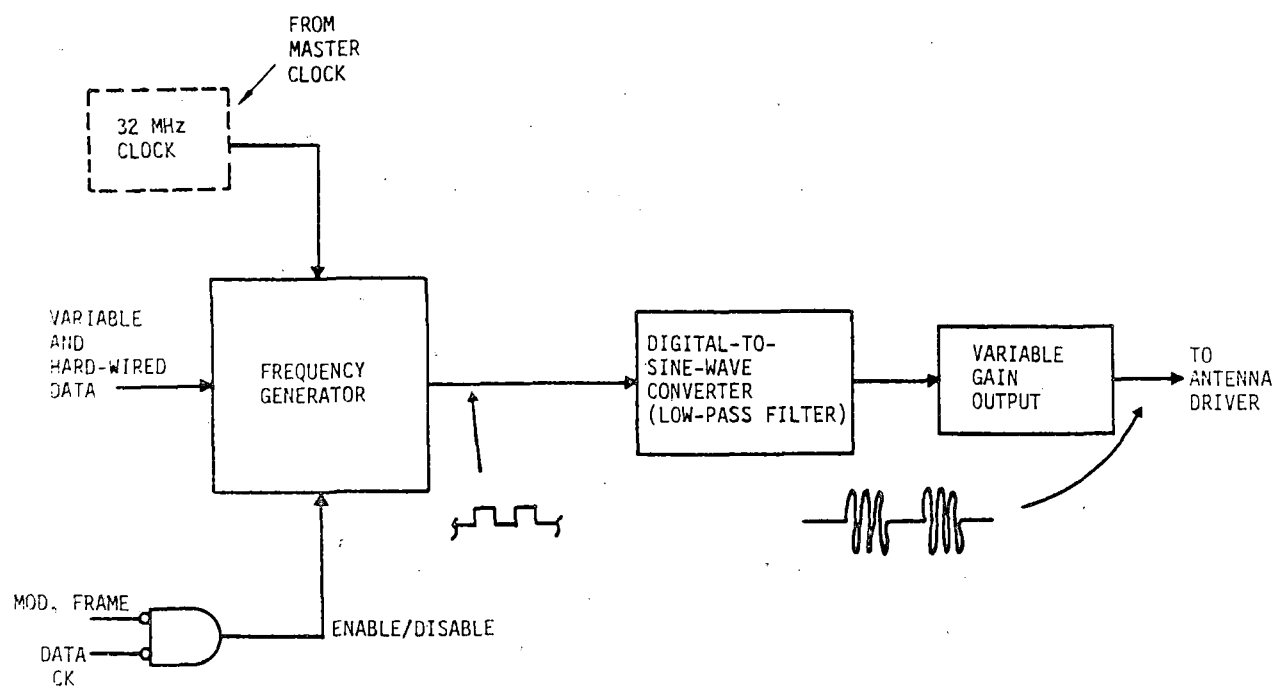


FIGURE 4.1.1.2.1-1: FSK DOWNLINK MODULATOR

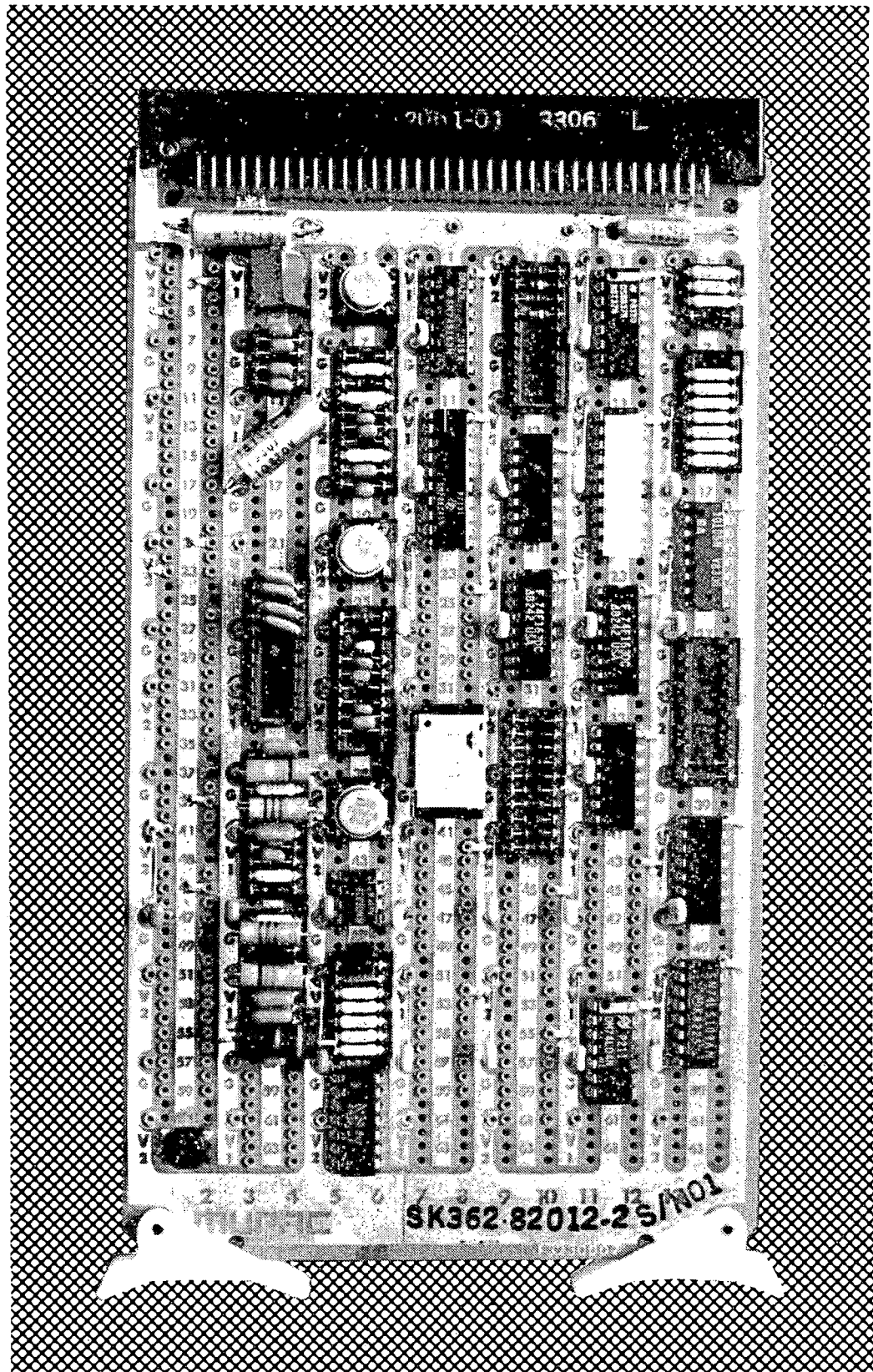


FIGURE 4.1.1.2.1-2: FSK MODULATOR CARD

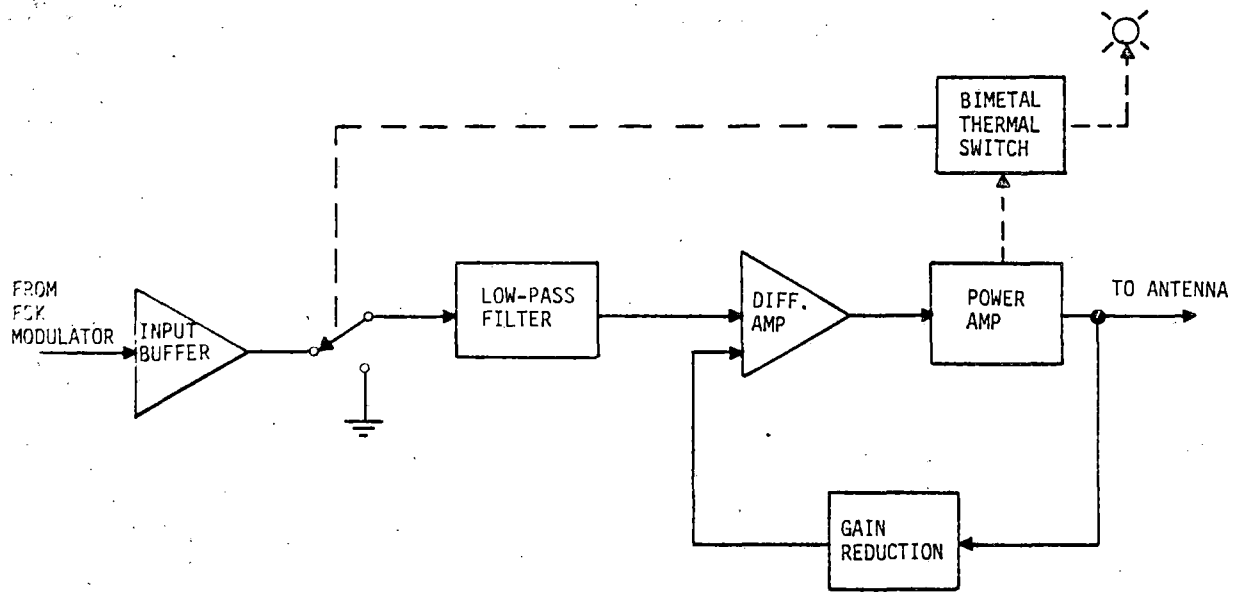


FIGURE 4.1.1.2.2-1: FSK TRANSMITTER ANTENNA DRIVER

in the guideway surface which actuate reed switches mounted to the underside of the vehicle and a pair of permanent magnets also mounted to the underside of the vehicle which actuate reed switch assemblies embedded in the guideway surface. Figures 4.1.2-1 and -2 show the guideway and vehicle mounting locations for the magnetic signalling components.

There are three sets of vehicle reed switches and each initiates a different vehicle action. The switch actuations are position sensitive, dependent on the lateral positioning of the guideway magnet. The permanent magnet attached to the vehicle actuates the guideway embedded reed switch assemblies as the vehicle travels along the guideway. This actuator/sensor combination is the guideway Presence Detector (PD) communications circuit.

#### 4.1.2.1 Reed Switches

The guideway reed switch assembly (see Figure 4.1.2.1-1) consists of four reed switches in a plastic package approximately 1" by 1" by 2.5". The four reed switches are arranged in a dual series parallel circuit such that two series switches are in parallel with the other two series switches. The reed switches close when a magnetic field passes in close proximity. The vehicle reed switch assembly consists of two switches in parallel.

The three functions actuated by the reed switch assemblies are "Switch Initiate", "Station Stop Initiate", and "Position Correction/Calibration Request" (PC/CAL). The actions these switches initiate are described in Section 3.3.4.2.1 and will not be repeated but the switch mechanical and physical considerations will be discussed.

The AGRT magnetic signalling design is based on the MPM design; however, prototype design testing indicated that the MPM design would not totally satisfy all the AGRT requirements. The sensitive parameter was found to be lateral off-tracking; therefore, this error source had to be reduced. Extensive testing was performed in the AGRT laboratory and a solution

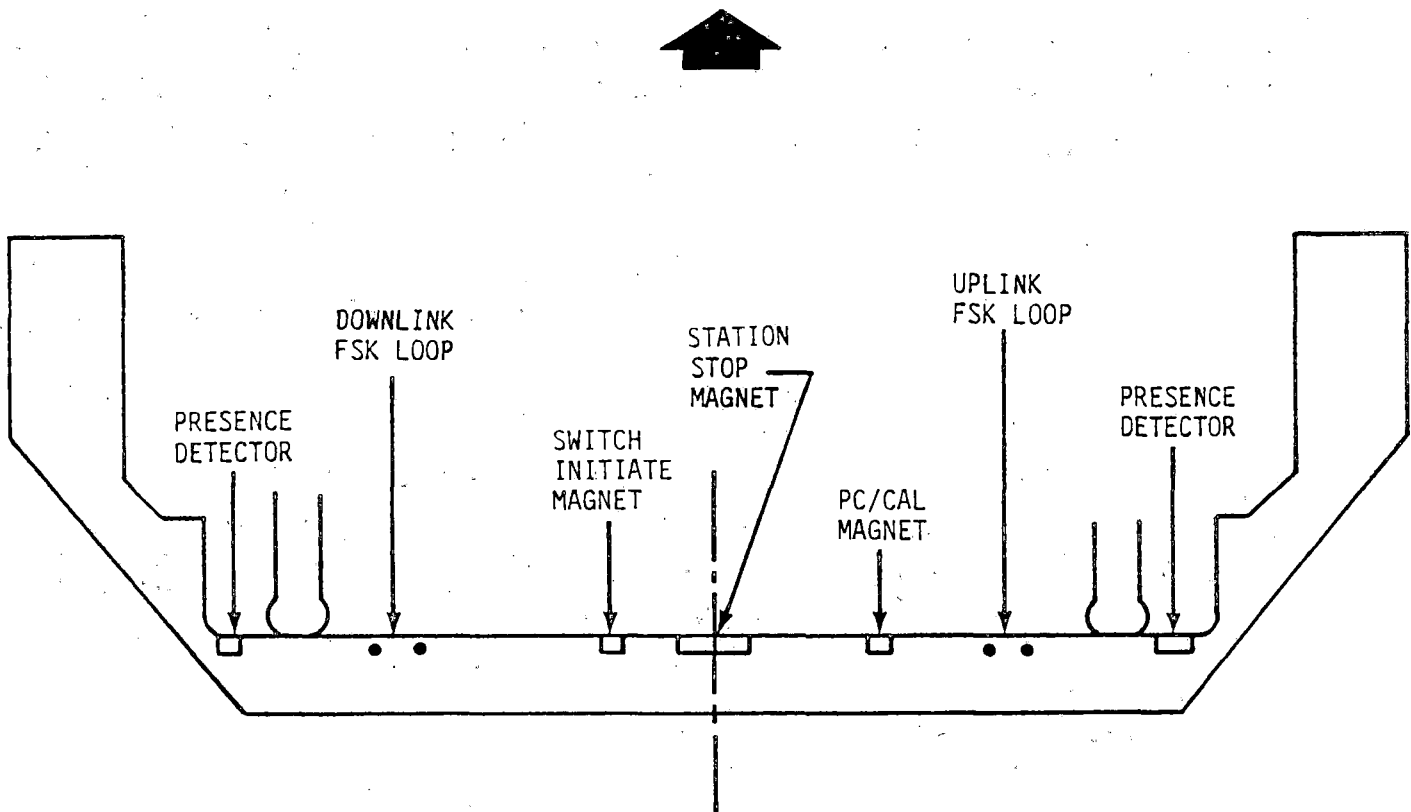


FIGURE 4.1.2-1: GUIDEWAY CROSS-SECTION

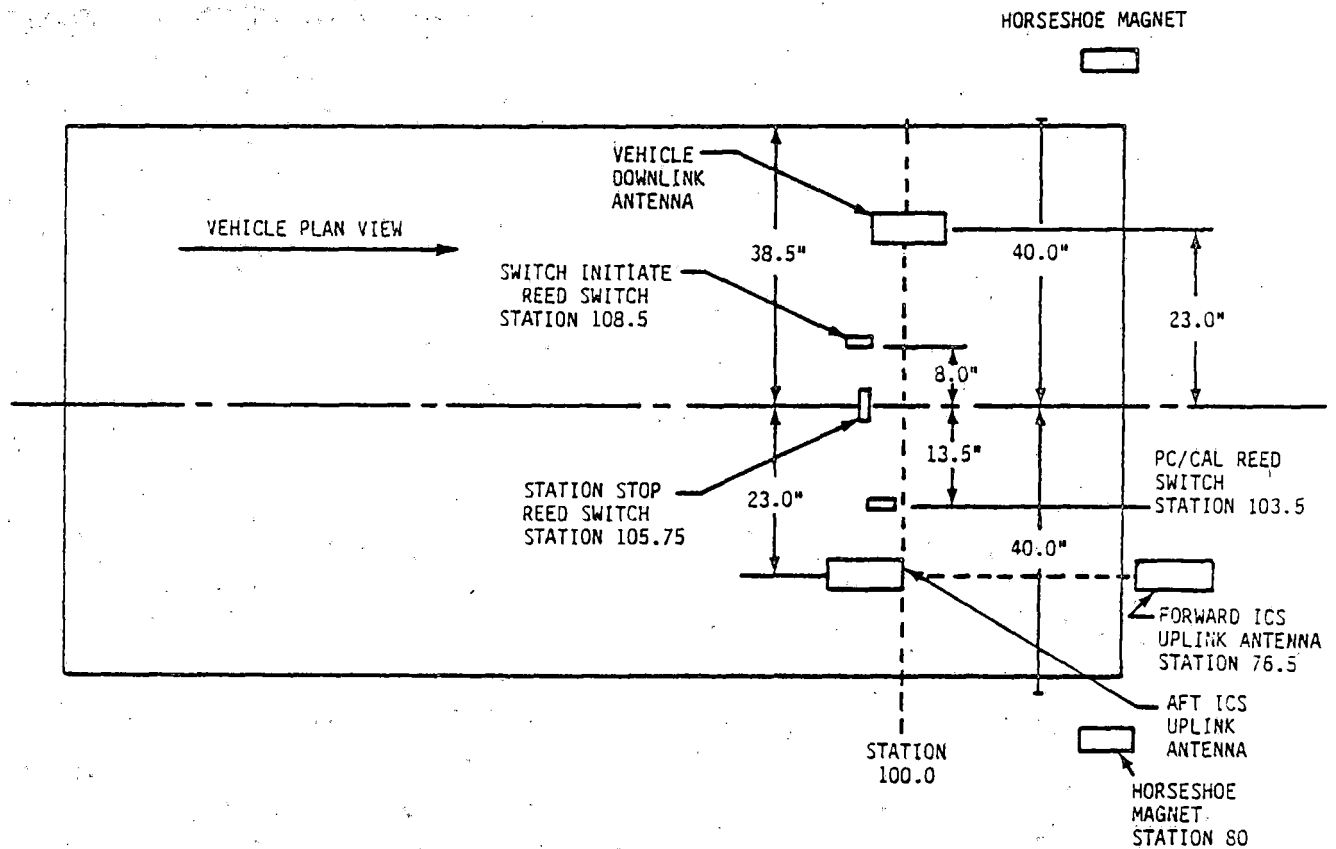


FIGURE 4.1.2-2: VEHICLE REED SWITCH LOCATIONS

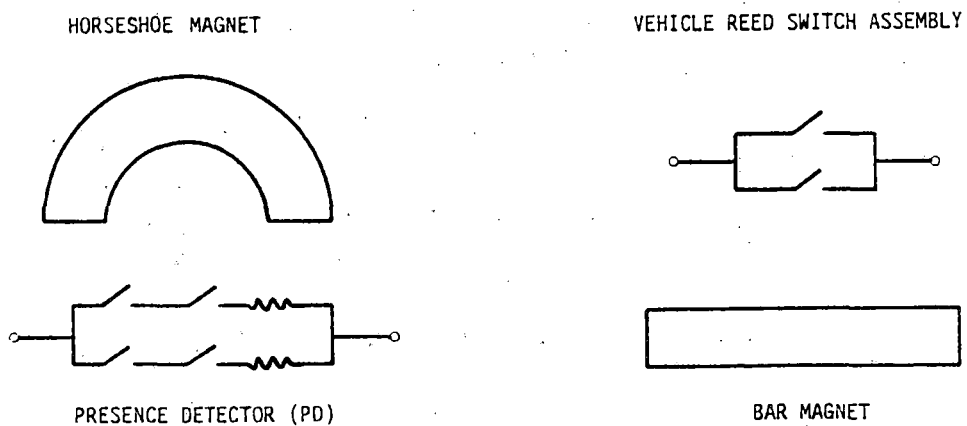


FIGURE 4.1.2.1-1: PRESENCE DETECTION AND MAGNETIC  
SIGNALLING COMPONENTS



was formulated. Each magnet, before it is embedded in the guideway, must undergo a pre-installation test which consists of placing a magnet in a test fixture and determining the closure distance to a calibrated reed switch. This distance is used as an offset when the magnet is installed. This solution gives a  $\pm 3.6$  inch distance uncertainty for the longitudinal configuration and a  $\pm 1.5$  inch uncertainty for the transversal configuration. These numbers satisfy the AGRT design tolerances.

#### 4.1.2.2 Presence Detector Magnets

The Presence Detectors are reed switch assemblies installed just below the guideway surface. These detectors may be installed on either side of a guideway, depending on the situation. The vehicle carries a pair of permanent magnets (Presence Detector Magnets) mounted to its guide axle on either side of the vehicle. As the vehicle travels along the guideway it activates the Presence Detector reed switches.

The function of the Presence Detection Subsystem is to detect vehicle entry into FSK loops and to detect vehicle entry/exit to/from station berths. Figures 4.1.2-1 and -2 (located in a previous section) show mounting positions on the guideway and vehicle.

### 4.2 Vehicle Control Hardware Elements

At this point in the document, the vehicle is traveling down the guideway communicating with the AGRT hierarchy through the Wayside/Vehicle communications elements. This section of the document will acquaint the reader with the electronics hardware that provides the intelligence, the decision making elements that have the responsibility for the operation and safety of the unmanned vehicle.

This area, unlike the previously described Wayside/Vehicle Communications element, is based not on MPM design, but on state-of-the-art microprocessor and associated software design techniques. The use of microprocessors in the design was dictated by the requirements to simultaneously maintain a safe vehicle separation, detect and promptly react

to faults, and perform specific longitudinal speed and position control algorithms. Realistically, only a microprocessor based system could perform within these timing and performance limits. A system built of discrete parts, such as transistors, resistors, capacitors, and inductors, to function within the timing and performance limits, would be of such immense bulk that it would probably fill the vehicle it was trying to control.

The VCU control electronics configuration is shown on Figure 4.2-1. The circuits to implement this configuration were built on six wire wrap type cards, five of which are common to each channel. The sixth card is the timing circuit that provides clock signals to each channel and is positioned in channel one's chassis only. The cards were partitioned and named, as much as was practical, by the function performed.

The cards are the Main Processor, the Communications Processor, the Analog I/O, the Digital I/O, the Timing, and the RS232. For design and development purposes, functional separation was very desirable, so three sizes of cards were used. There is a standard single wide card (approximately 5 inches by 8 inches), a double wide card (10 inches by 8 inches), and a triple wide card (15 inches by 8 inches). A diagram of the cards positioned in the card cage is shown on Figure 4.2-2, and a picture of the two channels mounted in a rack is shown as Figure 4.2-3. Each card and the functions performed are discussed in detail in the following pages.

#### 4.2.1 Main Processor

The Main Processor card contains, as named, the main controlling processor and associated memory system of the VCU electronics. In addition, this card contains the Data Exchange Unit, the Memory Circuit shared with the Communication Processor, and the Watchdog Oscillator and Window Generator circuitry (refer to Figure 4.2-1). A photograph of this card is included as Figure 4.2.1-1.

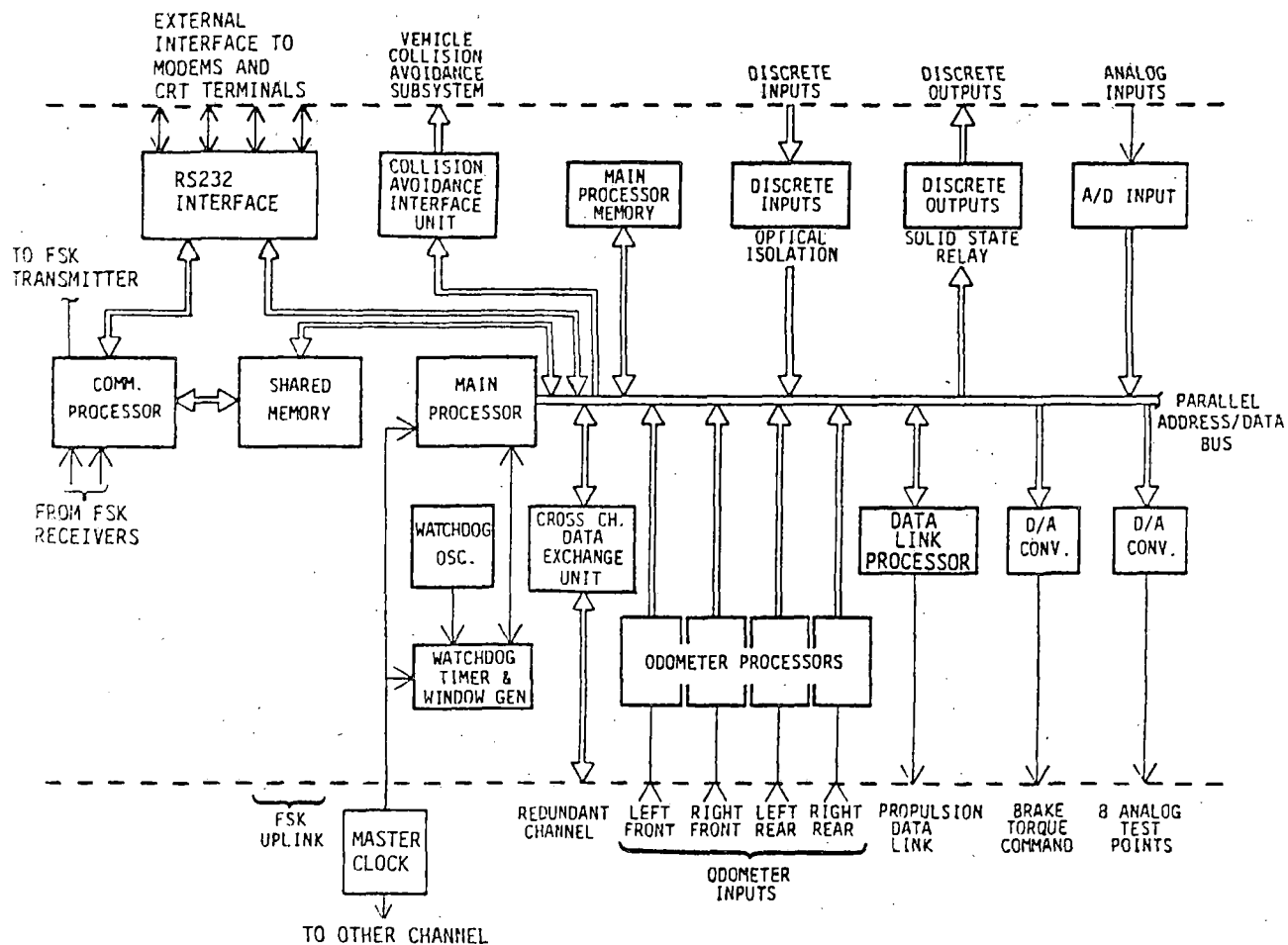


FIGURE 4.2-1: BLOCK DIAGRAM OF VCU CONTROL ELECTRONICS

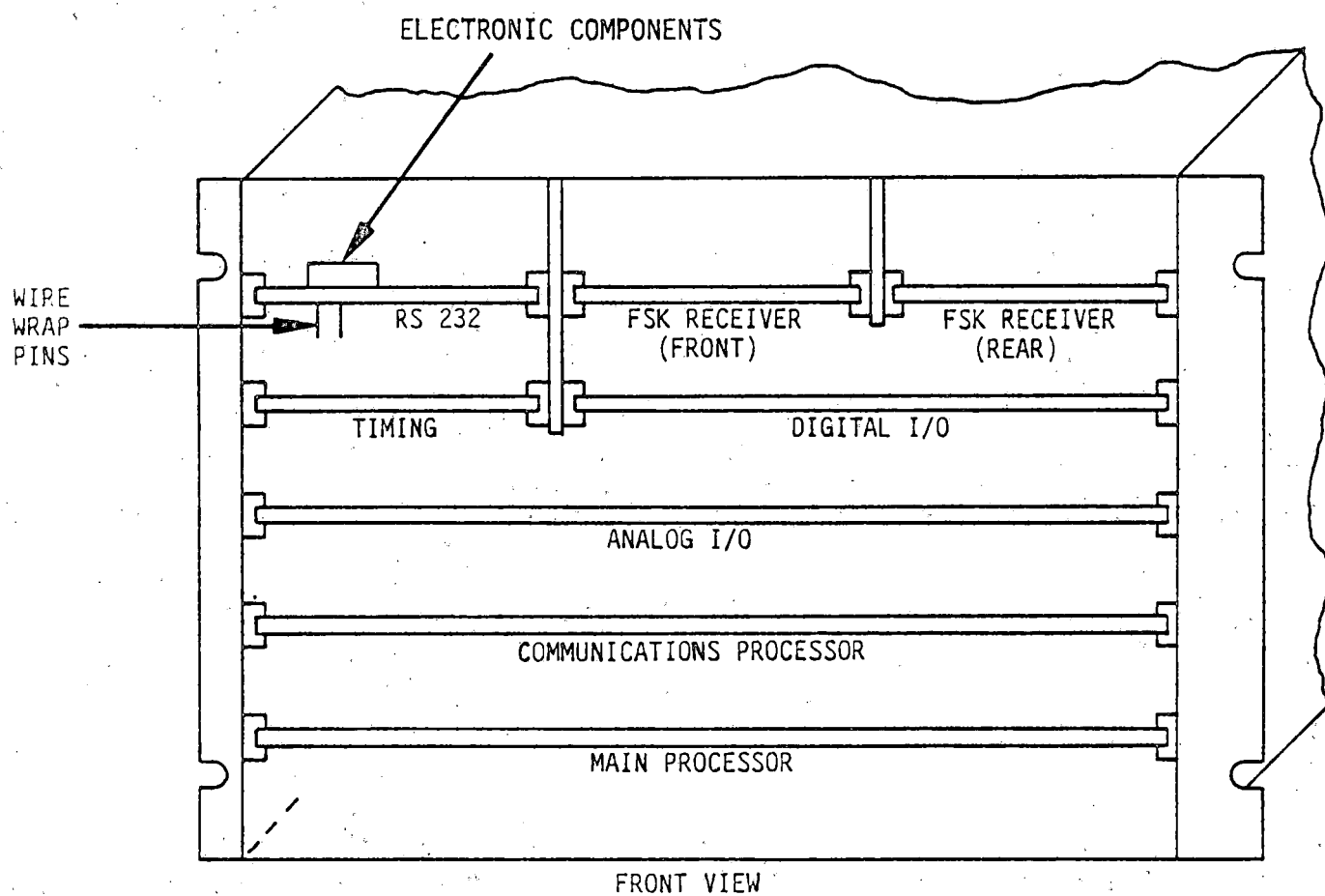


FIGURE 4.2-2: VCU CARD CAGE

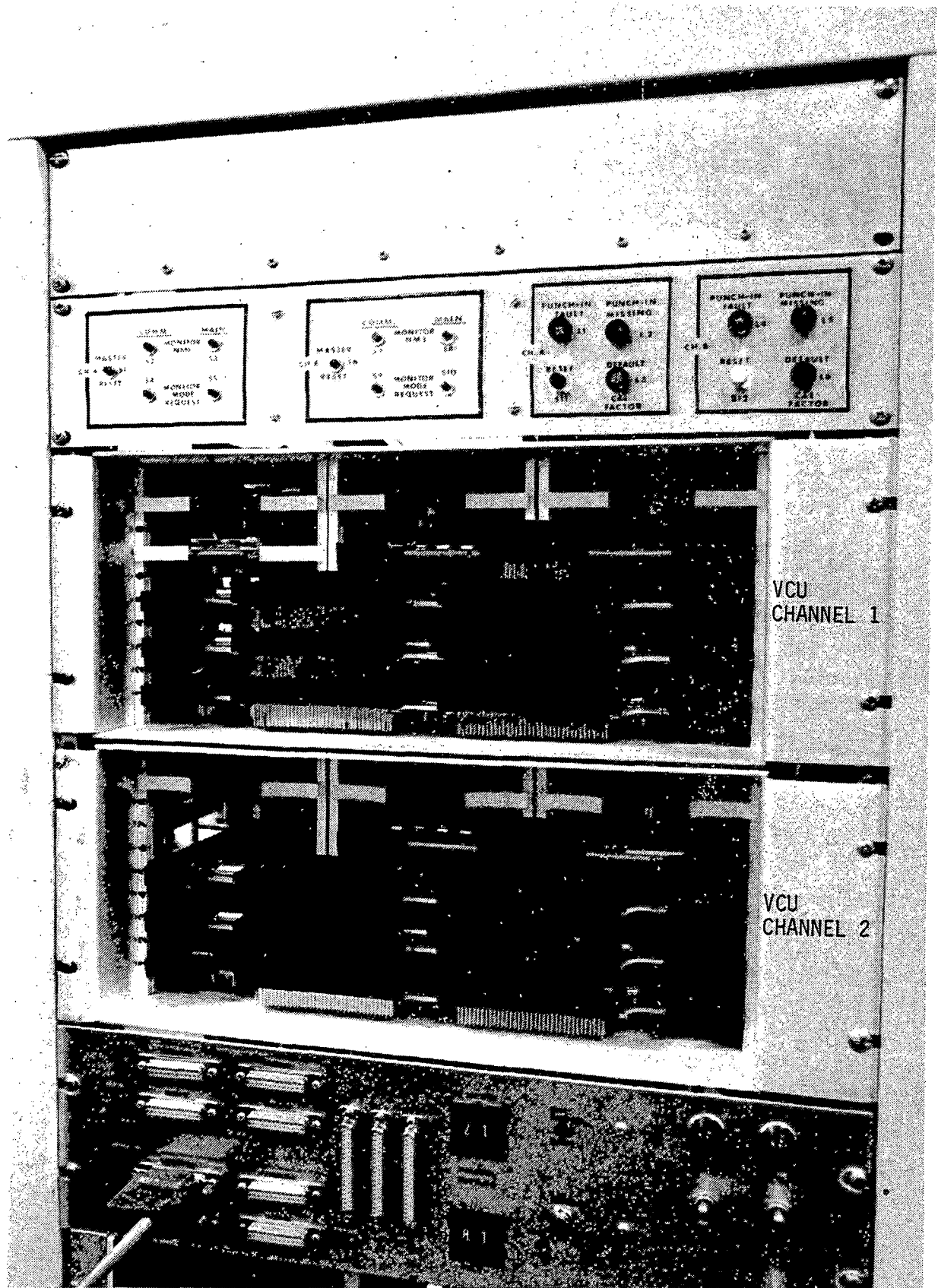


FIGURE 4.2-3: PHOTOGRAPH OF VCU CHANNELS 1 AND 2

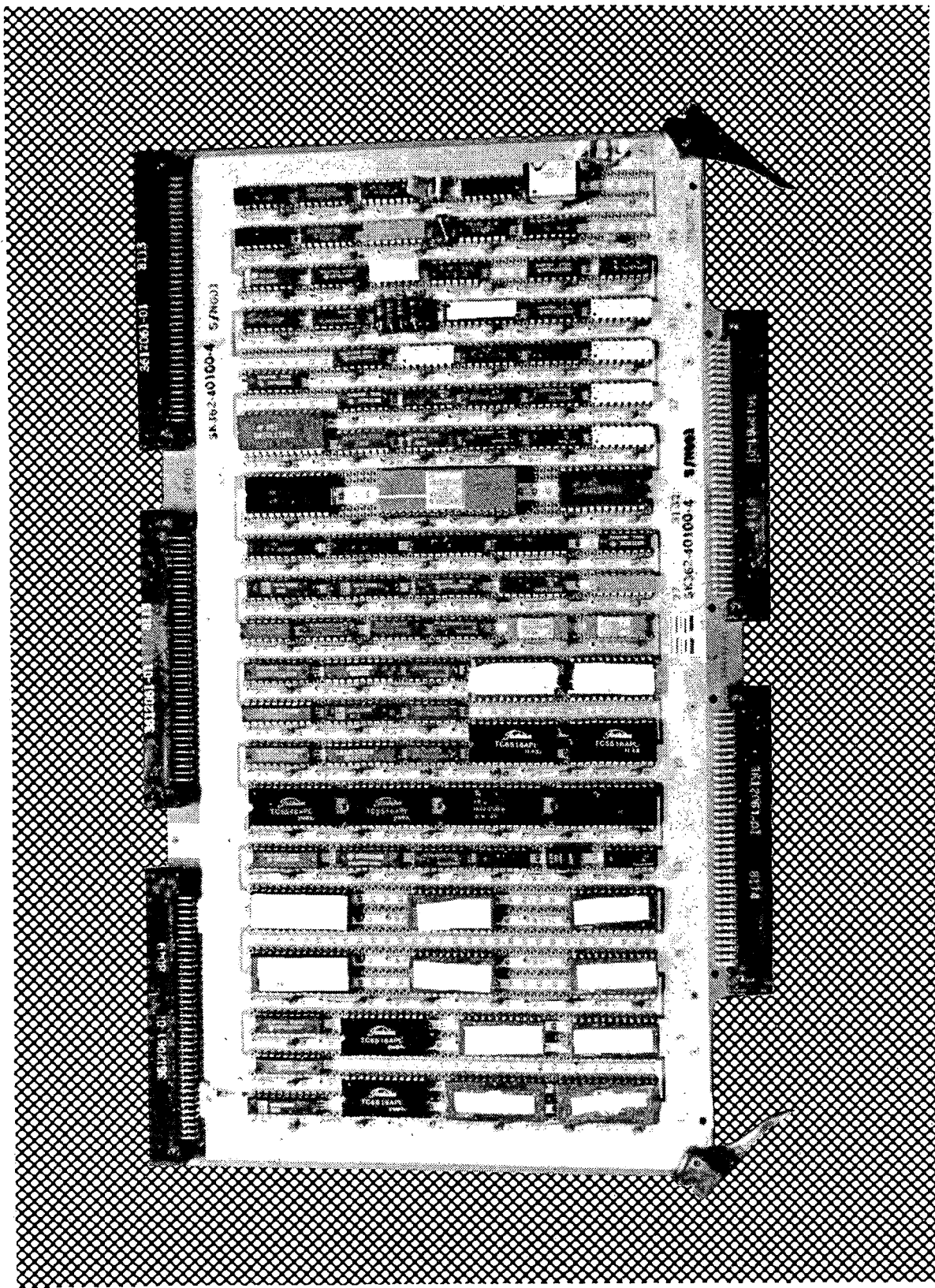


FIGURE 4.2.1-1: MAIN PROCESSOR CARD

A Zilog Z8002 16-bit microprocessor was selected as the main controller element. An analysis of the control functions to be performed and trade studies of the microprocessors available, at the time the selection was made, said the Z8002 had the desired processing power and memory addressing capability to perform the AGRT VCU functions with a comfortable margin for expansion. In retrospect, the processor selected does perform the VCU functions well within the prescribed limits and was a good choice at the time the selection was made. If the selection were made today, however, a different processor would possibly be selected.

#### 4.2.1.1 Microprocessor and Memory

The Zilog Z8002 microprocessor may be described as having a 16-bit central processing unit and a 16-bit multiplexed address/data bus plus additional control lines. It can directly address 32K words of memory. It executes 110 basic instructions with 410 combinational instructions at a speed of 4 MHz. It has eight addressing modes plus a repertoire of block and string operations. It is an NMOS device requiring a single +5 volt supply, and comes in a 40 pin DIP package. It is originally built by Zilog and is second sourced by Advanced Micro Devices (AMD).

Figure 4.2.1.1-1 shows the microprocessor and memory configuration. There are sixteen multiplexed address/data lines on the bus, and a number of control signals (only the significant control lines are shown on the diagram). The multiplexing of the bus with address information followed by data allows fewer pins on the microprocessor package, but necessitates using an address latch circuit to capture and hold the address information. The "AS" (Address Select) signal is present when address data is available, allowing the address information to be latched into a 16-bit holding register. The register outputs are then directed to all devices needing address information.

The "DS" (Data Select) signal is present whenever data is to be taken into the microprocessor (a read function), or directed out of the microprocessor (a write function) to some other element. The "R/W" signal provides the read/write direction control to all elements needing this

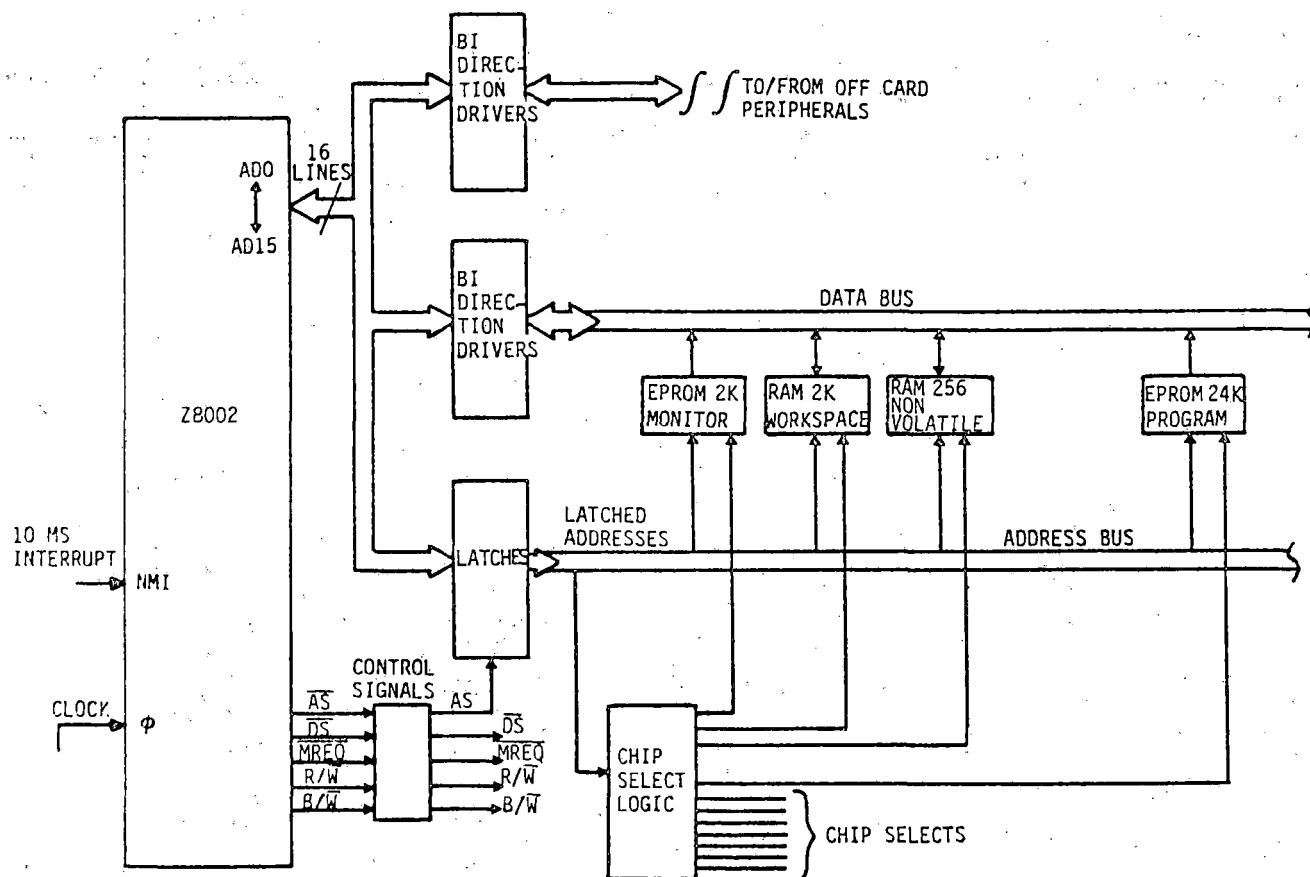


FIGURE 4.2.1.1-1: MICROPROCESSOR AND MEMORY



information. An additional signal is the "MREQ" (Memory Request), which is used by the memory elements to gate the critical timing of a data transfer. The "B/W" signal informs the system whether a byte (8-bit) or a word (16-bit) transfer is in progress on the Data Bus.

The Chip Select logic decodes an address within a certain range of addresses, then sends a select or enable signal to the selected device informing it that it is to respond on the bus with a read or write data exchange as directed. The elements controlled by the chip select logic are the memory chips and the Input/Output (I/O) peripheral chips. (There is a range of addresses that are devoted to elements other than memory chips, such as Input/Output devices. There are 1024 addresses reserved for this purpose, thus reducing the memory addressing potential of the microprocessor by 1024 locations. This method of executing I/O operations as a memory transaction is fast and efficient and is referred to as Memory Mapped I/O.)

The Z8002, with sixteen address lines, will address 32,768 words of memory. The memory (see Figure 4.2.1.1-2 for memory addressing configuration) is configured with 2K words of Erasable Programmable Read Only Memory (EPROM) containing a Monitor program used as a troubleshooting and maintenance aid, 2K words of Random Access Memory (RAM) used as workspace memory, a 256 byte non-volatile memory for storing the calibration factor and fault data, and 24K words of EPROM program memory. Also included in the memory addressing configuration is the Communication Processor's Shared RAM and the Data Exchange Unit's RAM. However, these two memory elements are isolated from the address and data busses by buffer amplifiers. These buffers are normally in a high impedance state until a control signal activates their one/zero logic function (the device has three states: one, zero, and high impedance; thus, the term tri-state). The data bus devices have one additional control line which specifies direction of data flow; therefore, they are bi-directional tri-state buffers.

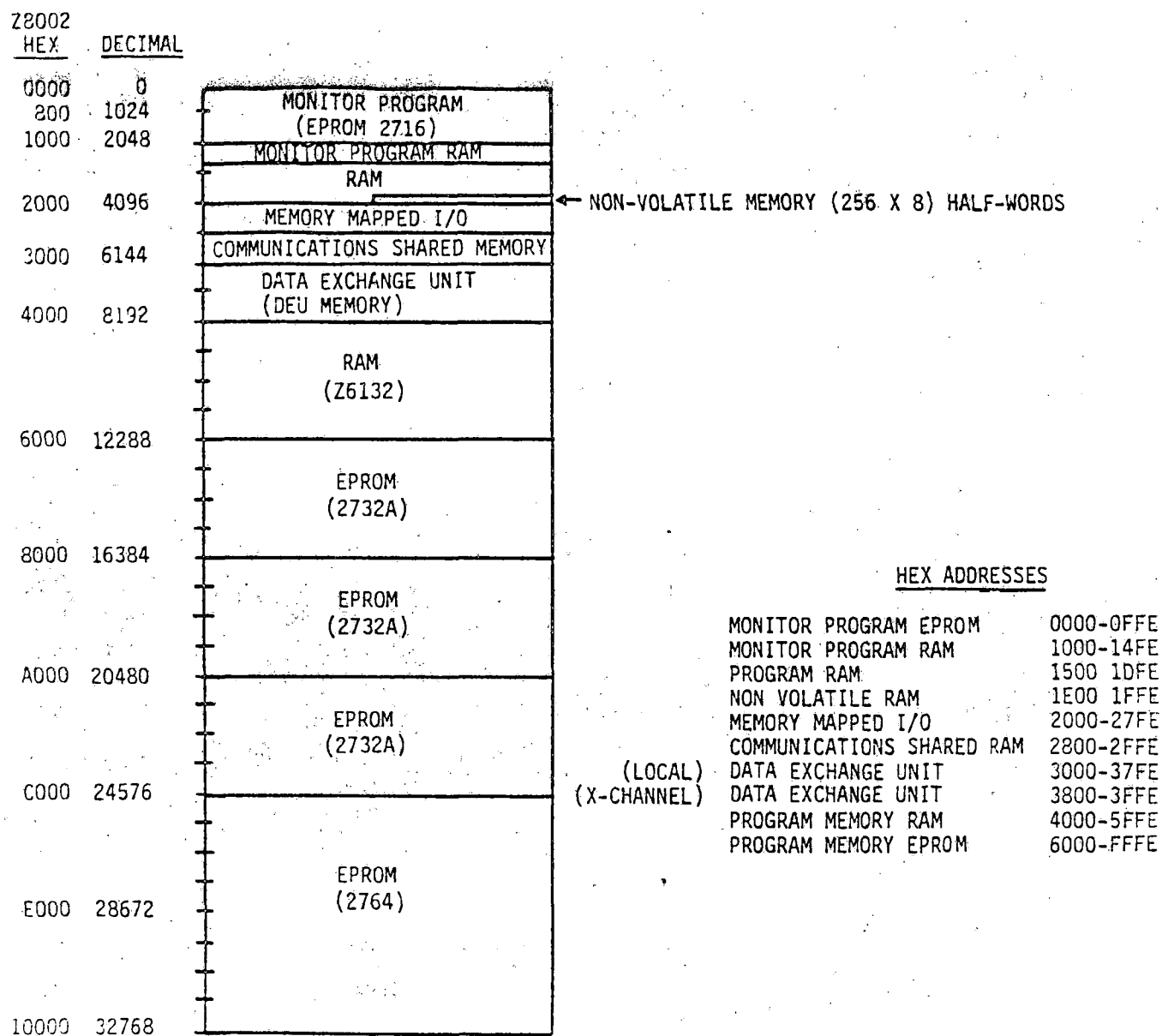


FIGURE 4.2.1.1-2: VCU MAIN PROCESSOR MEMORY CONFIGURATION

#### 4.2.1.2 Data Exchange Unit

The VCU Data Exchange Unit (DEU) is the communications artery by which each channel is able to receive data from the other channel and make safety critical decisions. Figure 4.2.1.2-1 shows the primary elements of the DEU. Each channel has been allocated 2K words of memory address space, but only 1K of local memory is provided. Each local processor can read and write to the first 1K of its local memory. When a processor addresses the second 1K of memory, the logic decodes this as a request to access the other channel's memory. A processor can only request a read from the other channel's memory; a write request to the remote memory is completely ignored. In fact, no signal exists across the interface to request a remote write.

As shown on the diagram, the data bus lines are buffered with tri-state devices on both sides of the interface and on the local bus system. The address bus is buffered only on the drive side of the interface. All of the tri-state devices are kept in their high impedance state except when the arbitration and control logic allows a memory transaction to be carried out. When a transaction is in progress, and the other processor makes a request to access the same memory, a wait signal is sent back to the most recently requesting processor and the tri-state buffers on both sides of the interface (of the waiting processor) are kept in their high impedance state. When the first processor's transaction is completed, the waiting processor is then allowed to make its transaction. Neither processor can keep control of a memory circuit for more than one access time if another processor is also requesting access to the same memory circuit. The longest delay due to an access conflict is less than one microsecond.

To verify that the operation of the DEU is fail-safe, a Failure Modes and Effects Analysis (FMEA) was conducted on the DEU. The conclusion of the FMEA was that all failures hypothesized resulted in a safe reaction.

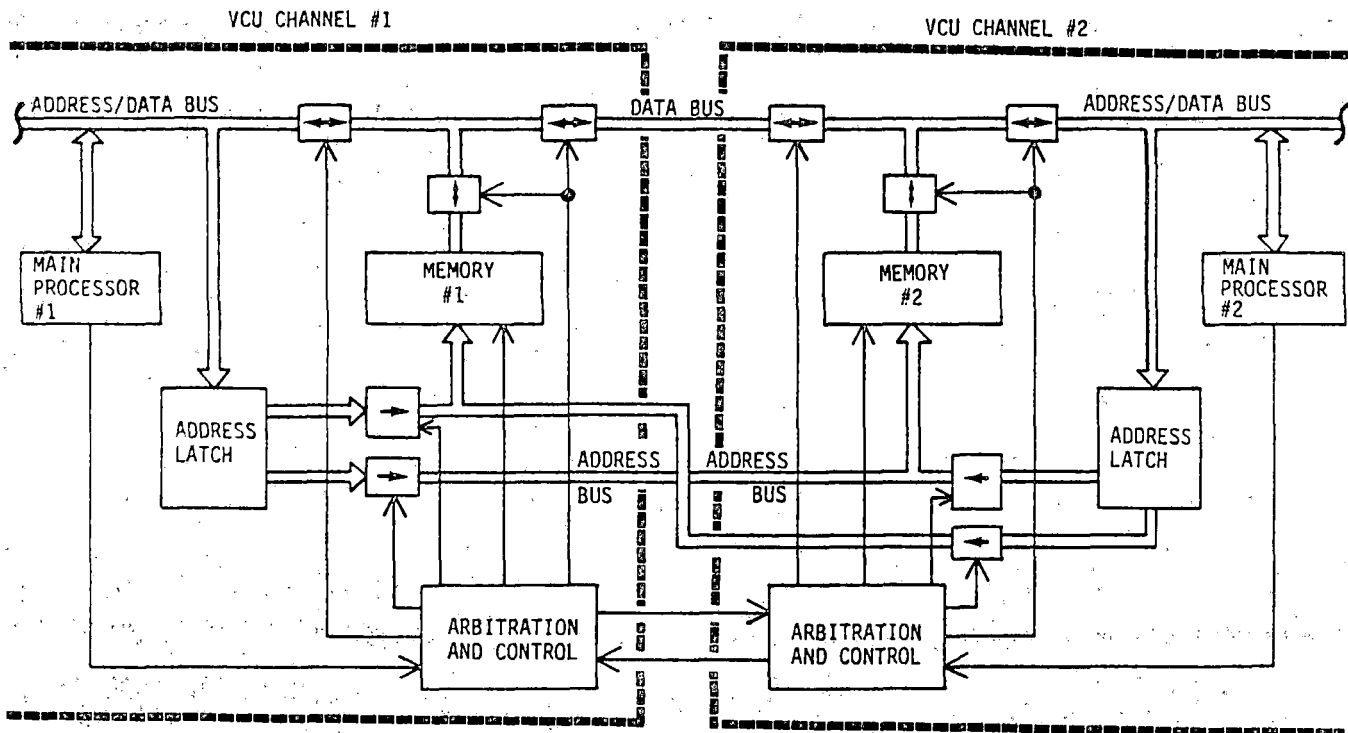


FIGURE 4.2.1.2-1: CROSS CHANNEL DATA EXCHANGE UNIT

#### 4.2.1.3 Communications Processor Shared Memory

The Communications Processor Shared Memory is the common link between the Main Processor and the Communications Processor. All data exchanges between the two processors are routed through the shared memory. Figure 4.2.1.3-1 is a diagram showing the primary elements of the circuit.

The memory is 1K words in size and either processor can access the memory with reads and writes. The tri-state buffers are always in the high impedance state except during a memory transaction. The Arbitration and Control logic handles any conflicts if both processors should request an access at the same time. Neither processor can take control of the memory for more than one access, so the maximum delay either processor should experience is less than one microsecond. The scenario for a processor requesting an access is as follows: The processor wanting to make an access sends a request to the Arbitration and Control logic. If the memory is not busy, the control logic enables the tri-state buffers for the requesting processor and the transaction is completed. If the memory is busy making a transaction to the other processor, the wait line to the most recently requesting processor is made active and the tri-state buffers to that processor remain in the high impedance state. When the memory completes its current transaction, the tri-state buffers to the other processor are made high impedance, then the wait line to the waiting processor is made inactive and the transaction is completed.

#### 4.2.1.4 Watchdog Circuit

In order to maintain the AGRT short headway system, the cross checked functions must be checked at precise time intervals; consequently, the VCU design requires a synchronous operation between the Main Processors. This design allows the redundant systems to make sequential calculations and perform disparity checking on each other's data in a close coupled synchronized manner. Also the integrity of certain calculations, using sensor input data, requires the clock frequency to be maintained within a close tolerance of its specified frequency for accurate calculations.

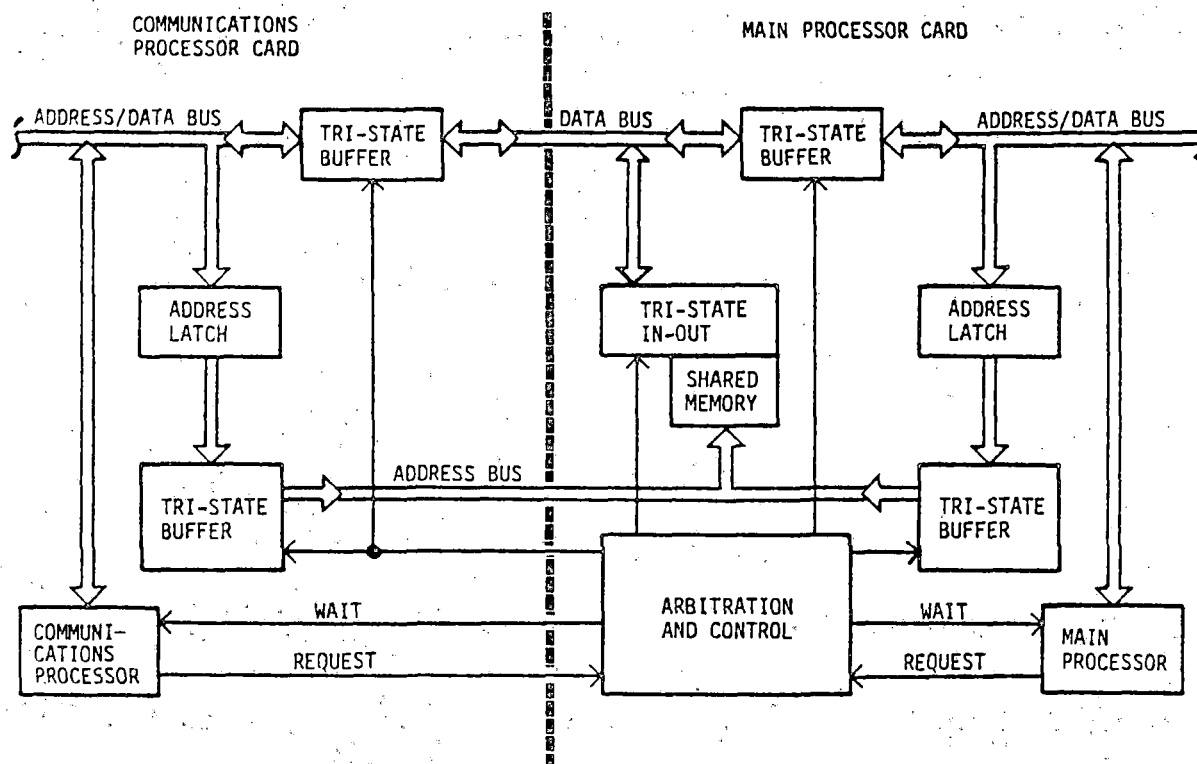


FIGURE 4.2.1.3-1: COMMUNICATION PROCESSOR SHARED MEMORY

The system designed provides inputs from a single clock to each channel, detects frequency out-of-tolerance conditions and hardware failures in the timing and checking circuits, and initiates safe responses when failures occur.

Figure 4.2.1.4-1 is a diagram of the Watchdog circuitry. The circuits identified as Watchdog are the Watchdog Oscillator, the Watchdog Timer Window Generator, the Check Flip-Flop (F/F), and the Punch-In F/F.

The timing system operates with a single oscillator and count down chain generating a 4 MHz system clock and 100 pulse/second Master Interrupt (10 millisecond interrupt) which is used by both channels' processors. With each processor utilizing the same timing signals, the synchronization complexity between the processors is minimized. To maintain the integrity of the two processors, each processor has a Watchdog circuit which monitors the timing function of its assigned processor; if a processor fails to output a pulse within a specified time window, a failure is reported by default. The mechanism by which a failure is detected is the absence of a pulse into a fail-safe hold-off circuit within a preset time period. The absence of the pulse relaxes or releases the hold-off circuit, causing a safe reaction.

Referring to the timing diagram (Figure 4.2.1.4-2), when power is initially applied a Master Reset (MR) is generated that synchronizes all three oscillator timing circuits and the Main Processors. The Master Interrupt pulses begin 40 milliseconds after the MR and continue at the 100 pulse/second rate. At MR the Watchdog Timer Window Generator is reset and begins generating a Window pulse every 10 milliseconds. When the system is in perfect synchronism, a Window is generated exactly 24 microseconds after each Master Interrupt and is 8 microseconds in width. Each Main Processor answers each Master Interrupt and then by executing a rigid software routine, outputs a Punch-In pulse that must occur somewhere within the 8 microsecond window. When the system is in perfect synchronism, the Punch-In occurs in the center of the Window. All three oscillators operate extremely close to the same frequency but are not identical. As time passes the Punch-In pulse drifts away from the

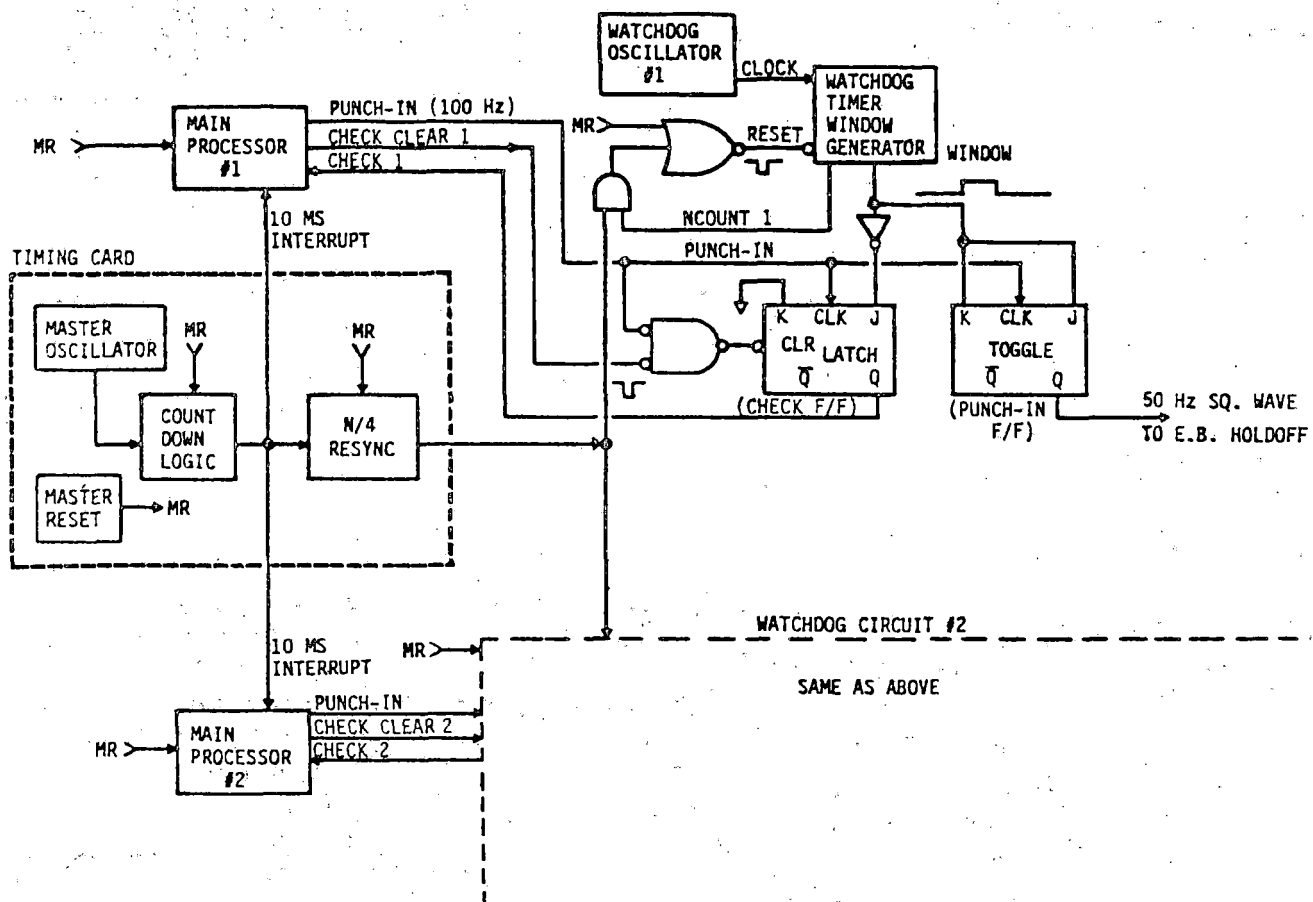


FIGURE 4.2.1.4-1: WATCHDOG CIRCUITRY



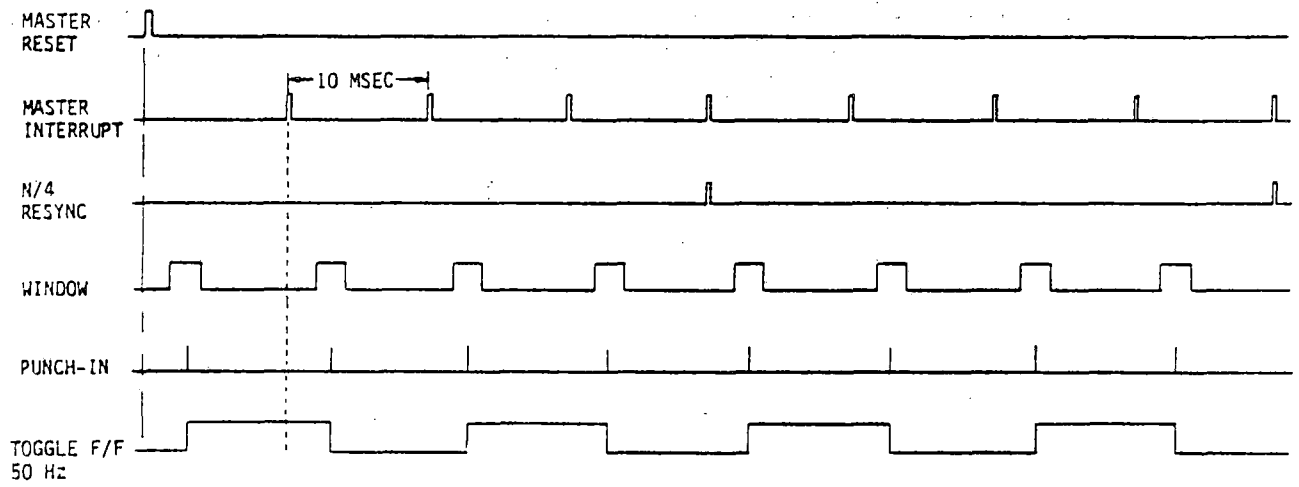


FIGURE 4.2.1.4-2: TIMING DIAGRAM

center of the window, and will eventually fall outside the window, so periodically the Window generating circuits must be reset. That is the purpose of the N/4 Resynch signal. The Window generation circuits are reset every 40 milliseconds. The length of the Window and the resynchronization period is based on the total system accuracy required, the total stability of the oscillators over a 3 year period, and the time variable of the processor answering the interrupt. The 8 microsecond Window and the 40 millisecond resetting of the Watchdog circuits maintain a system accuracy of  $\pm 0.0179\%$ , which is within the  $\pm 0.02\%$  design requirement.

The circuit used to determine if the Punch-In pulse is within the Window is a simple toggle flip flop. The Window is used to enable the clock input, which is the Punch-In pulse. As long as the Punch-In pulses occur within the Window, the F/F toggles at a 50 Hz square wave rate and maintains the emergency brake hold-off signal.

All circuits shown are effectively checked every 40 milliseconds by normal operation except the Check F/F. The purpose of the Check F/F is to report to the Main Processor if a Punch-In pulse occurs outside a Window, thus allowing the Main Processor to initiate a safe reaction. Under normal operation this circuit is not exercised; hence, something could fail and go undetected. To detect a failure in the Check F/F the circuitry is exercised on a periodic basis by the Main Processor issuing a Punch-In pulse outside the window with the operation monitored by the Main Processor. The Main Processor then commands a reset of the Check F/F and monitors to make sure it reset properly.

#### 4.2.1.5 Non-Volatile RAM

Today's RAM technology is based primarily on memory devices that reliably store data as long as the applied voltage remains within a specified range. When the voltage decreases below a point, the data is lost forever (a volatile static RAM). There is a requirement to store calibration factors in every vehicle and not lose these factors for long periods of time (power will likely be cycled on/off many times). There

is also the requirement to be able to change a factor readily when the need should arise; for example, when a new tire is installed.

A special non-volatile RAM is used to store the calibration factors; this device is called a NOVRAM (Non-Volatile static RAM). It combines two memory technologies on one chip. Figure 4.2.1.5-1 shows the structure of the device. The NOVRAM contains a static RAM and an electrically erasable PROM (EEPROM). In this NOVRAM, data gets read and written exactly as in a standard static RAM. In addition, the "Store" signal transfers each RAM cell's data to an EEPROM cell. The EEPROM stored data then gets reloaded into the RAM via a "Recall" pulse. The data in the EEPROM cells is retained even when power is lost for long periods of time.

#### 4.2.2 Communications Processor

The Communications Processor card contains a 16-bit microprocessor and associated memory system that functions as the communications center in the VCU electronics (see Figure 4.2.2-1). The communications card includes inputs from both uplink receivers and provides the output to the downlink transmitter. In addition, this card contains the vehicle identification, the store/recall pulse generation circuit for the non-volatile RAM, and a Monitor program interface similar to the one used on the Main Processor card. A photograph of this card is included as Figure 4.2.2-2.

A Zilog Z8002 16-bit microprocessor was selected as the communications controller element. An analysis of the functions to be performed and the peak loading timing predictions indicated that a 16-bit processor was necessary from a data throughput standpoint. An 8-bit processor was considered but could not handle the peak load situations. The communications controller function has a small program memory requirement but a high processing rate factor. Once again it is felt that the processor selected performs well within the prescribed limits and was a good choice.

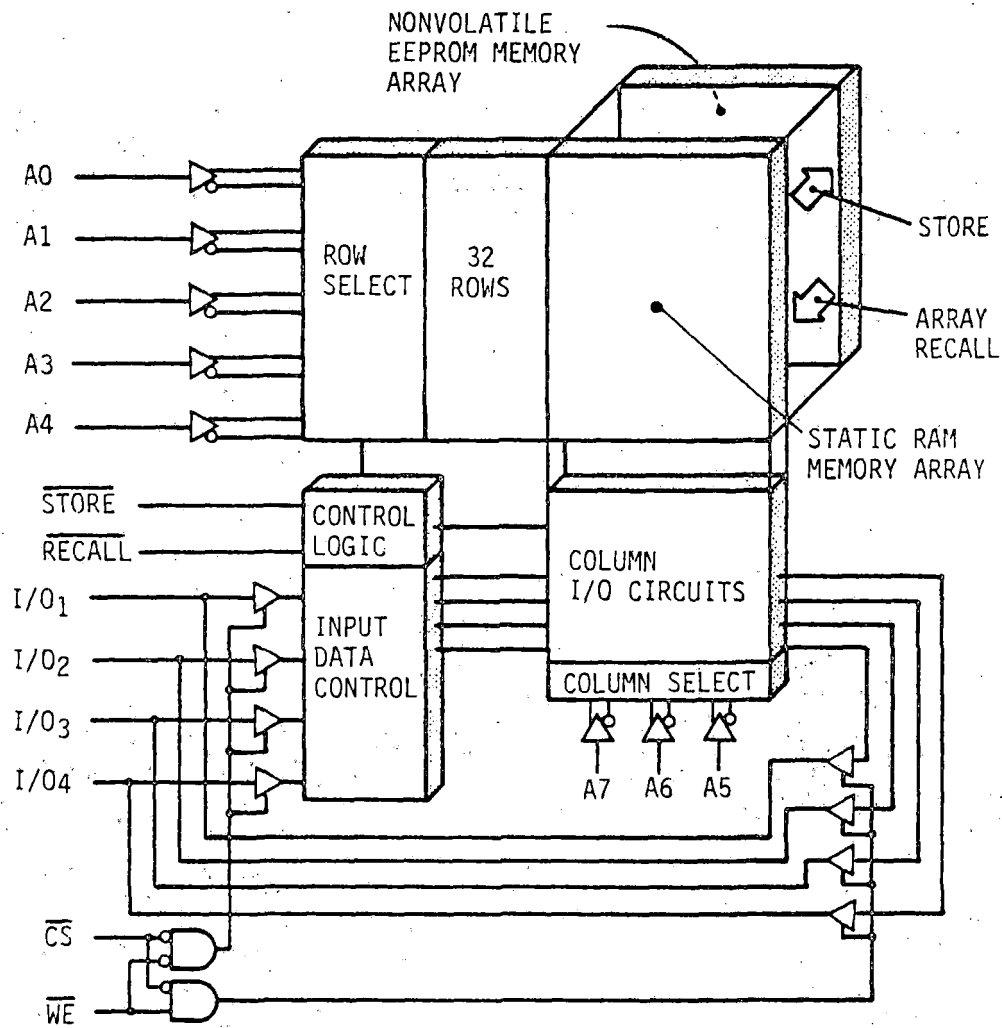


FIGURE 4.2.1.5-1: NON-VOLATILE RAM (NOVRAM)

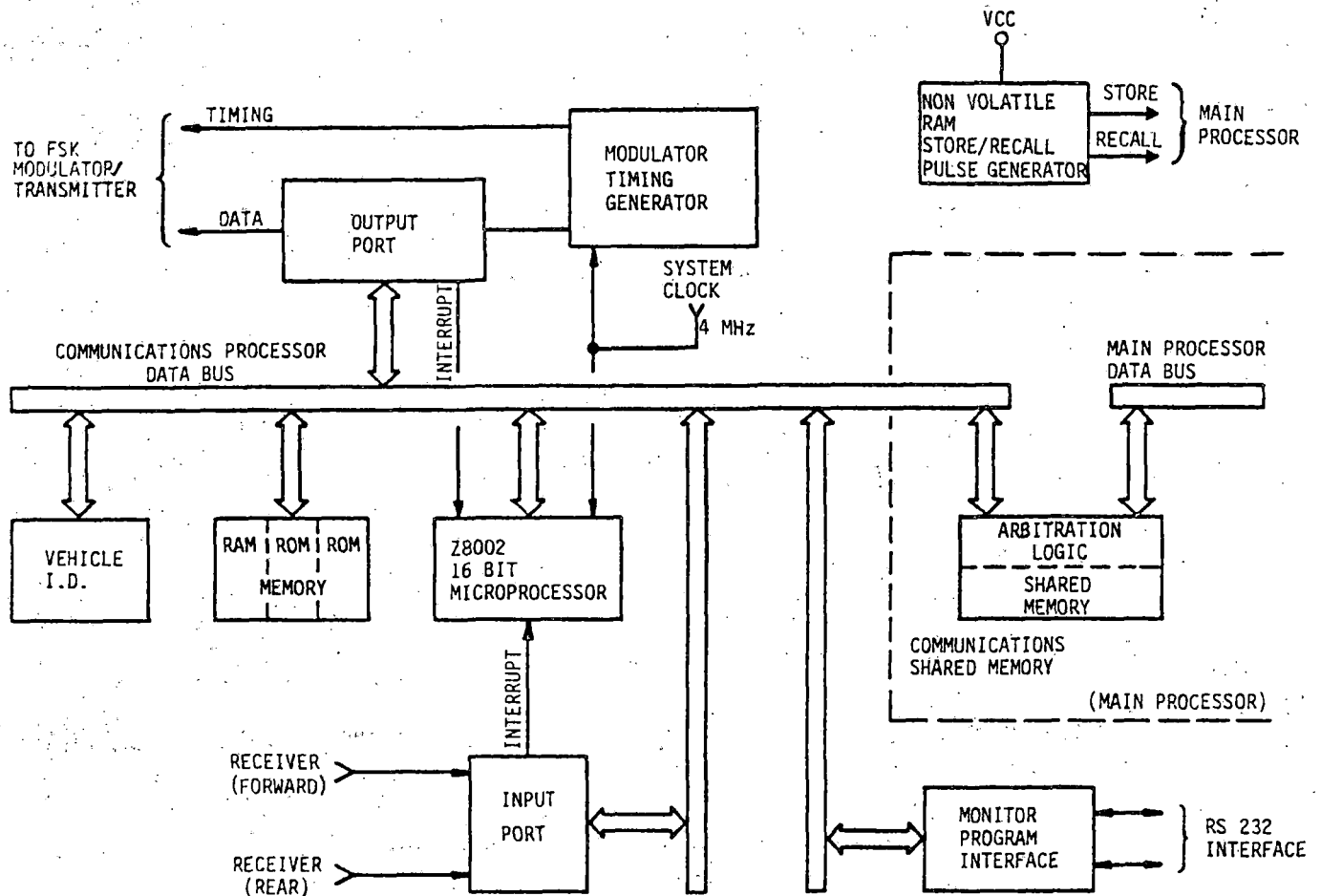


FIGURE 4.2.2-1: COMMUNICATIONS PROCESSOR CARD BLOCK DIAGRAM

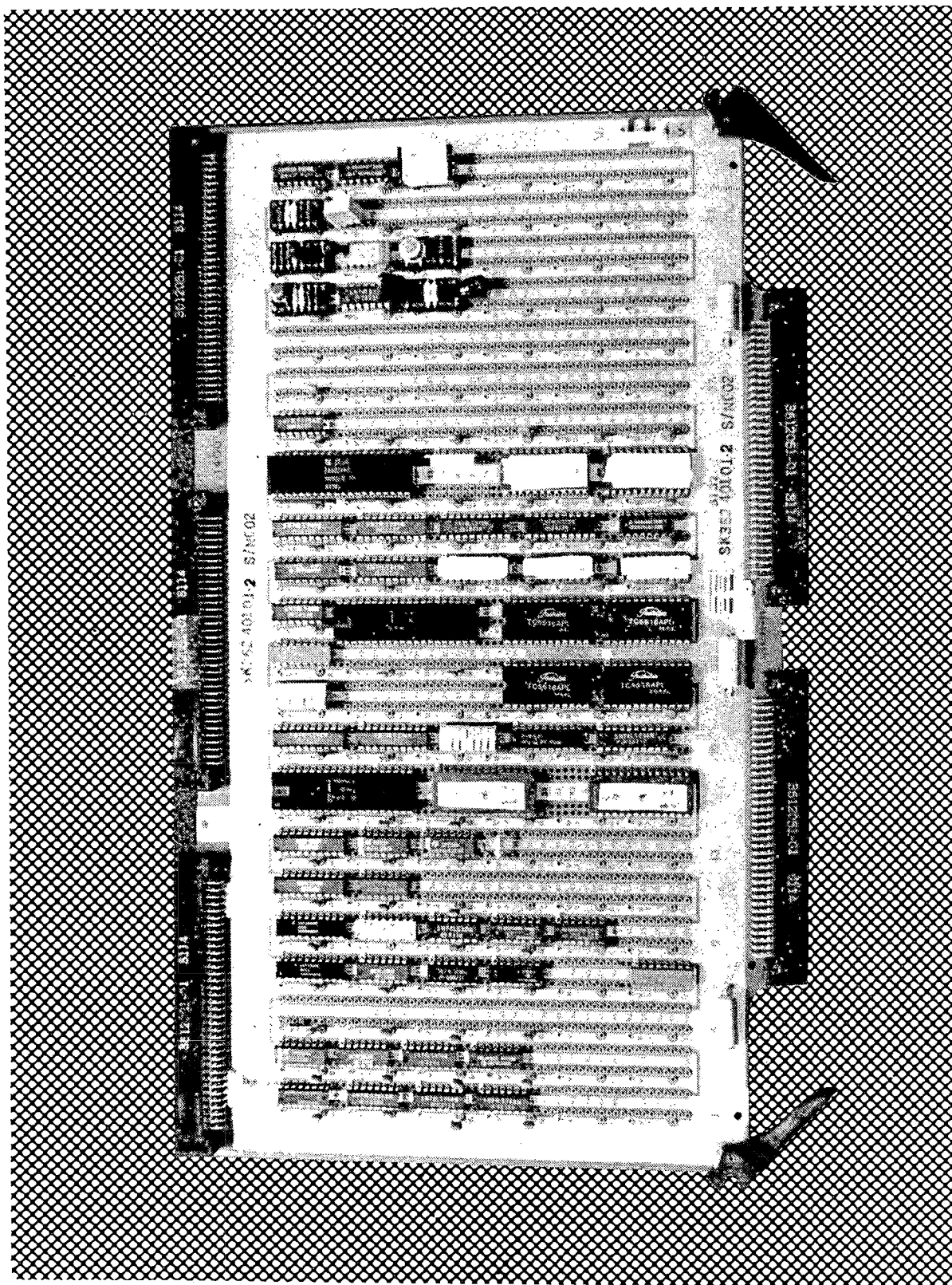


FIGURE 4.2.2-2: COMMUNICATIONS PROCESSOR CARD

#### 4.2.2.1 Microprocessor and Memory

The Communications Processor microprocessor and memory configuration is very similar to the Main Processor's except on a smaller scale. Figure 4.2.2.1-1 is a block diagram showing the microprocessor, memory, and control functions. It again is a 16-bit multiplexed address/data bus configuration with the appropriate control lines coming from the microprocessor.

The Chip Select logic decodes addresses within a certain range of addresses, then sends a select or enable signal to the selected device telling it to respond on the data bus with the appropriate read or write response. On this card most of the chip select and control logic was done using programmable array logic (PAL). This technology allows more logic functions to be placed in one chip, thus replacing several TTL type chips with one PAL chip.

The memory (see Figure 4.2.2.1-2 for memory addressing configuration) is configured with 2K words of EPROM containing the Monitor program, 4K words of RAM used as workspace memory, and 16K words of EPROM program memory. There are allocated 1K words of shared RAM addressing, but the actual RAM is located on the Main Processor card. The amount of RAM and EPROM actually needed is considerably less than what is installed, and could be reduced even more in an operational configuration.

#### 4.2.2.2 Receivers/Transmitter Interface

The Communications Processor card interfaces with the forward antenna's FSK receiver, the rear antenna's FSK receiver, and the FSK modulator/transmitter. In addition the 32 MHz oscillator, which supplies the primary frequency to the receivers, is located on this card. Figure 4.2.2.2-1 is a block diagram showing the interface connections to the data bus. Each receiver provides three inputs to a programmable peripheral interface device. The inputs are a clock, a frame marker, and the data. The clock is used to signal the input port that a data bit is present on the data line. The frame marker denotes that bit one

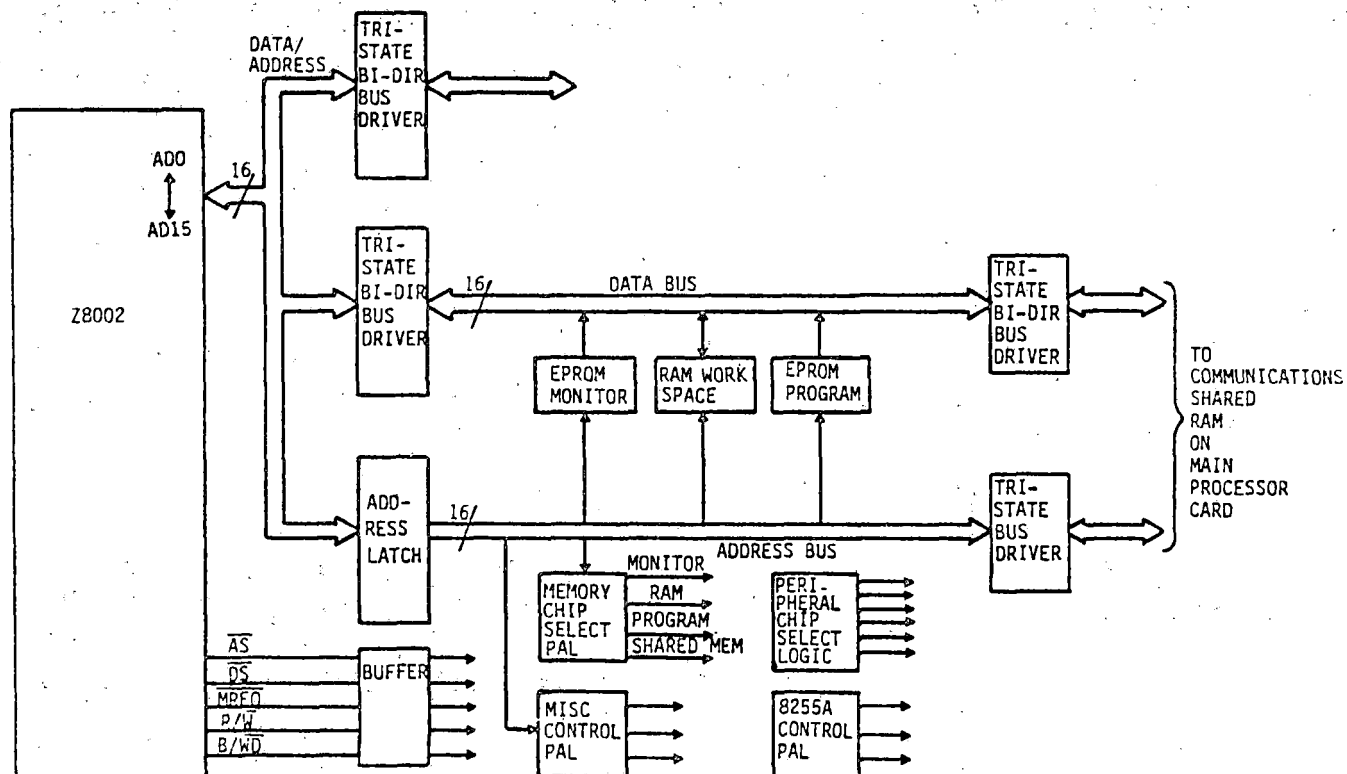


FIGURE 4.2.2.1-1: COMMUNICATIONS PROCESSOR MEMORY AND CONTROL DIAGRAM



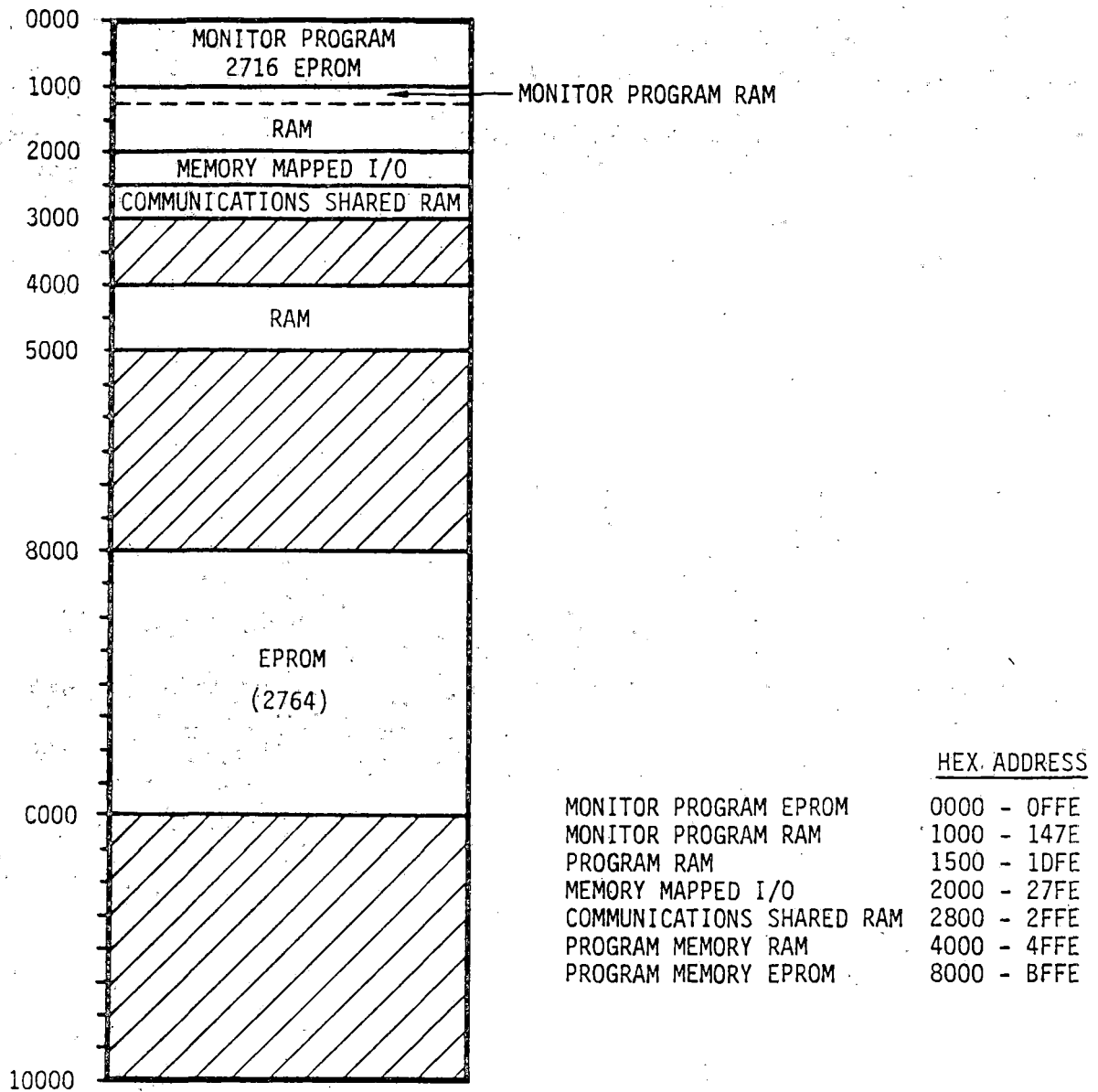


FIGURE 4.2.2.1-2: VCU COMMUNICATIONS PROCESSOR MEMORY CONFIGURATION

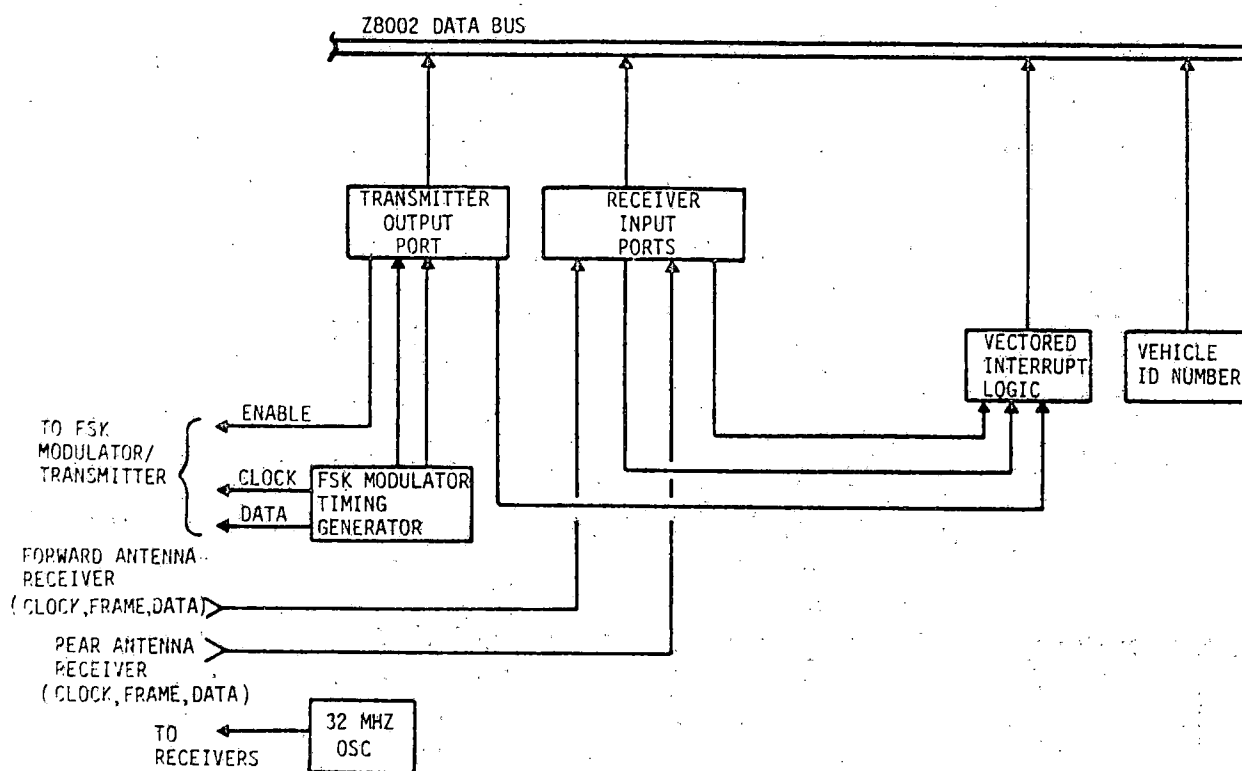


FIGURE 4.2.2.2-1: RECEIVERS/TRANSMITTER INTERFACE

of a message is the current data bit. When a clock pulse is sensed by the input port peripheral device, the interface device sends an interrupt to the vectored interrupt logic. The logic sends an interrupt to the microprocessor, which answers the interrupt by first taking an address vector from the logic which vectors the program to the appropriate receiver data input routine. This is a continual process since up-link FSK data is normally transmitted continuously.

The outputting of FSK data requires the microprocessor to enable the output port peripheral device whenever a message is to be transmitted. When the device is ready it sends an interrupt to the vectored interrupt logic, which in turn sends an interrupt to the microprocessor. The microprocessor takes the address vector and goes to the data output routine and outputs one bit of data to the output device. After that bit has been transmitted the next interrupt is sent; this process continues until all the bits of the message or messages have been sent.

#### 4.2.2.3 Store/Recall Pulse Generation

The non-volatile RAM, located on the Main Processor card, requires a "Store" and "Recall" pulse when power is turned off and on. The required circuitry is located on the Communications Processor card because of space considerations. The "Store" pulse circuit senses when the voltage decreases below 4.72 volts and generates a Store pulse that is fed to the NOVRAM. A large capacitor maintains the voltage above 4.5 volts on the NOVRAM and the pulse circuit long enough to complete the store operation.

The "Recall" pulse circuit generates a pulse of approximately 500 milliseconds whenever power is applied to the VCU. A pulse of that width ensures all the circuits are stable and no spurious Store pulses are generated (the Recall pulse inhibits the Store pulse).

### 4.2.3 Timing Functions

Figure 4.2.3-1 shows the system timing configuration. The timing card contains the Master Oscillator and the logic necessary to derive the needed signals for the two channels. In addition the Master reset function, which is also common to both channels, is located on this card. Figure 4.2.3-2 is a photograph of the Timing card. The functions performed on this card are few; therefore, the card is only partially populated.

The Master Oscillator frequency was chosen to be 24 MHz. This particular frequency was chosen to accommodate a large number of possible frequencies that might be needed during the design phase. A frequency of 24 MHz readily divides down to 12, 8, 6, 4, 3, 2, and 1 MHz using standard digital counter circuits. In the final configuration, 4 MHz was the highest frequency used. The 4 MHz clock is fed to Main Processor 1 and the inverted 4 MHz is sent to Main Processor 2. The 4 MHz is counted down to a 100 Hz pulse (10 Millisecond Interrupt), and sent to both Main Processors. The 100 Hz is further divided by four and used to resynchronize the Watchdog Timer circuits (N/4 Resync).

### 4.2.4 Digital I/O

The Digital I/O Card (Figure 4.2.4-1) contains circuitry to interface the Main Processor to the discrete input and output signals, provides the communications link with the propulsion controller, and contains the buffer unit for output of the digital test point data. In addition, this card contains the four Odometer Preprocessor microcomputers and their support circuitry. Circuit layout is indicated in Figure 4.2.4-2.

An important design requirement in interface circuitry is protection of the low power level VCU circuits from the severe electrical noise created by vehicle subsystems, particularly the propulsion unit and the rail power collectors. In order to minimize this noise contamination, discrete signals are isolated either optically or magnetically (Figure 4.2.4-3).

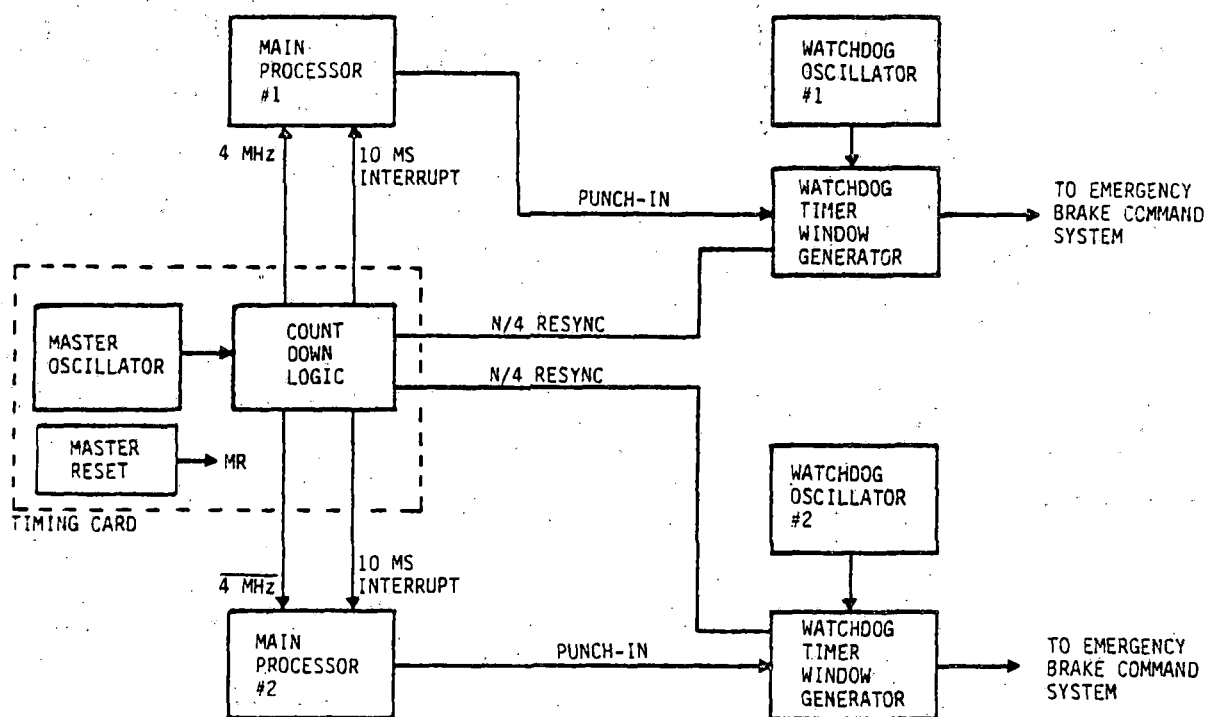


FIGURE 4.2.3-1: SYSTEM TIMING CONFIGURATION

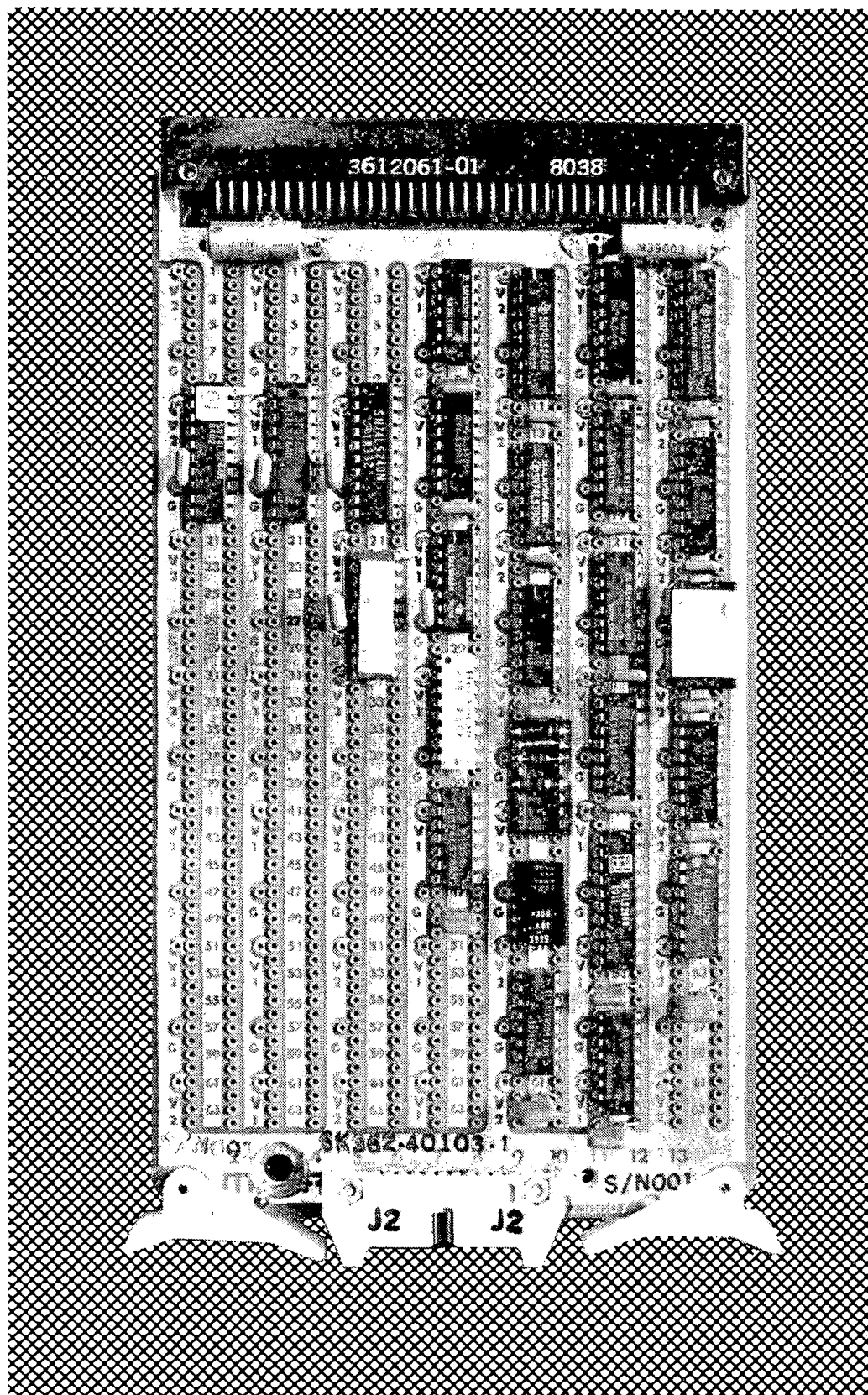


FIGURE 4.2.3-2: TIMING CARD

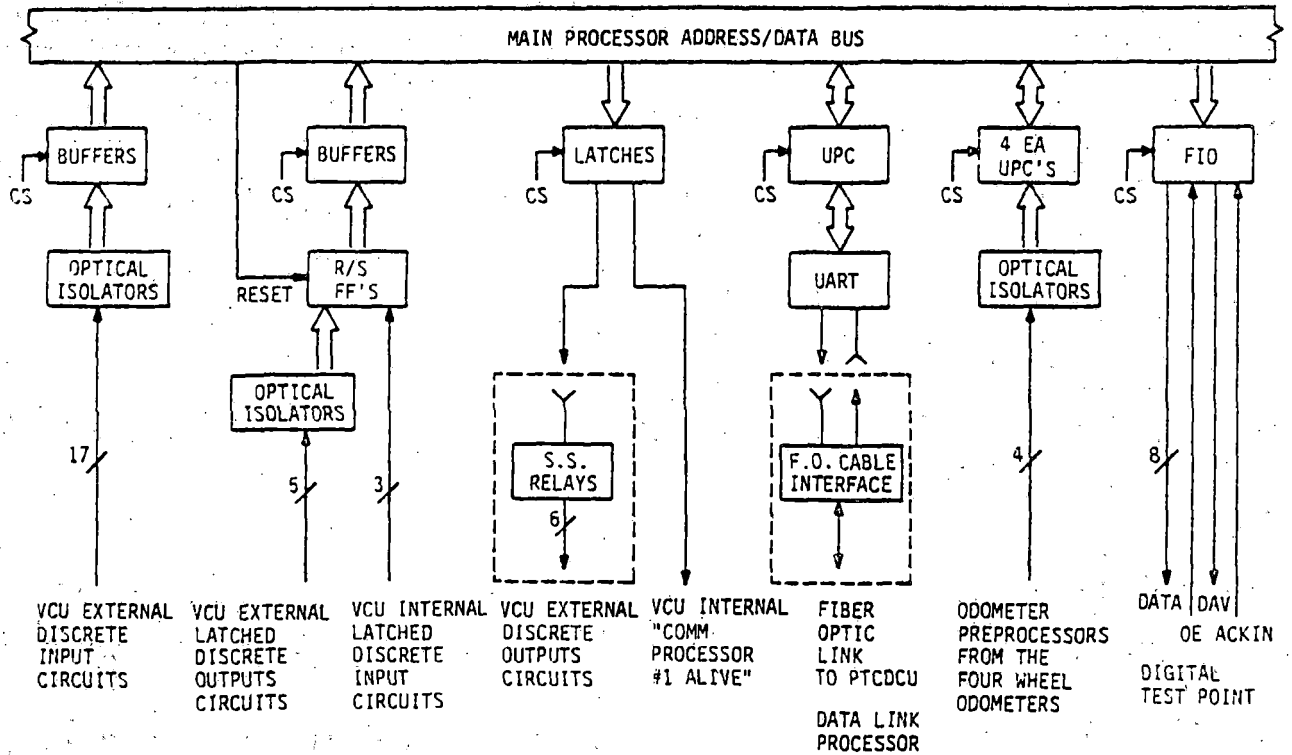


FIGURE 4.2.4-1: DIGITAL I/O CARD FUNCTIONS

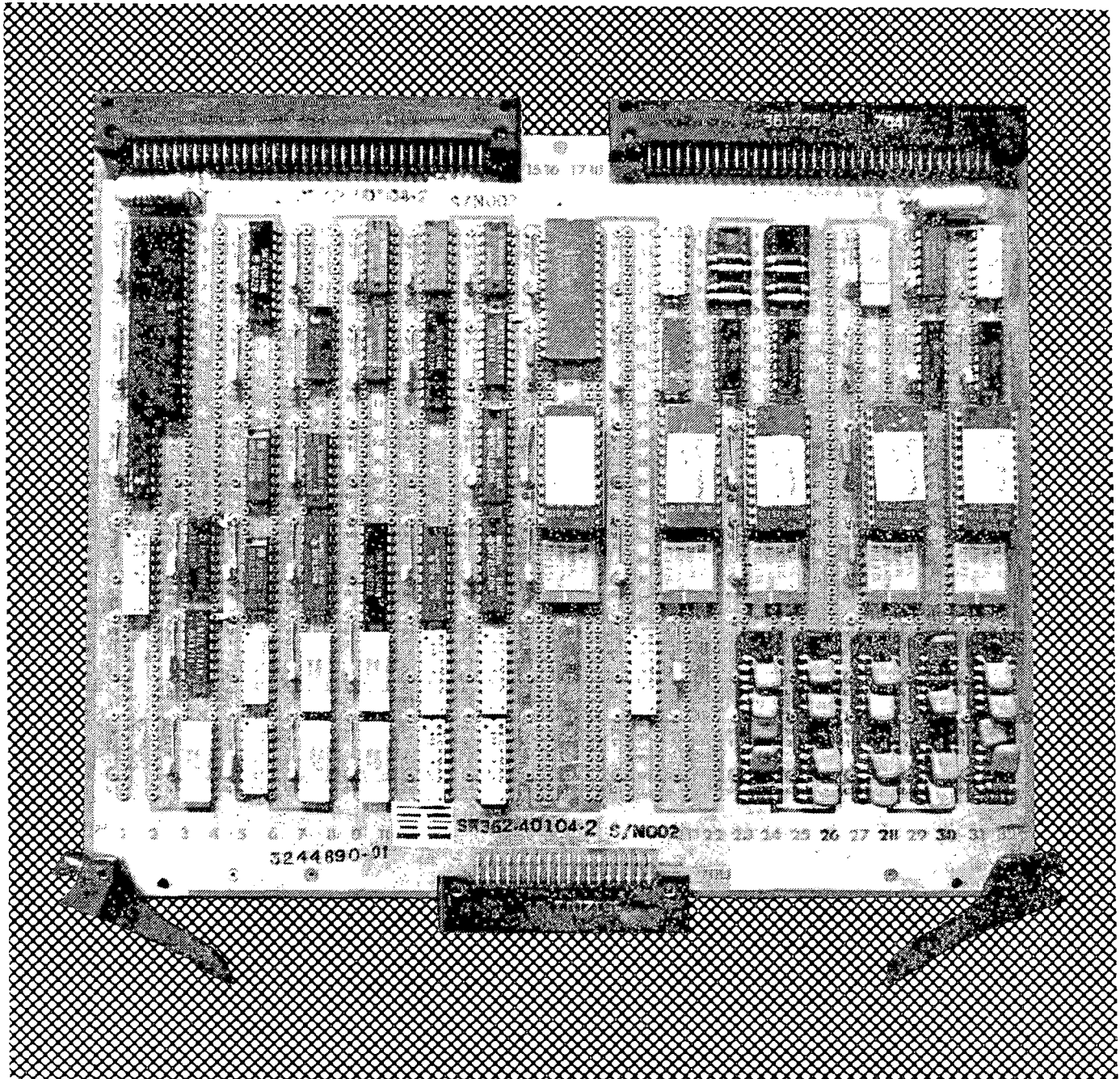


FIGURE 4.2.4-2: DIGITAL I/O CARD



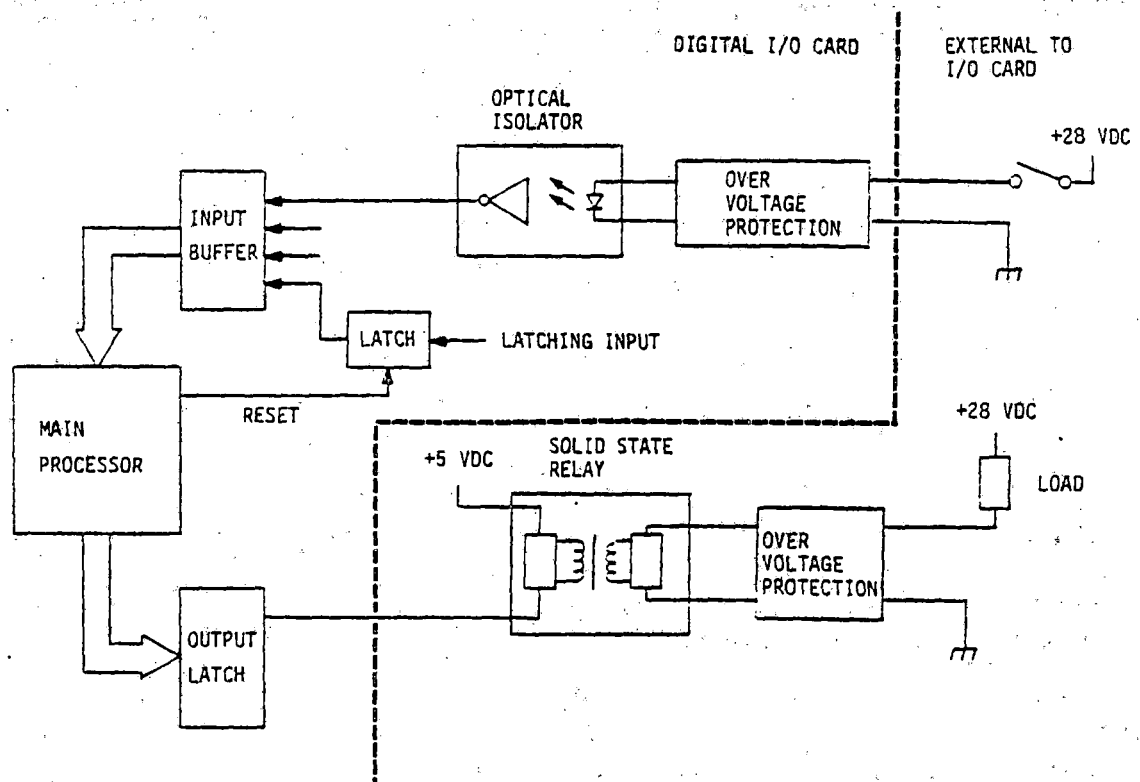


FIGURE 4.2.4-3: DISCRETE INPUT/OUTPUT SIGNALS

Each discrete input signal that originates outside the VCU enclosure (always generated by a 28 VDC circuit) is routed through an overvoltage protection circuit which provides diode protection against reverse voltage and an RC filter to reduce noise spike amplitudes. The filter resistor also serves to establish the current level for the light emitting diode in the optical isolator.

All discrete input signals are enabled onto the Main Processor data bus via a tri-state buffer activated by the appropriate chip select. In the case of latched discrete inputs, which includes those signals associated with onboard magnetically activated reed switches, R-S flipflop circuits preceeding the buffers latch the discrete input state changes; the Main Processor clears these flipflops following a read of the data.

Discrete output signals are magnetically coupled to vehicle actuators via solid state relays. The Discrete I/O Card contains the latches necessary to hold the output data, but does not carry the relays and associated protection circuitry which would be mounted external to the VCU enclosure to minimize the effects of switching noise.

Communications between the VCU electronics and the Propulsion Torque Command Data Conversion Unit (PTCDCU), an electronics subassembly attached to the propulsion unit controller assembly, is carried out using serial data transmission over fiber optic lines. This approach provides the maximum isolation between the VCU and the extremely noisy propulsion unit. The interface to the PTCDCU fiber optic cable pair, the Data Link Processor, is comprised of an Universal Peripheral Controller (UPC) and an Asynchronous Receiver/Transmitter (UART). The UPC, an 8-bit microcomputer, features a two-port RAM that allows asynchronous data communication between the Z8002 and the microcomputer. In operation, the UPC accepts commanded motor torque and motor switch state values from the Z8002 and formats them for serial data transmission to the PTCDCU. Serial data from the PTCDCU, which includes measured motor torque and discrete status data, are decoded, filtered, and made available to the Z8002 via the two-port RAM.

Four UPC units provide the preprocessing of the wheel odometer signals. Toothed gears (refer to Figure 4.2.4-4), one mounted at each wheel, produce pulses in Hall-effect pickups. The four pulse signals are routed via optical isolators and Schmitt triggers to their respective UPC preprocessors. Pulse period and frequency are calculated using a 200 KHZ clock reference and the data made available to the Z8002.

Digital test point data, which consists of internal VCU data selected and scaled for testing purposes, is made available via a programmable 128X8 bit first-in-first-out (FIFO) circuit (Zilog Z8038 Z-FIO). This device allows loading of data by the Z8002 and unloading of data by an external device simultaneously. Two lines indicating data available and data ready implement a simple protocol to manage the asynchronous communications. No special isolation is used for the data and control signal buffers, as this circuit is intended for test purposes only.

#### 4.2.5 Analog I/O

The Analog I/O Card (Figure 4.2.5-1) is constructed to support the analog data conversion circuitry necessary for the following interface signals: commanded brake torque, analog test point outputs, caliper pressure, and battery bus voltage. The triple-wide Mupac card uses an analog groundplane with plus and minus 15 VDC carried on the top side power busses. The central portion of the circuit board, designed to carry the control logic for the data conversion circuits and the circuitry for the Odometer Data Downlink Collision Avoidance System (ODDCAS) to VCU interface (a digital function), is bussed separately for 5 VDC and digital ground (see Figure 4.2.5-2).

Both the brake command signal and the analog test points (which have 8 identical channels) use 12-bit successive approximation type digital to analog converters (DAC). Each DAC contains on chip registers that latch in the digital code value from the Main Processor data bus when selected by the appropriate chip select. The DAC current output is converted to a voltage and applied to an output buffer amplifier. Circuitry for the test points and the brake command signal are similar; however, the brake

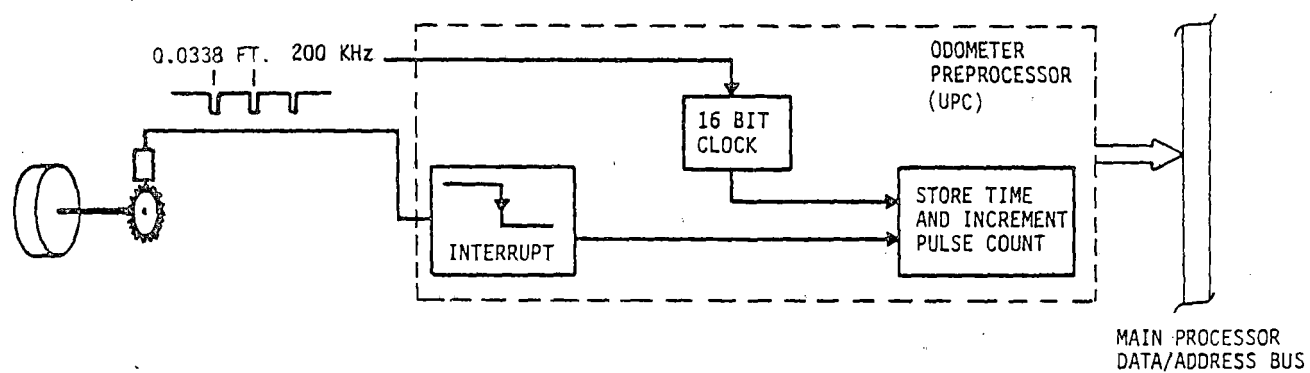


FIGURE 4.2.4-4: BASIC SPEED AND POSITION MEASUREMENT SYSTEM

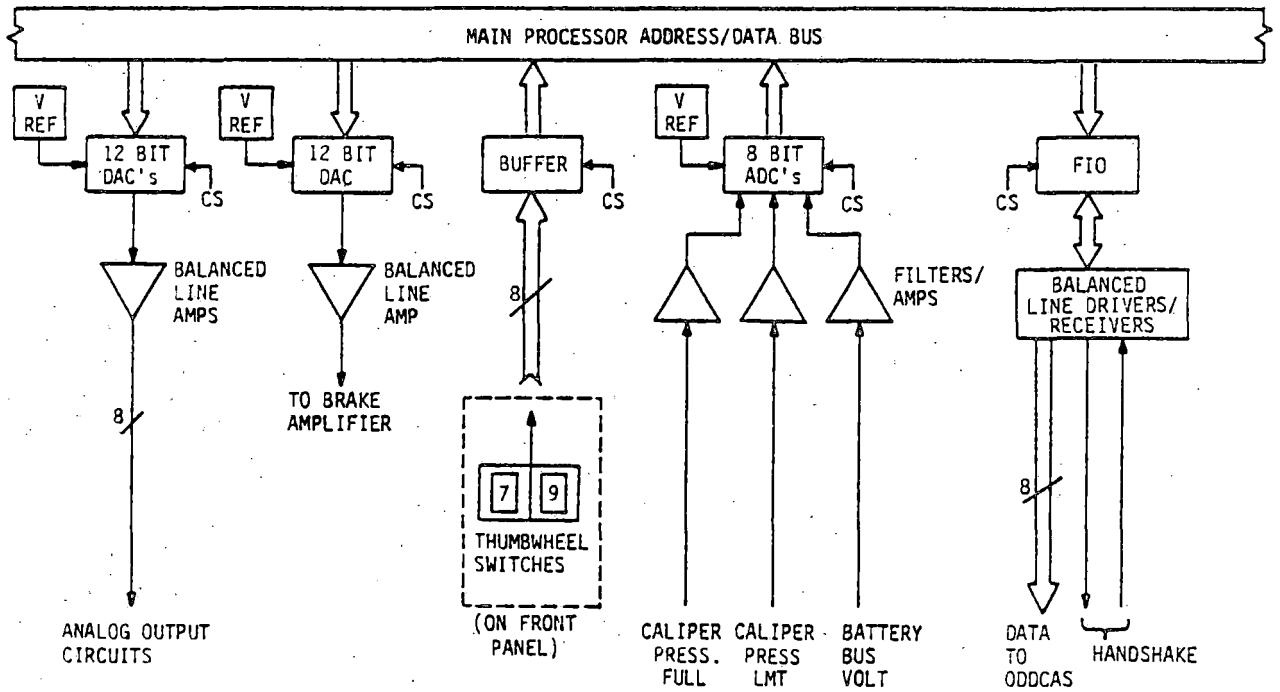


FIGURE 4.2.5-1: ANALOG I/O CARD FUNCTIONS

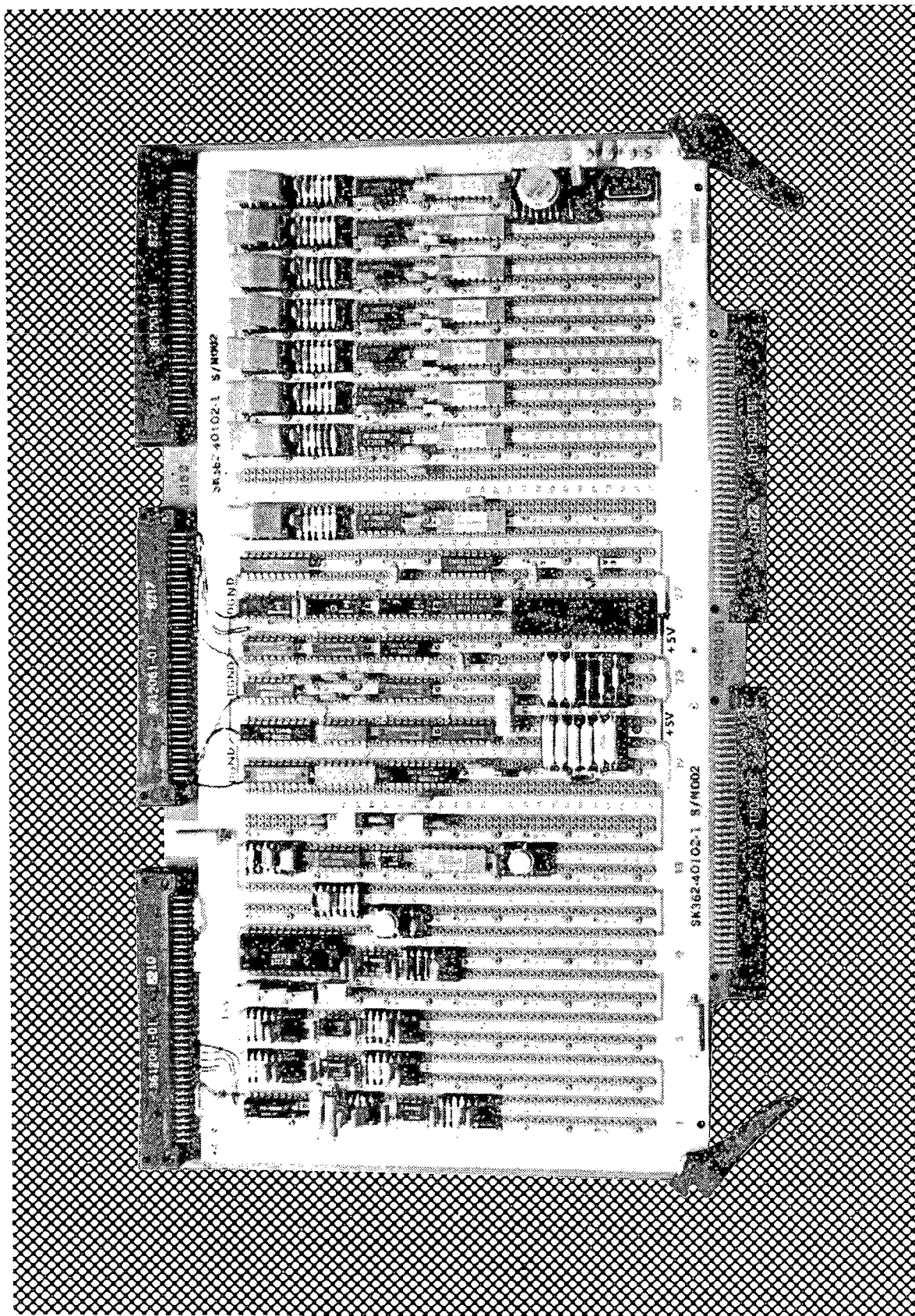


FIGURE 4.2.5-2: ANALOG I/O CARD

command circuitry contains trimming controls to allow it to meet stringent offset and gain tolerances.

The two caliper pressure signals (full range and limited range) and the battery bus voltage signal are sampled and converted to digital words with an 8-bit analog to digital converter (ADC). The particular ADC used, an Analog Devices AD7581, continuously converts up to 8 input channels and places the digital data into an 8 X 8 dual-port memory; in this application, only the first three channels are used. The Main Processor may access the dual-port memory at any time and read the latest data value. A common-mode choke and an active low-pass filter in each channel protect circuitry from common-mode noise and limit the differential noise bandwidth.

ODDCAS data is transferred to the Vehicle Collision Avoidance Processor (VCASP) via a Zilog Z8038 first-in-first-out (FIFO) unit. The 8 parallel data lines and two handshake lines are buffered with optical isolators, providing system to system electrical isolation.

The digital section of the card contains a tri-state buffer for thumb-wheel switches mounted on the front panel of the VCU. Selection by the Main Processor enables the buffer onto the data lines, transferring the two-digit binary coded decimal values (00 to 99) to the CPU.

#### 4.2.6 External RS232 Interface

In any complex control system involving microprocessors and memory, it is essential that there is a means to insert and extract information. This is especially true during the development phase of a microprocessor system. The External RS232 Interface card provides this capability. Figure 4.2.6-1 is a block diagram of the card and Figure 4.2.6-2 is a photograph of the card. Actually there are two identical circuits as shown on the block diagram, one for each of the 16-bit microprocessors in a VCU channel.

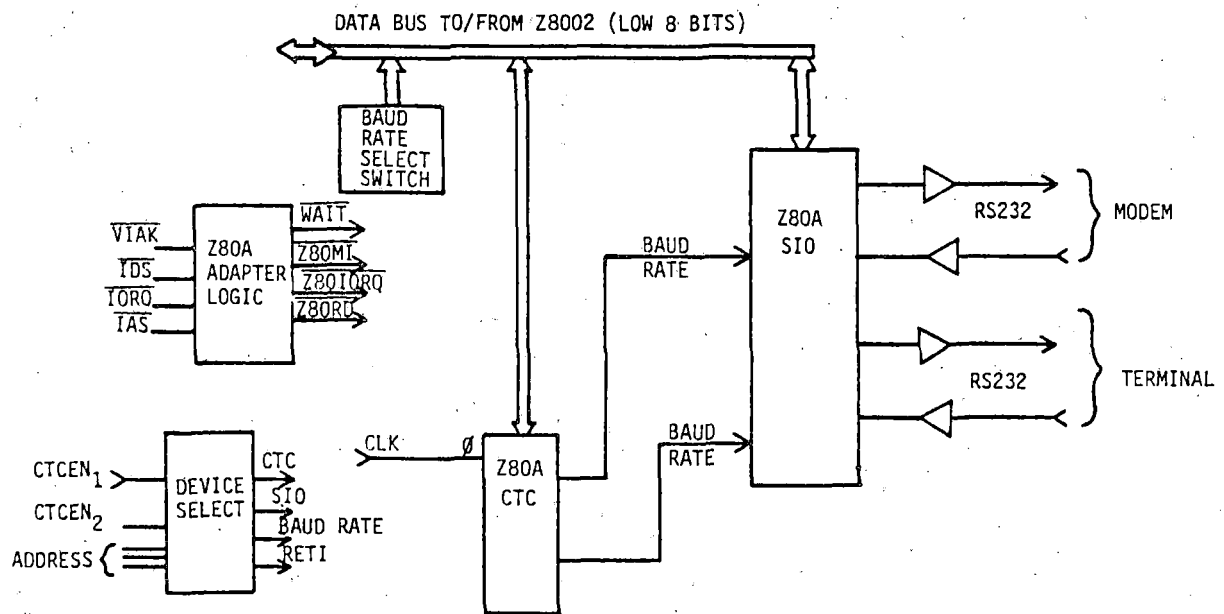


FIGURE 4.2.6-1: EXTERNAL RS232 INTERFACE CARD BLOCK DIAGRAM



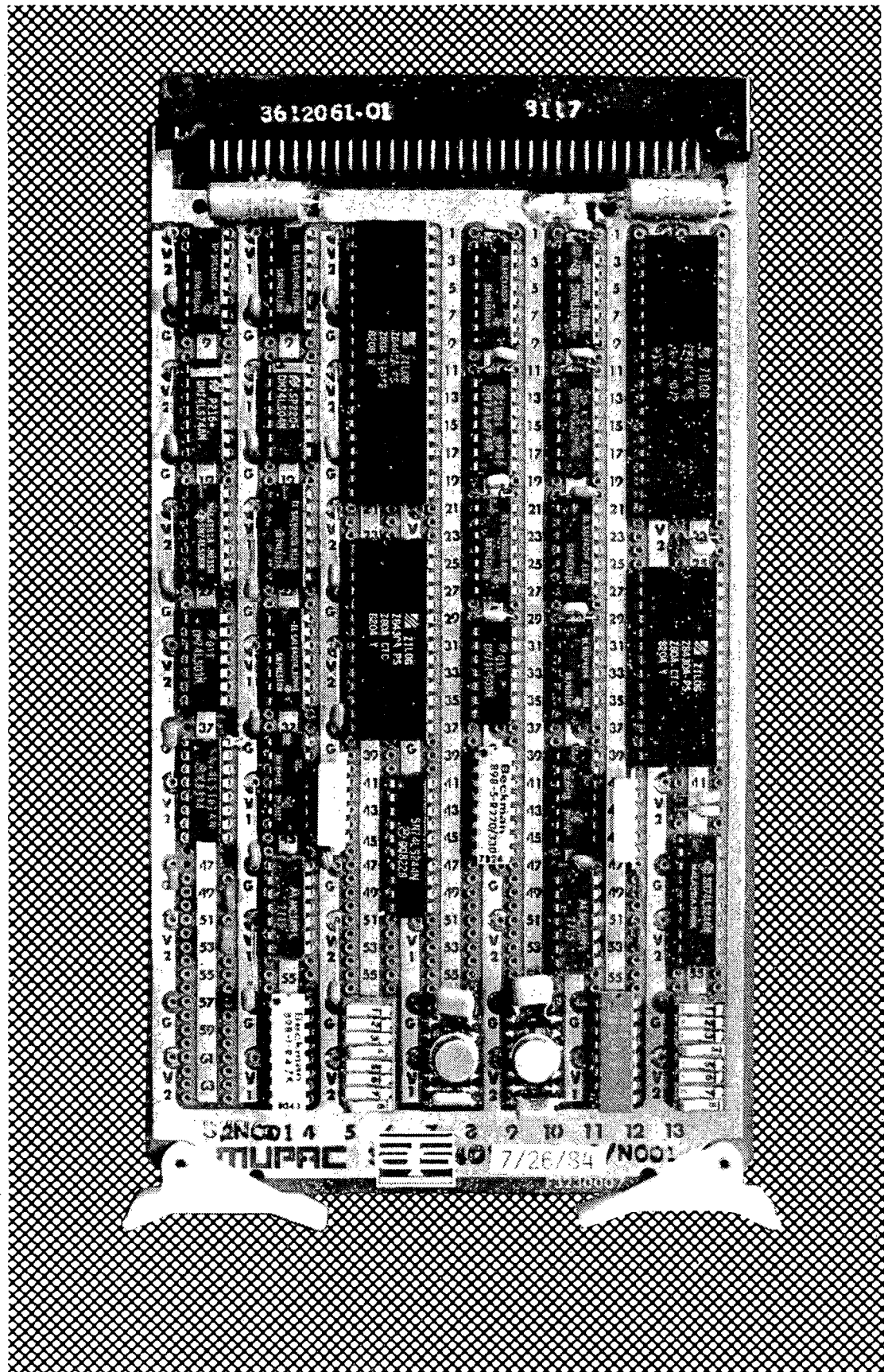


FIGURE 4.2.6-2: EXTERNAL RS232 INTERFACE CARD

The circuit is quite simple; a Serial I/O (SIO) chip, a Counter Timer chip (CTC), and Device Select and Adapter logic. Both the SIO and CTC chips are Z8002 bus compatible. The baud rate select is normally set to 1200 baud. With a front panel select switch the system can be put into the Monitor mode. In this mode, the Z8002 microprocessor communicates with a terminal (operator interface) and a modem (download programs if desired) through an RS232 serial interface.

#### 4.2.7 Propulsion Torque Command Data Conversion Unit

The Propulsion Torque Command Data Conversion Unit (PTCDCU) is a special purpose piece of hardware designed to interface between the AGRT VCU and the modified MPM propulsion unit. The PTCDCU would not be employed in an operational AGRT as the Propulsion Controller itself would contain the necessary interface circuitry. However, a design description of the PTCDCU is included since it is a part of the configuration that was tested.

Figure 4.2.7-1 presents an overview of the VCU/Propulsion system interface, and Figure 4.2.7-2 is a picture of the unit. The purpose of the interface is to transfer data between the VCU and the Propulsion Controller while protecting the VCU and the interface circuitry from the effects of noise generated by the propulsion unit. These signals include commanded and measured motor torque (both analog signals) and the propulsion enable switch closure and motor status signals (all discrete signals).

The PTCDCU is physically located near the propulsion unit. Signals between the VCU and the propulsion subsystem are carried in serial, digital form over fiber optic cables. The fiber optic link eliminates electrical noise interference on the connecting cables. The discrete signals are input to the PTCDCU through optical isolators to minimize electrical noise interference.

The VCU end of the data link is managed by a dedicated interface circuit, the Data Link Processor. The data link is implemented in a

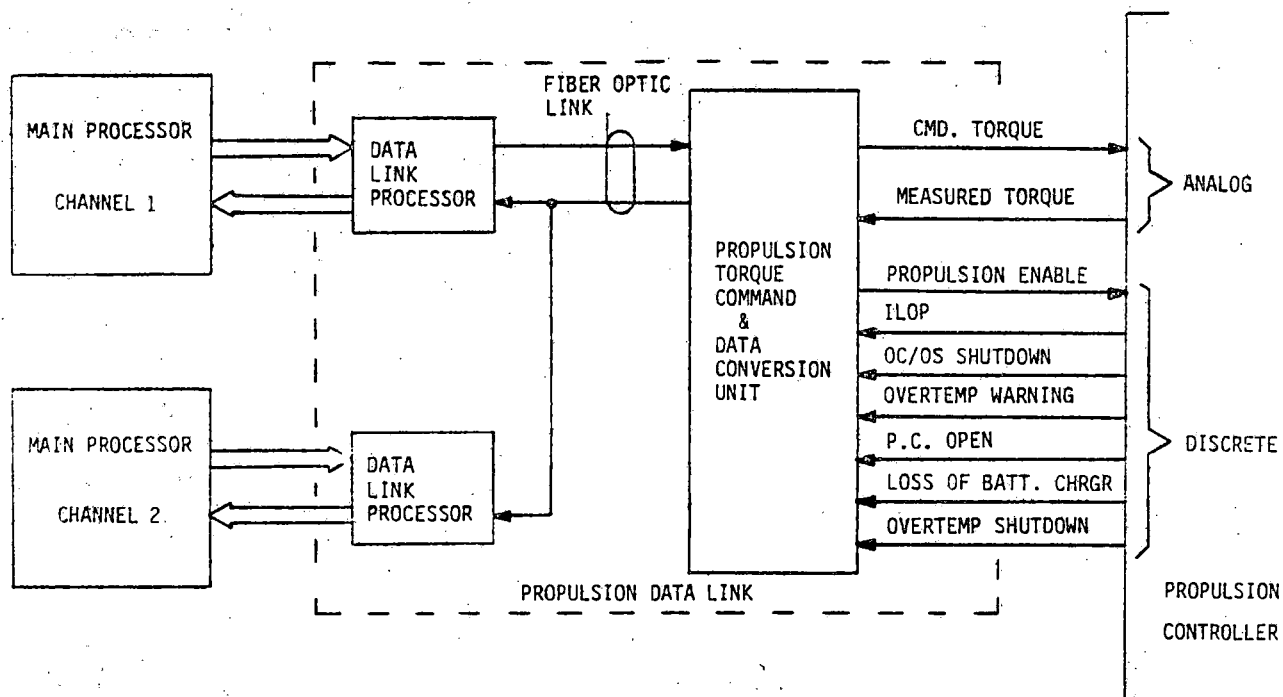


FIGURE 4.2.7-1: VCU/PROPULSION SYSTEM INTERFACE

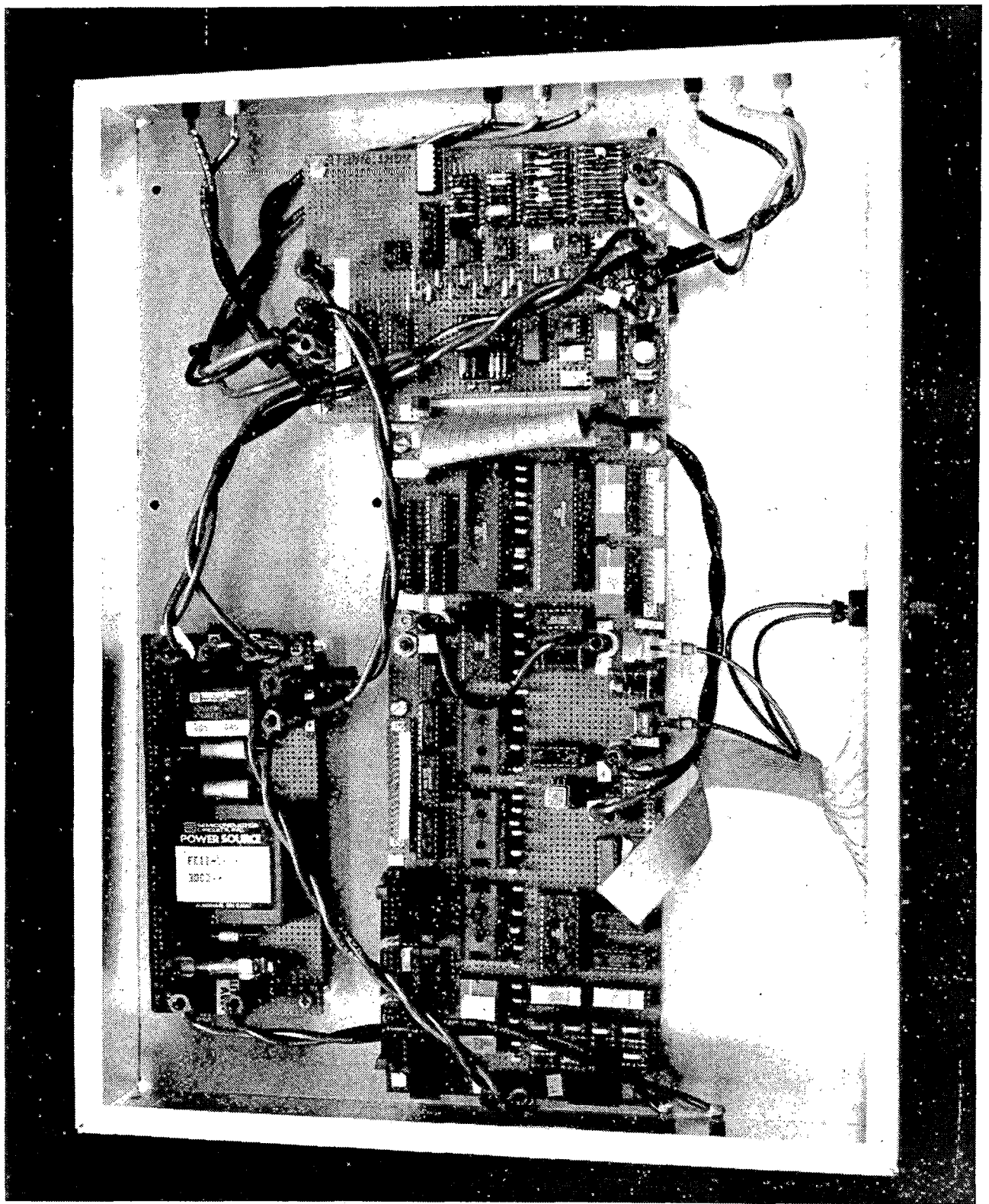


FIGURE 4.2.7-2: PHOTOGRAPH OF PTCDCU

"single thread" fashion: only one of the redundant VCU channels issues the voted commanded torque signal and the propulsion enable signal to the PTCDCU. The measured propulsion torque and discrete status signals, processed and transmitted to the VCU by the PTCDCU, are distributed to both VCU channels. This arrangement at the VCU end of the data link supports a dually redundant propulsion control system that, although not implemented, forms the baseline AGRT configuration. The PTCDCU (Figure 4.2.7-3) is a data acquisition/transmission system organized around the RCA 1802 CMOS microprocessor. CMOS technology is utilized for the logic elements as well as a portion of the analog circuitry to gain reduced power consumption and improved noise immunity. The data communication chores are performed by a Universal Asynchronous Receiver Transmitter (UART) configured for full-duplex asynchronous operation.

The PTCDCU operates on a 10 millisecond cycle, initiated by transmission of a commanded motor torque value and a Propulsion Enable switch state from the Data Link Processor. The commanded torque, sent as a 12-bit unsigned binary number, is applied to a 12-bit D/A converter. The analog signal is then low-pass filtered and sent through a balanced driver to the propulsion controller. The Propulsion Enable command opens or closes a relay attached to the PTCDCU that provides the switch closure enabling the motor contactor.

Discrete and analog status data from the Propulsion Controller are processed by the PTCDCU each 10 msec cycle. The measured torque signal is converted into an unsigned eight bit binary number; required signal processing elements include an input difference amplifier, anti-aliasing low pass filter, sample and hold amplifier, and an eight bit analog to digital converter. Discrete signal states at the parallel data interface are sampled and this data, along with the digital measured torque value and a code indicating PTCDCU error conditions, are packed into bytes and transmitted back to the Data Link Processor.

Since the VCU cannot directly reset the 1802 the PTCDCU, in order to reach a safe state in the event of data link failure or initialization, incorporates a watchdog timer circuit. A countdown chain produces a

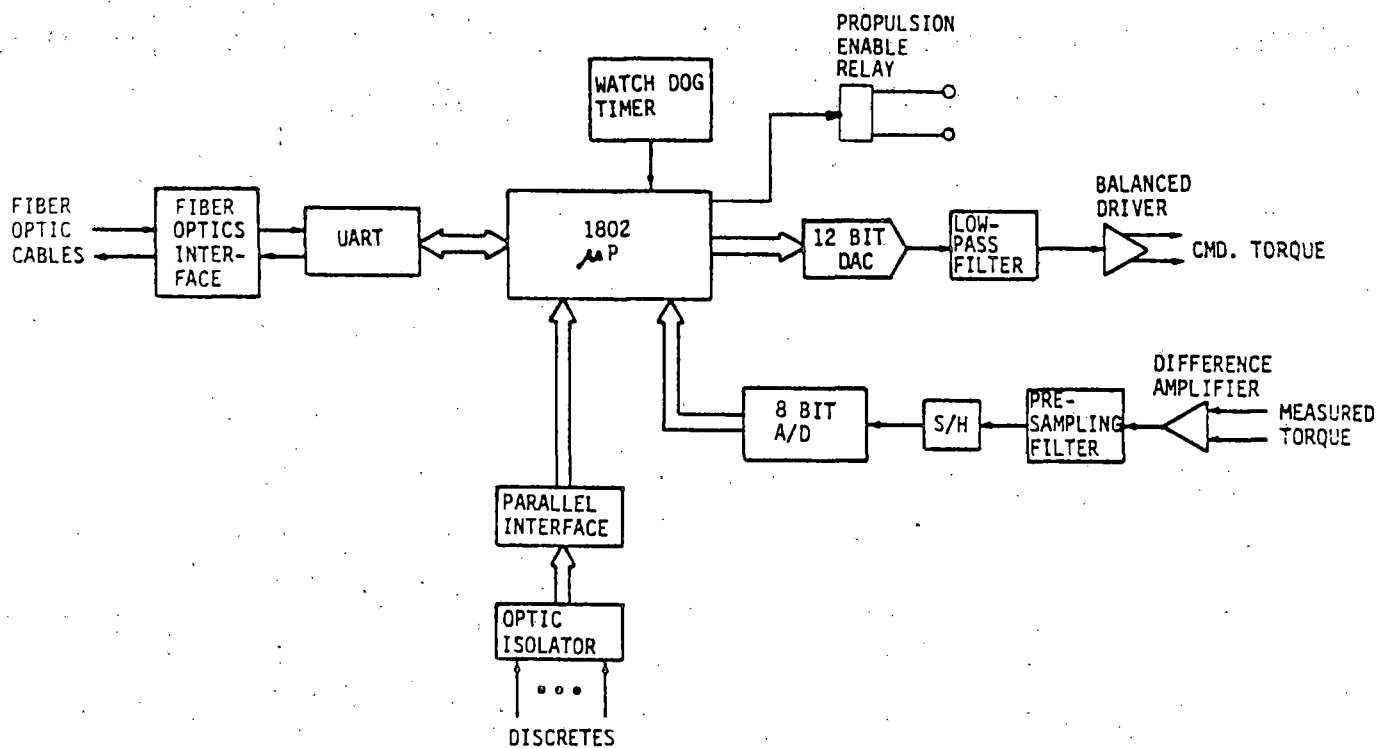


FIGURE 4.2.7-3: PTCDCU BLOCK DIAGRAM

pulse every 65.6 milliseconds if allowed to completely count down. This pulse, if allowed to occur, resets the microprocessor; this causes the output torque command to go to zero, commands open the Propulsion Enable relay, and initiates a fault message to the VCU. During normal operation the watchdog timer counter chain is reset during each 10 msec cycle.

As illustrated in Figure 4.2.7-4, the propulsion link data transfer involves interaction of three separate processing elements: the VCU Main Processor, the Data Link Processor, and the PTCDCU. Every minor frame (10 msec interval) the Main Processor writes the updated motor torque command value and motor switch command code value to the Data Link Processor two-port RAM and reads the latest measured motor torque, status discretes, and error code data. Following the Main Processor data write operation, the Data Link Processor zeros out the commanded motor torque value and motor switch code in the RAM and transmits this latest data down the link to the PTCDCU. Data received back from the PTCDCU is posted in the two-port RAM. Although the status data is made available to the Main Processor every 10 msec cycle, the data is actually read every major frame (40 msec interval); a digital filter routine in the Data Link Processor reduces the bandwidth of the measured motor torque signal to accommodate this 25 Hz sampling rate.

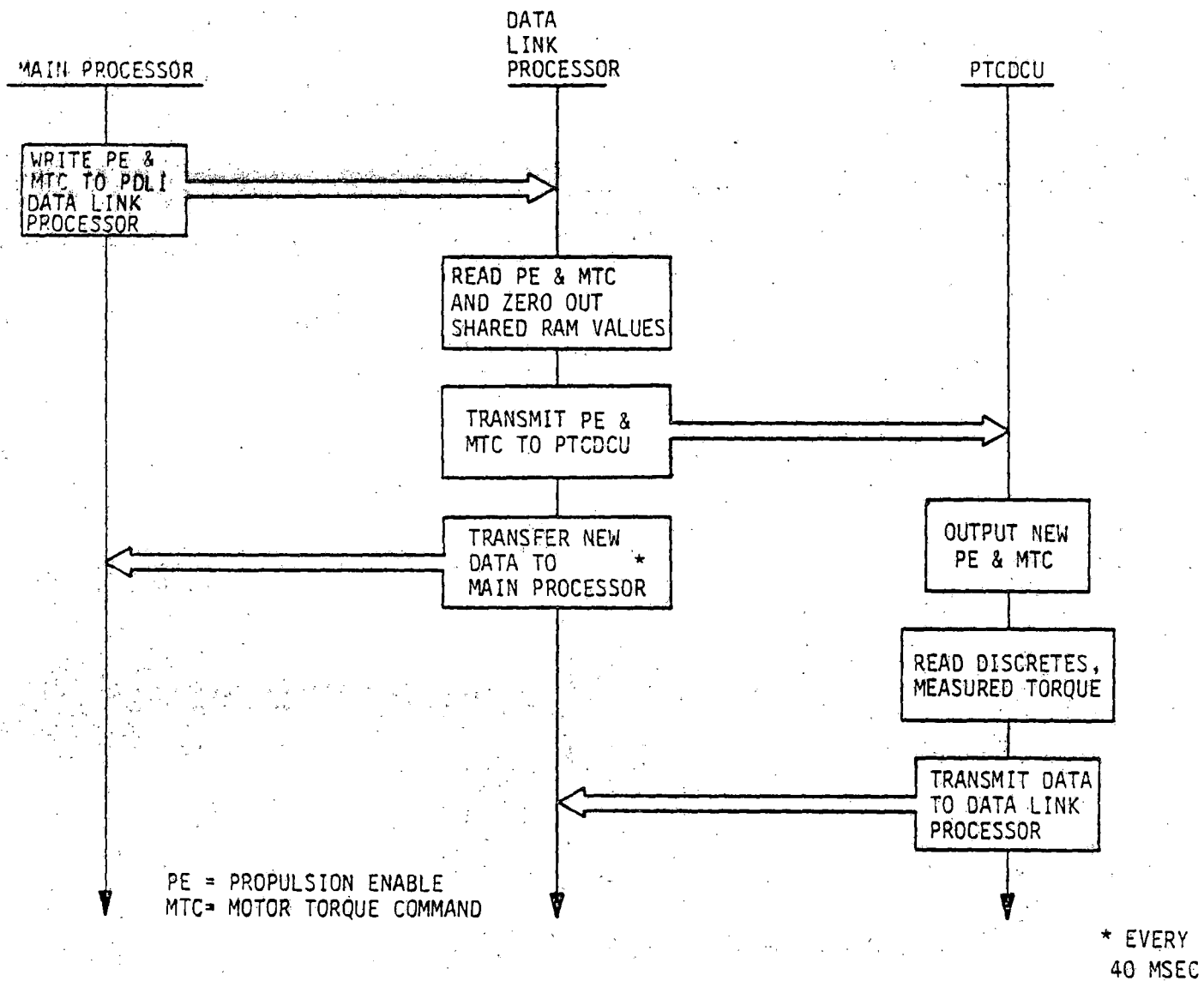


FIGURE 4.2.7-4: DATA TRANSFER IN THE PROPULSION DATA LINK



## 5.0

## DESIGN VERIFICATION

The purpose of this section is to provide an overview of the Design Verification tests as performed on the AGRT VCU and present the results of the tests in the form of a summary sheet for each test or test series.

In addition, an overview of the test set developed for providing a real-time closed-loop test environment, and the test and maintenance features provided within the VCU are discussed.

### 5.1 Test Program Overview

A large portion of the VCU resources are devoted to the control of the longitudinal motion of the vehicle. The VCU, together with an electric propulsion system, a friction braking system and the vehicle itself, form what is called the Vehicle Longitudinal Control System or VLCS. These interactive VCU VLCS functions cannot be adequately tested via simple open-loop input/output checks. Some means of operating the VCU in a real-time closed-loop environment, similar to actual operation on a vehicle, is required to verify correct control system operation.

#### 5.1.1 Design Verification Test Set

An extensive test set was developed to provide the capability to operate, in the laboratory, the final VCU hardware and software in a real-time closed-loop manner. A block diagram of the VCU test setup is shown in Figure 5.1.1-1. The major elements shown are the Test Scenario Generator (TSG), the Test Vehicle Simulator (TVS), and the article to be tested, the VCU. Figure 5.1.1-2 is a picture showing the VCU and the TSG, and Figure 5.1.1-3 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

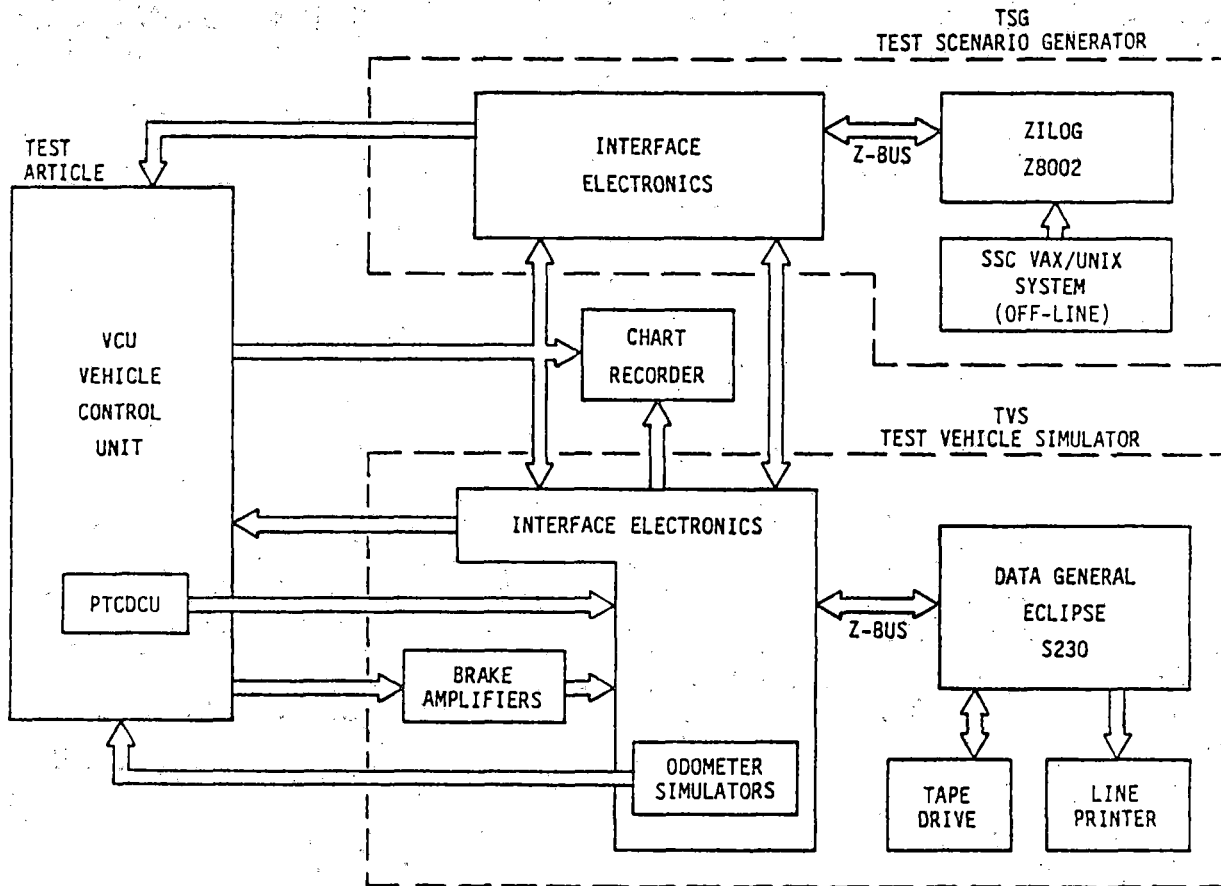


FIGURE 5.1.1-1: DESIGN VERIFICATION TEST CONFIGURATION



FIGURE 5.1.1-2: TEST ARTICLE AND TSG

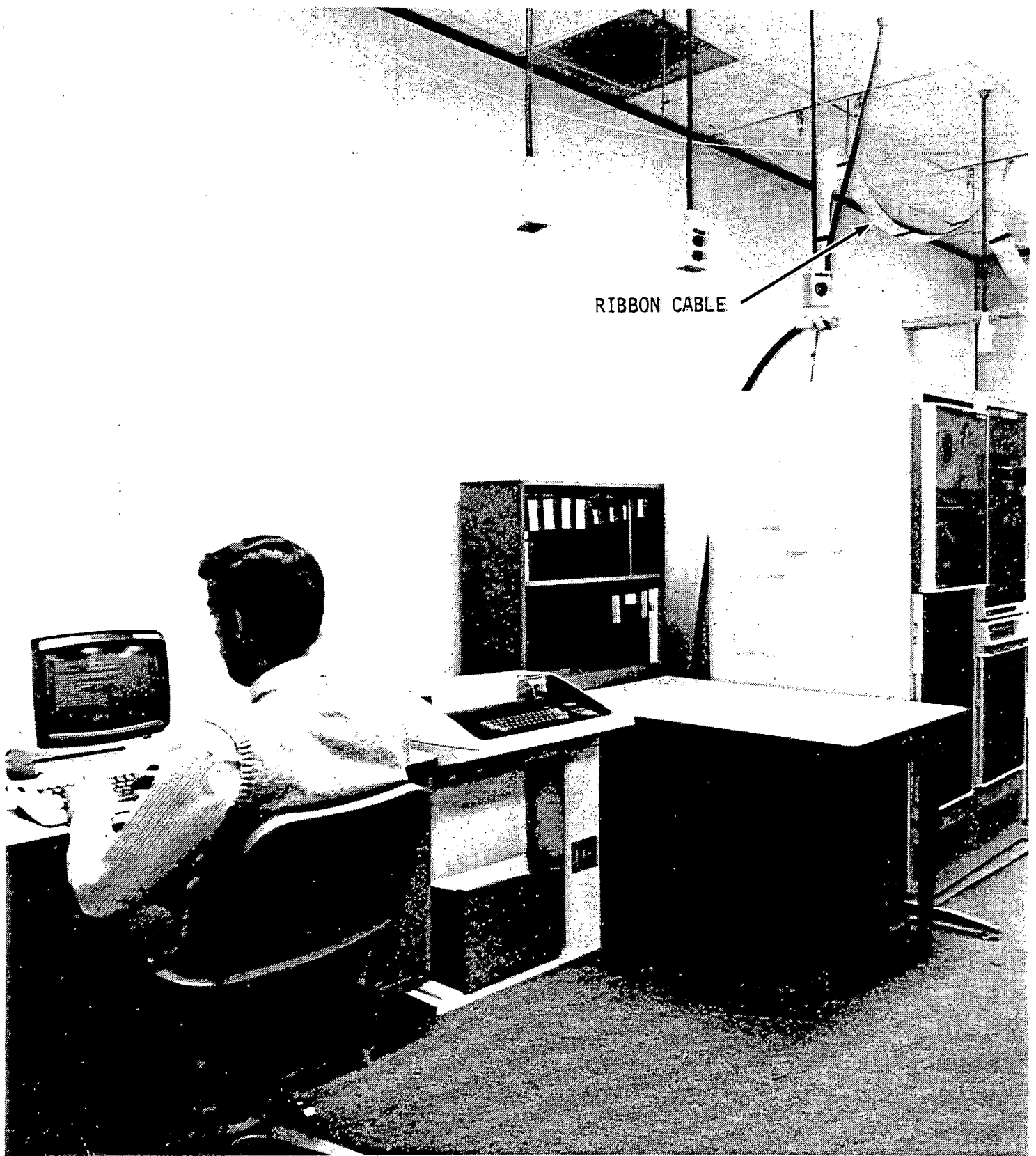


FIGURE 5.1.1-3: TEST VEHICLE SIMULATOR

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.

Primary functions of the TVS are to simulate the motor/brake/vehicle dynamics and to generate odometer pulse trains which are similar to the interface signals that will be seen in actual operation. This function is provided by means of software within a Data General Eclipse S230 minicomputer in conjunction with a set of interface electronics developed for AGRT. Use of a digital computer, rather than an analog computer, allowed for the inclusion of an extensive data collection and data processing capability that would not have been possible with conventional analog computer techniques. The present design provides for the storage of large amounts of test data on tape during a test run. After a test is run, the Eclipse is used to process the data and generate hardcopy listings of the data obtained.

The VCU test set was originally developed to conduct developmental tests of the VLCS algorithms implemented in the VCU using a single-string VCU configuration. In this form, the test setup proved invaluable in identifying and resolving a variety of anomalies. The test set was then extensively upgraded prior to the start of the Design Verification tests. This upgrade added the elements necessary to accommodate a complete dual channel VCU and corrected the majority of the nuisance problems encountered during developmental testing.

#### 5.1.2 Design Verification Tests

The Design Verification test effort, itself, was originally planned as an exhaustive test of all VCU functions and was to be followed by a test track test program using a modified Morgantown People Mover vehicle. This plan was scaled down following receipt of a contract modification

that deleted track testing of a wheeled vehicle and redirected program resources towards the development of a magnetically levitated vehicle configuration.

The philosophy in the revised test program 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 5.1.2-1 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.

### 5.1.3 Summary and Conclusion 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. This action was taken, to conserve resources, in areas where additional changes are anticipated as a result of the current emphasis on a magnetically levitated vehicle and longer headway systems. In all cases, careful problem tracking and correction records have been maintained to support potential future uses of the current design.



TABLE 5.1.2-1: VCU TEST PROGRAM OVERVIEW

FUNCTION	OBJECTIVES	Test Type	SPEC PARA (System / VCU)	SUCCESS CRITERIA
1.0 VCU INITIALIZATION	Verify that the VCU issues safe commands during initialization.	S	V-3.2.4 3.5.2.4	Commands initialized to safe state: - doors commanded closed - emergency brake hold-off withheld (initially) - forced brakes commanded - propulsion off commanded. Dispatch requests not honored.
	Verify command and internal status is correct after initialization.	S	V-3.2.4	Commands at safe state at end of initialization - as above except emergency brake hold-off present. Brake torque command at forced brake level and propulsion command at minimum level. Parameters initialized properly. Dispatch requests honored.
	Verify that commands are in safe state after initialization failure.	S	V-3.2.4	Initialization failure leaves - doors commanded closed - emergency brake hold-off withheld - forced brakes commanded - propulsion off commanded. Dispatch requests not honored.
2.0 LONGITUDINAL CONTROL - Routine			S-2.3.2	
2.1 Speed and Position Measurement	Verify odometer accuracy.	S	V-3.2.2.1 3.2.2.1.3 3.5.2.6.2.1 3.5.2.6.2.2 S-2.1.1.3 3.1.2.6.4 V-3.5.2.6.2.3 V-3.4.1.6	Measurement error within specified limits (0.997 probability) for: Centerline speed Long term centerline position  Odometer calibration correct. Odometer interface correct.
	Verify selection of default calibration factor	S	V-3.5.2.6.3	Manual selection sets default calibration factor to .0173 ft/pulse.
2.2 Speed and Position Control	Verify regulation of speed, position jerk, and acceleration.	S	V-3.2.2.1 3.5.2.7.2 (.1-.4) V-3.2.2.1.1 S-3.1.2.5.7.2 3.1.2.5.8.1 3.1.2.6.1 V-3.2.2.1.2 V-3.5.2.7.3	Speed and position regulation and jerk and acceleration within specified limits during: constant line speed speed changes  Brake and Motor commands correct and properly conditioned.
	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, (measured speed < 0.4 f/s) forced brakes are commanded. Command continues until dispatch.
2.3 VLCS Stability Margin	Verify stability margin meets performance and reliability goals.	S	None - implied requirement	Gain margins > or = 6 db for operating conditions assumed in analysis.

TABLE 5.1.2-1: VCU TEST PROGRAM 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	Verify response to position update and speed change cmds.	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	Verify accuracy of station stop.	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-3.2.2.1 3.5.2.7.1.2 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	Verify timing and profile of emergency rate 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	Verify switchover to open loop emergency braking occurs as required.	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	Verify transmission of CAS data.	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	Verify that all FSK Messages are processed.	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 5.1.2-1: VCU TEST PROGRAM OVERVIEW (Cont.)

FUNCTION	OBJECTIVES	Test Type	SPEC PARA (System / VCU)	SUCCESS CRITERIA
6.0 ANOMALY RESPONSE				
6.1 FSK Uplink Anomaly	Verify invalid messages are detected.	S	V-3.5.2.2.1	Message flagged as invalid when CRC fails or bit count incorrect.
	Verify response to loss of speed limit communication.	S	V-3.5.2.11.2.2	Normal rate stop commanded and speed limit profiled to zero when no valid message received from forward antenna for 0.40 sec. Communication loss reported.
6.2 Overspeed Protection	Verify response to speed limit violation.	S	V-3.2.3.3 3.5.2.11.2 3.5.2.11.2.2	Speed limit violation initiates closed loop emergency stop. Violation reported.
	Verify profiling of speed limit decrease.	S	V-3.5.2.11.2.2	Downward speed limit change profiled per specification.
	Verify detection of speed limit error or message loss.	S	V-3.5.2.11.2.1	Speed limit flagged invalid and old speed limit retained when no valid message received from forward antenna or VRC fails.
6.3 Safe to Proceed Loss	Verify reaction to STP removal.	S	V-3.5.2.11.3 S-3.1.2.12	Closed loop emergency stop initiated unless both processors receive STP from the forward or aft antenna.
	Verify reaction time for STP loss.	S	V-3.2.11.3 S-2.1.1.1	STP removal for 30 ms or more initiates emergency stop within 50 ms of initial STP loss. (— STP loss reported)
6.4 Fault Induced Stop	Verify open loop brake initiation.	S	V-3.2.2.2 3.5.2.11.4 6.4	Anomalies listed in table 6.4-1 interrupt the emergency brake hold-off resulting in an open loop stop.
	Verify closed loop emergency stop initiation.	S	V-3.2.2.2 6.4	Anomalies listed in table 6.4-2 initiate a closed loop emergency stop.
	Verify irrevocable normal rate stop initiation.	S	V-6.4 S-3.1.2.5.7.1	Anomalies listed in table 6.4-3 initiate an irrevocable normal rate stop.
	Verify revocable normal rate stop initiation.	S	V-6.4 S-3.1.2.5.7.1	Anomalies listed in table 6.4-4 initiate a revocable normal rate stop.
	Verify propulsion is disabled for emergency stops.	S	V-3.4.2.4 3.4.1.3.2	Propulsion disabled whenever emergency rate braking commanded.

TABLE 5.1.2-1: VCU TEST PROGRAM 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.

TABLE 5.1.2-1: VCU TEST PROGRAM OVERVIEW (Cont.)

FUNCTION	OBJECTIVES	Test Type	SPEC PARA (System / VCU)	SUCCESS CRITERIA
7.0 GENERAL SAFETY				
7.1 VCU Self Checks	Verify that the dual dissimilar software checks (A/B) provide safety and are operable.	S	S-2.4.1	A/B parameter checks are sensitive to processor failure yet provide operability margin.
	Verify main processor timing margins.	S	derived requirement	Timing margins allow time for background checks.
	Verify that the speed limit check is exercised.	M	S-2.4.1 S-3.1.3	VCU verifies capability to detect speed limit violation.
	Verify that the STP check is exercised.	M	S-2.4.1 S-3.1.3	VCU verifies capability to detect STP absence.
	Verify that memory and CPU operation are checked.	M	V-3.5.2.1 V-3.5.2.4.1	VCU checks RAM, ROM, and CPU. Processors operate if no failures present; lock up if any check fails.
7.2 Master Clock Tolerance	Verify safety of master clock failure.	A	V-3.2.3.4	Master clock frequency error > .02% initiates open loop emergency stop.
7.3 VCU A/A Disparity	Verify safe response to a single channel failure.	M	S-2.4.1	Independent channel failures are detected and interrupt the emergency brake hold-off.

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.

Three major conclusions can be drawn from the test effort:

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 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.

## 5.2 Test and Maintenance Features

To facilitate the testing of the system both during initial development and subsequent enhancement, certain monitoring features were built into the system:

1. Monitoring of the control law execution in real time is provided via the test point output ports.

2. Monitoring of the duty cycle utilization in real time is provided via the memory mapped frame-end points.
3. Inspection of the data base after the control system is halted is made possible by the monitor program.

#### 5.2.1 Test Point Outputs

A function is provided which controls the output of data to the Test Point Outputs interface unit. It has the capability to monitor up to eight internal Main Processor variables per channel and control the output of this data to memory mapped parallel ports.

Eight analog output ports are provided for each VCU channel. Data presented at the outputs are scaled and converted to an analog signal of 12 bits resolution and are suitable for input to a multiple channel oscillographic strip chart recorder. Internal data chosen for the test point outputs are variables normally available to the Main Processor during operation under automatic control. Selection of specific groups of output variables is made by way of switches mounted on the VCU rack front panel.

An eight bit, first-in-first-out (FIFO) buffering device is provided for each VCU channel. The same data presented to the eight analog ports is passed to the FIFO in raw, sixteen bit form. This feature was specifically designed to interface with the test set so that specific algorithm variables can be collected by the test set during a test run.

#### 5.2.2 Duty Cycle Monitoring

To allow monitoring of the time spent executing control laws versus time spent executing self tests in background, each of the four minor frames ends with a software controlled pulse being sent to a test point on the Main Processor board. By monitoring the 10 millisecond interrupt pulse (also available on a test point), which starts a minor frame, and the end of the frame signal with an oscilloscope, the actual percentage of frame utilization is measurable.

### 5.2.3 Monitor Program

In addition to the main program, both the Main Processor and the Communications Processor systems contains a small, separately stored monitor program. This program allows memory and register examination and manipulation for the purpose of testing and debugging.

Two full-duplex serial data lines allow each processor to communicate with a video display terminal and a telephone modem.

The memory elements of interest for examination via the monitor program during Verification Testing include:

1. The fault queue (stored in non-volatile RAM).
2. The failed selftest register (stored in non-volatile RAM).
3. All global control variables (stored in Data Exchange Unit).

#### 5.2.3.1 The Fault Queue

In the event of a failure of the system, which results in a software controlled detection and response, all failures are recorded in the order in which they happen. Even after a complete shutdown of the system this information is not lost.

#### 5.2.3.2 The Failed Self Test Register

In the event of a failure of a self test, all software processing is terminated. To read the index, which indicated which test failed, requires inspection of the failed selftest register in non-volatile RAM.

### 5.2.3.3 The Global Data Base

All variables shared by more than one control subroutine or used from one frame to the next are stored in a fixed, mapped data base. (Values passed to communication and fault queue management routines are not global.) If the vehicle control process is interrupted by a transfer to the monitor program, the complete state of the control system (except CPU register contents) at the time of the transfer is available for examination.

## 5.3 Design Verification Test Results

The results of the Design Verification tests are presented in the form of summaries for each test or test series. The summaries describe the objectives of the test, the approach taken, and the results obtained; they were written by the engineer responsible for each test.

### 5.3.1 VCU Initialization

VCU Initialization is summarized in one test titled, "VCU Initialization Characteristics."

#### 5.3.1.1 VCU Initialization Characteristics (Normal and Failed Initialization Response)

##### OBJECTIVES:

The major objective of this test is to verify that the VCU issues safe commands during initialization. Should initialization be complete, this test is to verify that the commands and internal status are correct for vehicle dispatch and control. In the event of a failed initialization, this test is to verify that the VCU put the vehicle in a safe state.

#### APPROACH:

VCU main processor initialization self tests consist of:

- a) CPU chip self tests: flags and registers
- b) memory chip self tests: RAM and ROM
- c) emergency code exercising tests
- d) processor board hardware self tests: STP latch, single prime channel, cross channel synch
- e) subsystem response tests: steering bias unique, hydraulic pressure, doors, PTCDCU, vehicle motion, brake caliper pressure, emergency brake hold-off or "punch-in"

Of these five sets of tests, only set e) can be verified with the VCU in its baseline configuration. Sets a), b), and c) must be accepted as verified from results of tests of software modules run on an instruction level simulator. Set d) must be accepted as verified during VCU integration tests using non-standard software configuration. Sets a), b), c) & d) have been so accepted. Set e) is part of this initialization verification test.

In the first run of the test all of the vehicle status conditions required for successful VCU initialization are set. Upon completion of initialization the data base is checked for proper data base conditions and the vehicle is instructed to dispatch.

In the second run of the test one by one of the vehicle status conditions required for successful VCU initialization are set to fail. When initialization is confirmed as failed, the data base is checked for proper data base conditions.

#### BASIC RESULTS:

The first test run demonstrated that the VCU initialization process sets the external conditions which are required for a successful VCU initialization, i.e., sets the data base as required, sets brake and propulsion



system to idle levels, and initiates the emergency brake hold off process. It also demonstrated that the VCU initialization process sets the external conditions which are required for an anomaly free dispatch of the vehicle.

The second run demonstrated that the VCU initialization process halts if there is a failure to get confirmation of any of the following required vehicle status conditions: a unique steering bias, operational hydraulic pressure in both channels, all doors closed, PTCDCU not in error state, vehicle not in motion, brake pressures set to emergency brake levels at start of emergency brake test sequence, and emergency brake levels changed to forced brake levels in 1/2 second from start of emergency brake hold-off (punch-in). In each case the data base was found to be in its proper state.

#### UNEXPECTED RESULTS:

There were no unexpected results.

### 5.3.2 Longitudinal Control - Routine

The Longitudinal Control testing is partitioned into three categories: routine, special purpose, and emergency stop. The routine section tests are summarized as: "Speed and Position Measurement," "Speed and Position Control," and "VLCS Stability Margin."

#### 5.3.2.1 Speed and Position Measurements

##### OBJECTIVES:

The objective of this test is to verify that the speed and position measurements for the AGRT concept are made in a manner that gives both accurate and safe results. To meet this objective the speed and position measurements must fall within the accuracy and safety requirements of the VCU and System Specifications.

#### APPROACH:

This test series consists of five test runs. Two of the test runs verify the accuracy requirements and the voting logic for the speed and position measurements. One of the test runs verifies the ability to perform a calibration and other calibration related functions. The last two runs test the fault detection logic.

The accuracy is verified by comparing the final measurements to the correct values and checking the ability to perform a calibration. The verification of the safety requirements is done by checking that the measurement voting logic and fault detection logic are implemented per the design.

#### BASIC RESULTS:

The primary result of the test is that the speed and position measurements are made accurately and safely in all except two cases. With these exceptions, the measurements meet all accuracy requirements. Further, it was shown that the system is able to accurately calibrate itself, which assures accurate measurements over the life of the vehicle. In all cases, the voting logic chooses the channel of odometer data providing the safest operation.

A secondary result is that the two speed and position measurement fault checking algorithm tests (excessive levels of missing and extra pulses and the position measurement tolerance checks) were verified as being implemented per the design. In particular, it was found that the missing and extra pulse detection algorithm will accept 2.26 times the maximum allowed level of odometer pulse jitter before declaring a false alarm.

#### UNEXPECTED RESULTS:

Two unexpected results were found in this test series. They both provide the possibility that the measurements will not meet their respec-

tive requirements. The first item occurs at low speeds. Due to the discrete time digital implementation of the odometers, there is a possibility the VCU will measure a speed of zero while the vehicle is still moving at up to 0.84 fps. Although this is technically not within the specification, the effect of the error on the control and safety of the vehicle is negligible. The second area where an unexpected result occurred was in the position measurement. Due to a shortcoming of the position measurement voting, there is a possibility that the position measurement will get ahead of the true position by an amount greater than the allowed accuracy. The probability of exceeding stated measurement accuracy limits is small; however, the impact on the vehicle longitudinal control system operation was found to be significant.

Specifically, the anomaly causes the vehicle to run slow and causes the station stopping distances to be shorter than allowed by requirements. A correction of this anomaly has been deferred to conserve resources. It will be worked in-line as part of future application efforts.

#### 5.3.2.2 Speed and Position Control

##### OBJECTIVES:

The major objective of this test is to verify that the Vehicle Longitudinal Control System (VLCS) regulates position, speed, acceleration, and jerk in accordance with requirements during normal operation when system parameters are at nominal values. Conditions to be studied include dispatch, normal speed transitions, constant speed operation, and the dynamics during the final portion of a normal rate stop, i.e., the transition to the forced brake mode or parked mode of operation. Special modes of the VLCS, such as Station Stopping, are the subject of other tests.

A second objective of this test is to verify the accuracy of the off-line EASY5 VLCS simulation used to support design of the VLCS. Test data will not conclusively confirm compliance with requirements since the test is to be run under nominal conditions. However, if test re-

sults are a close match of EASY5 predictions, then EASY5 predictions for worst case or 0.997 probability conditions are validated.

#### APPROACH:

This test consists of two test runs. The first involves a dispatch to 58.7 fps followed by a normal rate stop. The second involves transitions between each of the standard AGRT line speeds. Time history data is recorded in each run on those VLCS variables required to evaluate its basic performance.

#### BASIC RESULTS:

To expedite comparisons with single string test data and with EASY5 predictions, the emphasis in this test was on a configuration which used a single odometer pulse train without jitter to drive all of the VCU inputs. Data was also taken for a four odometer configuration, met requirements, and was free of any observed anomalies. In addition, results were a close match of EASY 5 predictions which validates the model used for the conditions under test.

This same test was performed in an earlier single string developmental test effort. The expansion to a dual string VCU configuration did not significantly alter VLCS performance.

#### UNEXPECTED RESULTS:

The purpose of taking data with a four odometer configuration was to evaluate initial dispatch and final stopping transitions. This data later proved useful in confirming the presence of a problem with the odometer voting logic discovered in the test of Station Stopping.

The odometer voting logic problem involves a conflict in requirements. Two measures of speed and position are computed and independently voted in the present design. A single common measure of each is then sent to all functions using these measurements. The VLCS requires that the

speed and position measurements be from the same pair of odometers. This is not always the case with the present logic. The impact is to cause stopping distances to be significantly shorter than predicted and to cause the vehicle to run slow and off point. The magnitude of the impact was a surprise. Other users of the measurements have different requirements which suggest that different measures of speed and position will have to be used depending on the application.

Correction of the odometer voting logic problem has been deferred. A comprehensive study of all uses of the data is necessary before a change can be made; future applications will likely have different requirements than the application assumed in the present design.

#### 5.3.2.3 VLCS Stability Margin

##### OBJECTIVES:

The primary objective is to verify that the stability margin of the Vehicle Longitudinal Control System (VLCS) is adequate to prevent control system instability when subject to normal system operating tolerances. The design goal for minimum gain margin is 6 decibels. A secondary objective is to verify the accuracy of the linear model of the VLCS used to predict stability characteristics.

##### APPROACH:

The VLCS is subjected both to tests using a simplified loop closure model in place of the real Vehicle Control Unit (VCU) and to tests using the real VCU. The nominal gain margin is measured by varying a dummy gain in front of the propulsion loop until the point of system instability is found. To obtain a rough idea of the shape of the frequency response curve, the magnitude of the open-loop transfer function is found at frequencies other than the marginal stability frequency of the system. A technique that employs a notch filter is used to extract the open-loop gain data from the closed-loop test system.

Also calculated is the amount of pure delays the system can tolerate, in addition to already-existing delays, before going unstable.

Only operation with the propulsion system in the loop is considered. Drive line dynamics, the main potential cause of instability, is not a significant factor in the braking mode.

#### BASIC RESULTS:

- (1) The VLCS system design has a sufficient stability margin of 13.8 dB, well above the design goal of 6 dB.
- (2) A maximum of 120 milliseconds of additional interface delays can be tolerated before the gain margin falls below the design goal of 6 dB.
- (3) The linear model of the VLCS provides accurate response predictions of the real control system, provided that the predictions are modified to reflect the addition of 42 milliseconds of pure delays.

#### UNEXPECTED RESULTS:

There were no unexpected results.

### 5.3.3 Longitudinal Control - Special Purpose

The Special Purpose section of Longitudinal Control testing is summarized as: "Position Update Response," and "Station Stop and Berth Moveup."

#### 5.3.3.1 Position Update Response

#### OBJECTIVES:

The objective is to verify that the Vehicle Longitudinal Control System (VLCS) carries out position updates from information sent to it by the

wayside in accordance with requirements. The position update algorithm has been extensively revised to increase operability as a result of the findings of single string developmental tests. For this reason, operability is extensively examined during this formal Design Verification testing.

#### APPROACH:

The test consists of four runs, each containing several position updates. The first run tests basic position update response under nominal conditions. Position corrections in constant speed zones and position corrections in speed transition zones are both examined. The second run tests a range of cases designed to verify that the time period for which the vehicle will receive position correction messages is of the duration and timing expected. The third run tests responses to anomalies including missing information, incorrect information, and new position corrections or linespeed changes being commanded before old position corrections are complete. The fourth run tests cases in which the commanded duration of the position correction procedure is equal to or less than zero. Data in the form of time histories of key variables is collected during each run.

#### BASIC RESULTS:

The vehicle's response to position update commands met every requirement. The VLCS correctly implements position corrections in the absence of anomalies. It also maintains operability under anomalous situations to the extent that the headway between adjacent vehicles is sufficient to accommodate an anomaly.

#### UNEXPECTED RESULTS:

There were no unexpected results.

### 5.3.3.2 Station Stop and Berth Moveup

#### OBJECTIVES:

The objective is to verify that the system can execute a station stop and a berth moveup within dynamic limits for ride comfort and stopping-distance accuracy.

#### APPROACH:

The simulated test vehicle is run through a scenario containing a dispatch to 8 fps followed by a standard station stop and a berth moveup under nominal conditions. Collected data provides measures of such dynamic parameters as peak acceleration, speed error, and stopping distance.

Key logic variables are also recorded to help verify that findings from an earlier, more comprehensive, developmental test are still valid concerning the logical operation of the station stop and berth moveup algorithm. The algorithm code has not been changed since this previous effort.

#### BASIC RESULTS:

Provided that a one-odometer configuration was used, the vehicle satisfied all predictions and success criteria. Of particular interest is the stopping distance. The requirement was for  $16 \pm 0.5$  feet; in the station stop the vehicle stopped in 15.8 feet and in the berth moveup it stopped in 15.9 feet. This is satisfactory performance under nominal conditions.

Logic operation was per its specifications giving assurance that the basic algorithm has not lost its integrity since its earlier checkout.



## UNEXPECTED RESULTS:

When the system was operated in the baseline four-odometer configuration, stopping distances were short by 0.45 feet in the station stop and by 0.85 feet in the berth moveup. Since the maximum allowable error is 0.5 feet under worst-case conditions, these are unacceptable results for nominal conditions. The source of the problem has been shown to be within the logic that selects which odometer pair to use for position measurement and for velocity determination and not within the station stop logic. The problem is discussed in the summary sheet for the test titled "Speed and Position Control."

### 5.3.4 Longitudinal Control - Emergency Stop

The Emergency Stop section of Longitudinal Control testing is summarized as: "Closed Loop Emergency Stop," and "Open Loop Emergency Stop."

#### 5.3.4.1 Closed Loop Emergency Stop

## OBJECTIVES:

The objective of this test is to verify that the transition to a closed loop emergency stop mode is done without error and that the closed loop emergency stop is performed within the requirements of the dynamic operation. The requirements upon the transition to the closed loop emergency stop mode are that it begin within 50 ms of the loss of the safe-to-proceed signal and that the jerk and acceleration limited command profiler be set to a prescribed state. These requirements upon the dynamic operation assure the safety of both the vehicle and the passengers by limiting the jerk, acceleration, and stopping distance of the emergency stop.

#### APPROACH:

This test series consists of five test runs. Three of the test runs start the closed loop emergency stop from constant speeds of 58.7, 22, and 8 fps respectively. The other two test runs start the closed loop emergency stop from approximately 22 fps at acceleration levels of approximately +4 ft/sec/sec and -4 ft/sec/sec.

#### BASIC RESULTS:

The primary result was that the transition to the performance of the closed loop emergency stop met the applicable requirements. It was found that the transition to the emergency stop mode began within 10 milliseconds and never exceeded 20 milliseconds after the safe-to-proceed signal was commanded to be removed. This reaction is less than the maximum allowable delay of 50 ms. At the start of the closed loop emergency stop, the state of the jerk and acceleration limited command profiler was set as required, and the operation was as required.

During the closed loop emergency stop, all dynamic performance variables were well within their required limits. Further, the variables met the expected results as projected by the EASY5 model with a relatively close match. Discrepancies that did occur were a consequence of limitations in setting the initial conditions when making EASY5 predictions and not an indication of any VCU problems. The single most important dynamic variable, the stopping distance, matched the expected value closely with the EASY5 model giving conservative results.

#### UNEXPECTED RESULTS:

The only unexpected result was a problem with the transition to the forced brake mode at the completion of the closed loop emergency stop. The fading of the torque command to forced brake levels was found to inadequately account for the conditions that occur at the end of a closed loop emergency stop; particularly, a nonzero acceleration command. A correction to the logic was made and the resulting configuration was used for all formal testing.

#### 5.3.4.2 Open Loop Emergency Stop

##### OBJECTIVES:

The objective of this test is to verify the primary protection against anomalies in the performance of a closed-loop emergency stop. This protection is provided by placing thresholds on the variation of the speed error and change in position error during the closed-loop emergency stop. Within 50 milliseconds of violation of either threshold, the initiation of open-loop stopping must be commanded.

##### APPROACH:

This test series consists of nine test runs. Three of the test runs violate the change in position error threshold. The other six test runs violate the speed error threshold. The tests are designed to violate the threshold in various sections of the threshold curve.

##### BASIC RESULTS:

The primary result was that the protection was implemented as required. The only variation from the expected results was a difference in the implementation and requirement of the change in position error threshold that was caused by numerical considerations; the difference was minor.

##### UNEXPECTED RESULTS:

A problem in the dissimilar software algorithm on the protection against anomalies in the performance of a closed-loop emergency stop was discovered at the start of testing. This led to a revision of the algorithm to increase the operability of closed-loop emergency stopping. The final configuration used in this test included the revised algorithm.

### 5.3.5 Interfaces

The Interfaces section of testing are summarized as: "VCU-VCAS Interface," and "FSK Message Processing."

#### 5.3.5.1 VCU-VCAS Interface

##### OBJECTIVES:

Vehicle collision avoidance is provided by the Odometer Data Downlink Collision Avoidance System (ODDCAS). The ODDCAS consists of an onboard unit, the Vehicle Collision Avoidance System (VCAS) Processor, and way-side units, WCAS. The VCU provides data to the ODDCAS through a first-in first-out (FIFO) buffer to the VCAS. The data transfer is controlled by a two wire handshake protocol. The major objective of this test is to verify that the interface between the VCU and the VCAS operates in accordance with requirements during both nominal and anomalous conditions.

##### APPROACH:

The test has one run consisting of a dispatch, a VCAS FIFO handshake anomaly in Channel 1, another dispatch, and a VCAS FIFO handshake anomaly in Channel 2. The expected reaction to the anomalies is a resettable closed-loop emergency stop, i.e., when the stop is completed, dispatch should be enabled. The Channel 2 anomaly should persist long enough for the circular FIFO buffer to wrap around.

##### BASIC RESULTS:

The interface behaved as expected. Data was passed through the buffer at the specified rate and in the proper format. Vehicle response to anomalies was correct; the vehicle was dispatched following a closed-loop emergency stop without reinitializing.

##### UNEXPECTED RESULTS:

There were no unexpected results.

#### 5.3.5.2 FSK Message Processing

##### OBJECTIVES:

The VCU communicates with the wayside via inductively coupled data links. Data is encoded using Frequency Shift Keying (FSK) for both uplink (wayside to vehicle) messages and downlink (vehicle to wayside) messages. The major objective of this test is to verify that the VCU does process (i.e., recognize and respond to valid uplink messages) and does generate correct downlink messages.

##### APPROACH:

The test consists of one run to check that the VCU processes every uplink message function code and subcode and that the VCU generates every downlink message function code. The uplink processing will be recognized by a status change in speed/position or discrete output, or a downlink message. Additionally, an illegal function code and a message targeted to a different vehicle are uplinked to test discrimination of invalid messages.

##### BASIC RESULTS:

All success criteria were met and no defined-message processing anomalies were observed. The VCU does correctly process every implemented uplink message function code and subcode, and does correctly generate every implemented downlink message function code. A problem was found with illegal message processing. The VCU will not report as illegal some illegal uplink function codes targeted to the vehicle.

##### UNEXPECTED RESULTS:

The VCU will not report certain illegal uplink function codes, 'a' to 'f', targeted to the vehicle. Analysis of this problem raised several other related communications concerns. These problems have been documented; however, the analysis and corrective action have been deferred.

### 5.3.6 Anomaly Response

The test results for Anomaly Response are summarized as: "FSK Uplink Anomaly," "Overspeed Protection," "Safe-To-Proceed," "Fault Induced Stop," "Power Monitoring," and "Status Monitoring."

#### 5.3.6.1 FSK Uplink Anomaly

##### OBJECTIVES:

The VCU communicates with the wayside via inductively coupled data links. Data is encoded using Frequency Shift Keying (FSK) for both uplink (wayside to vehicle) messages and downlink (vehicle to wayside) messages. The validity of FSK uplink messages is determined by the VCU using a cyclic redundancy check (CRC). The major objective of this test is to verify that the VCU does detect and react correctly in response to uplink messages with invalid CRC data.

##### APPROACH:

This test has one run consisting of a dispatch followed by valid idle messages interspersed with a single invalid message, ten invalid messages (one below the anomaly threshold), 11 invalid messages, and 1151 invalid messages (the remainder of the test run). The expected result for 1 and 10 consecutive invalid messages is that none of the messages is accepted by the VCU. The expected result for 11 or more consecutive invalid messages is that none of the messages is accepted by the VCU, the anomaly is reported, an irrevocable normal rate stop is commanded, and the speed limit is profiled to 10.5 fps as long as the anomaly persists.

##### BASIC RESULTS:

The test results were exactly as expected; no incorrect behavior in the CRC anomaly processing was observed.

## UNEXPECTED RESULTS:

There were no unexpected results.

### 5.3.6.2 Overspeed Protection

#### OBJECTIVES:

The primary objective of this test is to verify that a closed loop emergency stop is initiated in response to any speed limit violation and that subsequent dispatch requests are rejected. In addition, the test must verify that the current speed limit is retained whenever a new speed limit is commanded but the command is in error.

The secondary objective is to verify that the vehicle cannot be auto restarted following a speed limit violation.

#### APPROACH:

This test consists of three test runs. The first run initiates a speed limit violation by commanding a line speed that exceeds the speed limit. The second run reduces the speed limit while retaining a constant line speed. The third run generates a communication failure (VRC error) in a series of messages that attempt to increase the speed limit just before a vehicle exceeds the original speed limit.

In the first run, a dispatch is attempted after the closed loop stop to verify that an auto dispatch is inhibited.

Time history data is recorded in each run as required to evaluate its basic performance.

#### BASIC RESULTS:

Speed limit commands are uplinked to a vehicle every 40 milliseconds. A closed loop emergency stop is to be initiated any time the speed limit

is violated, i.e., any time the measured speed plus 0.5 feet/second exceeds the speed limit. When the speed limit command is decreased, the VCU profiles the speed limit downward at a rate which allows time for the vehicle speed to be reduced at a normal rate. When the speed limit is increased, the new speed limit becomes effective immediately; however, the old speed limit is retained if the new speed limit is invalid. This is detected by an invalid VRC code. Performance of the VCU met all these requirements and was free of any observed anomalies.

#### UNEXPECTED RESULTS:

There were no unexpected results. All reactions in all three runs were just as expected.

#### 5.3.6.3 Safe-To-Proceed

##### OBJECTIVES:

The major objective of this test is to verify that the transition from normal operation to the closed loop emergency stopping mode occurs when the Safe-To-Proceed (STP) signal is removed, that the auto restart capability after the stop is complete, and that the timing requirements are met.

The second objective of this test is to verify that normal operation continues when STP is present on the forward antenna only and then on the rear antenna only.

##### APPROACH:

This test consists of two test runs. The first involves a dispatch to 8 feet/second followed by the removal of STP from Channel 1. After adequate time for the vehicle to complete a stop, a dispatch to 8 feet/second is commanded followed by removal of STP from Channel 2.

The second run consists of removing STP from the rear antenna only and then from the forward antenna only.



Time history data is recorded in each run as required to evaluate its basic performance.

#### BASIC RESULTS:

The STP signal is a critical element of the AGRT safety concept. For the vehicle to proceed along the guideway, the STP signal must be present on at least both forward or both rear receivers. If for any reason this minimum condition is violated, the vehicle is required to execute a closed loop emergency stop and issue a downlink message reporting that an emergency stop is being executed. Performance of the VCU met requirements and was free of any observed anomalies.

#### UNEXPECTED RESULTS:

There were no unexpected results. All reactions in both runs were just as expected.

#### 5.3.6.4 Fault Induced Stop

##### OBJECTIVES:

Failure of a variety of safety assurance tests require stopping of the vehicle and in emergency situations shut down the propulsion system. Four categories of stops are available:

- 1) Revocable normal rate stop
- 2) Irrevocable normal rate stop
- 3) Closed-loop emergency stop
- 4) Open-loop emergency stop

The major objective of this test is to verify that all categories of fault induced stops can be initiated and that propulsion is disabled for both types of emergency stops.

#### APPROACH:

All categories of stops, except a revocable normal rate stop, are done in other tests of the VCU Design Verification Test series. This test collects data from the other tests and includes one test run to verify that a revocable normal rate stop can be initiated. The run consists of a dispatch to 22 fps with a 0.5 second loss of propulsion during up-speed. At constant speed there is a one second propulsion loss. The run ends with a propulsion loss that persists long enough for the vehicle to come to a complete stop.

#### BASIC RESULTS:

The objectives of this test have been met. All categories of fault induced stops were initiated and propulsion was disabled for both types of emergency stops.

Data has been collected on revocable normal rate stopping. Behavior was as expected; vehicle movement continued when propulsion was restored. Jerk, acceleration, and speed are within limits and are well-behaved.

#### UNEXPECTED RESULTS:

There were no unexpected results.

#### 5.3.6.5 Power Monitoring

##### OBJECTIVES:

The first objective of this test is to verify that the VCU will detect out-of-tolerance battery bus voltages and report the anomaly conditions to the wayside. The second test objective is to verify that the VCU fails in a safe manner when the voltage level of the 5 VDC power feed to the Vehicle Control Electronics (VCE) is reduced below the level necessary for continued operation.

#### APPROACH:

For the first part of this test the simulated battery bus voltage level is set to anomalous levels during the test run. Inspection of Test Set data records indicated time and type of VCU reaction.

The second part of the test has two distinct phases. In the first, the voltage is reduced slowly until VCU failure in order to locate the minimum operational voltage threshold. In the second phase, a run from a previous design verification test (intended to demonstrate transition from closed-loop to open-loop stopping) is repeated at several different voltage levels just above the critical threshold.

#### BASIC RESULTS:

The VCU performed as expected when presented with anomalous battery bus voltage levels.

Testing with declining voltage indicated safe failure of the VCU. In all runs as the voltage was reduced, one channel of the VCU would eventually cease processing, followed immediately by the remaining channel declaring an open-loop stop. The tests performed with the voltage held at a steady level just above the critical threshold gave identical results to the earlier design verification test. In addition, examination of the data recorded from the Odometer Data Downlink Collision Avoidance System (ODDCAS) interface showed transmission of correct safety-critical data up to the point of failure.

#### UNEXPECTED RESULTS:

The Test Point Data Communication System, FSK downlink system, and ODDCAS data communication system remained functioning up to the point of CPU failure permitting the collection of data valuable in confirming the safe response of the VCU. It is realized that, in any particular VCU, variation in hardware parameter values may result in any or all of these functions failing prior to loss of a CPU. Although perhaps ultimately

safe, a system without low voltage detection and shutdown may present operability and testability problems, as well as displaying unit to unit variation in modes of degradation.

#### 5.3.6.6 Status Monitoring

##### OBJECTIVES:

The purpose of this test is to verify correct VCU reaction to anomalous conditions in vehicle status as detected via an analog type and a discrete type of interface. The vehicle functions chosen are brake caliper pressure (analog) and hydraulic fluid temperature and accumulator pressure (discrete).

##### APPROACH:

Reaction to brake caliper pressure anomalies is tested by increasing or decreasing the simulated measured caliper pressure fed back to the VCU by the Test Set. As two different disparity criteria are used in the VCU, depending on which occurs first, anomalies are introduced both prior to vehicle dispatch (high commanded brake torque) and while the vehicle is stopping (moderately low commanded brake torque).

Simulated discrete status signals for hydraulic fluid temperature and accumulator pressure are commanded to switch state under scenario control, and time and type of VCU reaction are recorded.

##### BASIC RESULTS:

Proper reaction to measured brake pressure anomalies was verified. In particular, the proper disparity criteria were employed at the different commanded pressure levels, and the VCU waited for any disparity to persist for one second, as designed, before declaring an anomaly.

In all cases, the correct reaction was observed to anomalous conditions introduced into the hydraulic fluid temperature and accumulator pressure.

## UNEXPECTED RESULTS:

No unexpected behavior was observed. It was noted that, although not directly under test, the VCU analog input interface displayed excellent accuracy.

### 5.3.7 General Safety

The tests under General Safety are summarized as: "VCU Self Checks," "Master Clock Tolerance," and "VCU A/A Disparity."

#### 5.3.7.1 VCU Self Checks

##### OBJECTIVES:

The objectives of this test are to verify:

- that the dual dissimilar software checks (A/B) allow tight enough margins to provide safety and loose enough margins not to degrade operability;

- that main processor timing margins allow enough time for the execution of background tests;

- that speed limit check is exercised to demonstrate it will respond if presented with data indicating an anomalous condition;

- that STP check is exercised to demonstrate it will respond if presented with data indicating an anomalous condition; and

- that memory and CPU operations are checked.

##### APPROACH:

The subject of this test is dissimilar or "B" algorithms and background checks. Both of these checks are intended to trap failures in the code

or the code processors. As such, they cannot be expected to show both pass and fail states under standard VCU configuration. For this reason all verification associated with this test has been drawn from analysis of previous subsystem tests. In two cases, however, test runs were required to verify the "A" algorithm - "B" algorithm operability margins.

#### BASIC RESULTS:

Analysis of code for the "B" algorithms and some nominal test runs confirm that the A/B checks are sensitive to processor failure yet provide operability margin.

Duty cycle measurements confirm timing margins allow time for background checks.

Examination of the module tests on the emergency code exercisers confirm:

- VCU capability to detect speed limit violation;

- VCU capability to detect STP absence; and

- VCU checks RAM, ROM and CPU register and control flags. Processors operate if no failures are present and lock up if any checks fail.

#### UNEXPECTED RESULTS:

There were no unexpected results.

#### 5.3.7.2 Master Clock Tolerance

##### OBJECTIVES:

The Master Clock is vital for all measurements. All timing and integration rates used by the control laws are determined by the Master Clock. Assuring the tolerances allowed for operation and the response of the system when those tolerances are violated is safety critical. The objective of this test is to verify safe reaction of the VCU in the event of Master Clock failure.

##### APPROACH:

Verification associated with this test was by analysis of the circuit design, and performance of the circuits during all Design Verification testing.

##### BASIC RESULTS:

The design solution to the problem of how to maintain synchronization between the redundant microprocessors of the VCU includes mechanisms for the detection of frequency out-of-tolerance conditions. When those conditions occur, a safe response is initiated.

##### UNEXPECTED RESULTS:

There were no unexpected results.

### 5.3.7.3

### A/A Disparity Checks

#### OBJECTIVES:

Fundamental to the hardware architecture are redundant main processors to assure validity and safety of control law processing. That assurance is established by comparison of processing output from one channel with the output from the other channel. If there is a disparity, some form of insanity in one of the two processing systems is assumed and open-loop emergency stopping must be initiated. The objective of this test is to verify safe response of the VCU in the event of a single channel failure.

#### APPROACH:

This check is intended to trap failures in the code processors. As such they cannot be expected to show both pass and fail states under standard VCU configuration. For this reason, all verification associated with this test will be drawn from analysis of previous subsystem tests.

#### BASIC RESULTS:

The module named "aachk" is the primary algorithm designed to detect and react to cross channel control command disparities. The allowance for disparity between what is expected in this comparison of the cross channel commands and what is measured is zero. No error is allowed. Confirmation that these tests are effective in detecting and reacting to failure of the CPU is found in the module tests for "aachk." The operability of this test is indicated by the fact that in all verification testing there has been no false alarming of the control system by this test.

#### UNEXPECTED RESULTS:

There were no unexpected results.



## 6.0

## CONCLUSIONS AND RECOMMENDATIONS

The AGRT VCU described in this report is a microprocessor based system employing advanced technology and innovative design features not commonly found within the transportation industry in the United States. The system analysts and designers have blended together hardware, software, and safety concepts into a control system that has the capability of safely controlling the movement of unmanned vehicles along a guideway. A number of design features evolving from this program merit consideration for current and future transit industry applications.

This section of the report contains a discussion of the unique features of the design, conclusions based on design experience, and recommendations and applications to current and future transit system designs. In addition, a section is included that discusses the VCU testing program and the overall testing philosophy.

### 6.1

#### Longitudinal Control System

The AGRT Vehicle Longitudinal Control System (VLCS) is a point follower control system which uses state-of-the-art microprocessor techniques. The majority of the VLCS control algorithms are implemented in the VCU.

The Morgantown People Mover (MPM) control system was used as a starting point; however, the current implementation has little in common with its predecessor other than the fact that both are point followers. One benefit of our Morgantown experience was to avoid configuration features which proved to be troublesome on MPM. The design includes numerous features necessary to meet the stringent AGRT performance and safety requirements.

This section describes the unique features of the AGRT VLCS, the knowledge gained as a result of the design effort, and future application possibilities.

### 6.1.1 Design Features

The following paragraphs describe the features of the VLCS that either represent new technology or are critical to meeting AGRT requirements.

#### 6.1.1.1 Jerk and Acceleration Command Limiter

The conventional method of limiting jerk (a ride comfort consideration) is to place a jerk limiter within the speed control loop. This was done on MPM and was found to be ineffective. In addition, it has the disadvantage of making the control system operation nonlinear; this prevents taking advantage of linear analysis tools.

The approach taken on AGRT is to limit both the jerk and acceleration commands sent to the closed-loop control system. Ride comfort control is achieved by designing the closed-loop system to accurately follow the profiled commands.

A unique software algorithm is used to perform the function of profiling the VLCS commands. The algorithm uses feedback techniques to insure that specified jerk and acceleration limits are met for all possible types of input signals. The specific advantages of the algorithm are that it requires a minimal execution time and that it allows the use of multiple acceleration limits. This latter capability is used to advantage in the AGRT design; specifically, five different acceleration limits are used depending on the mode of operation.

#### 6.1.1.2 Position Update Algorithm

Periodic updates of vehicle position (the onboard point) are required to meet headway regulation requirements. The function is allocated so that the wayside determines the magnitude of the correction and the VCU implements the correction.

The nature of the correction depends on the mode of operation. In constant speed zones, corrections are achieved by increasing or decreasing

the commanded speed. Flexibility is enhanced by allowing selection of both the increment in the speed command and the time duration for which the increment is in effect. In speed transition regions, corrections are achieved by varying the start time of the transition. The advantage of this approach is that it maximizes ride comfort.

The VCU portion of the position update algorithm provides the capability to support virtually any fleet management scheme that might be used. This is because the algorithm allows small corrections to the onboard point as well as large corrections on the order of one or more operational headways. Corrections as small as 0.04 seconds can be implemented. In addition to its performance capabilities, the algorithm includes a significant amount of anomaly detection and reaction logic designed to enhance system operability.

#### 6.1.1.3 Speed and Position Measurement System

The speed and position measurement system is noteworthy for two reasons:

1. It provides the best measurement accuracy possible in a system based on measuring wheel motion, and
2. It provides an extremely high level of safety, i.e., protection against excessive undetected measurement errors or equipment failures.

Digital sensors (based on the Hall effect) are mounted at each wheel to provide the basic measurement of wheel motion. The resulting output pulse trains are then extensively processed in the VCU to obtain accurate and safe measurements of centerline speed and position.

System accuracy is limited primarily by factors external to the VCU. The main unknown is variations in offtracking of the steering system. All major bias errors have been compensated for and other compensation features have been defined but not fully implemented because of some uncertainty regarding accuracy requirements.

The output measurements are used by a variety of functions other than the VLCS, e.g., Collision Avoidance and Overspeed Protection. Because these additional data users are safety critical, the measurements must now be protected against errors, a factor which has a major impact on the design. The safety requirement is met by using dual redundant sensor pairs, odometer preprocessors and VCU main processors, and by an extensive number of fault checks. Most of the fault checks are performed by the VCU main processor. An important exception is the check against missing or extra odometer pulses which is performed in the odometer preprocessors.

Odometer preprocessors are employed in order to off-load the main processor. This is because the time between odometer pulses can be as short as 340 microseconds. Servicing interrupts at this rate would leave the main processor little time to perform its other functions. An advantage of this distributed processing approach is that it allows doing the missing/extra pulse fault check in the preprocessor without adding the substantial amount of hardware that would otherwise have been required.

#### 6.1.1.4 Torque Control

The output of the basic control law is a single point torque command. The command is sent to the motor if positive and to the brakes if negative.

The torque control approach is a major departure from the MPM design which used a combination of motor speed control and brake torque control. The reason for torque control is to minimize or eliminate the brake/motor interaction difficulties experienced with the MPM design. A secondary benefit is a design simplification that allows more effective use of linear analysis techniques.

#### 6.1.1.5 Emergency Stopping Concept

The normal AGRT emergency stopping concept is to stop under closed-loop control and to use an open-loop backup if, and only if, the safety of the closed-loop system cannot be assured.

High emergency stop deceleration levels are a necessary characteristic of a short headway system. Open-loop systems, the traditional approach, further have the characteristic of large variations in deceleration level. To guarantee a minimum deceleration level means there will be the possibility of a much higher level under some conditions. The result is the possibility of high deceleration levels that could cause passenger injury.

Closed-loop control is used to reduce the effect of brake system variations and thereby reduce the maximum deceleration a passenger will experience. A closed-loop speed control scheme is used which is identical to that used in normal operation. The only significant difference is in the commanded jerk and acceleration levels. Closed-loop emergency stopping is accomplished using the same components as used in normal operation; this keeps the parts count low. It also has the safety advantage of regularly exercising the equipment that is used in an emergency situation; this enhances the ability to detect equipment failures.

A traditional open-loop backup is used when a failure is detected which casts the safety of the closed-loop system in doubt. In this mode, the possibility of high deceleration levels again occurs. The difference is that the probability of having to use the open-loop backup is low thus reducing the risk to an acceptable level.

The unique feature of the design is the method of detecting closed-loop system failures. Analysis results have been used to define a curve of speed and position error limits that represent the boundary between normal and failure responses of the system. These limits are independent of initial speed which simplifies the implementation. Their characteristics have also been used to advantage in the calculation of worst

case stopping distances for scenarios where a failure causing a switch-over to open-loop occurs.

#### 6.1.1.6 Station Stop / Berth Moveup

To increase throughput, the MPM station speed of 4 fps was increased to 8 fps on AGRT. This change required a redesign of the MPM station stop controls. A position dependent speed command profile is used on MPM to meet stopping accuracy. The AGRT system uses both time and position dependent command profiles to meet requirements. The AGRT system also requires use of a unique single berth moveup mode. The reason is that one berth length is not long enough for a vehicle to accelerate to and then stop from 8 fps. A target speed of 4 fps is used in the berth moveup mode.

The collision avoidance system is active in station channels on AGRT whereas it was not on MPM. This means that compatibility with the collision avoidance is an issue on AGRT. To achieve this compatibility or to avoid unnecessary emergency stops requires relatively long berth lengths when compared to the MPM design.

#### 6.1.2 Conclusions Based on Design Experience

##### 6.1.2.1 General

The AGRT VLCS is capable of supporting the requirements of a three second headway system but the overall system cost impacts of developing and maintaining the system warrant further study. Experience suggests that significant cost and operability improvements could be obtained by a moderate relaxation in the headway requirement from 3 seconds to somewhere between 5 and 7.5 seconds..

Likewise, the emergency stopping deceleration levels need further study. Concerns are the possible need to physically restrain passengers and the cost of maintaining adequate tire/guideway traction levels. Safety requirements should be studied to determine if a further reduction in the frequency of open-loop stops can be achieved.

#### 6.1.2.2 Use of Microprocessors

The capabilities and performance of the AGRT VLCS design are due, in large part, to the fact that it is a microprocessor-based design. Unlike many other designs, the VCU is not simply an alternative implementation of an existing design. The VLCS algorithms were designed, from the start, with the capabilities of the microprocessor in mind.

Relatively complex algorithms, which optimize performance, are used in the AGRT design to meet requirements. Without a microprocessor, implementation would be a significant problem because of the large number of components that would be required.

The VCU software uses a simple cyclic executive program. Experience confirms that this choice is superior to a more complex multi-tasking executive in this real-time controls application.

#### 6.1.2.3 Value of Analysis and Simulation

Extensive analyses were conducted using a detailed simulation of the VLCS. The results were used as the basis for the derived requirements levied against the VCU. This approach worked well and very few problems were encountered with the basic design choices made in this manner.

Future efforts should consider the possibility of using the off-line simulation to check out the actual VCU code. This would allow off-line closed-loop testing of the VCU code prior to hosting it on the VCU hardware. It would also simplify the task of keeping the simulation up to date.

Accuracy requirements were treated as 0.997 probability limits where possible and root-sum-square techniques were used to verify compliance. This approach worked well, recognizing that actual performance is statistical in nature, and avoids unnecessarily stringent derived requirements. A worst case approach was required in some safety related areas. Results using the worst case approach were less than satisfactory. The

problem is that performance estimates are unnecessarily conservative and the results do not provide any indication of the probability associated with exceeding a particular limit. The best approach in safety critical areas appears to be a judicious combination of worst case and statistical techniques where scenario factors are worst cased and equipment error sources are treated statistically.

#### 6.1.2.4 Specification of Requirements

The result of the VLCS analysis effort was a detailed definition of the required VCU algorithms. These algorithms are specified in considerable detail in the VCU specification. The reason is to prevent duplication of effort and to insure that details important to VLCS performance were not neglected. This approach worked well and provided the needed controlled communication medium between the analysis and design groups.

#### 6.1.2.5 Mode Switching

An area that did not receive adequate attention is the logic for switching between the various VLCS modes of operation. Most of the VLCS problems encountered during test involved deficiencies in the VLCS transition logic. The conclusion is that more attention should be given to switching logic in any future VLCS analysis and simulation effort.

#### 6.1.3 Applications

The overall VLCS design could be used on virtually any automated wheeled-vehicle system with relatively minor adjustments. It is particularly applicable to short headway systems where a point follower type of control is appropriate. It could also be used to advantage in longer headway systems.

Specific portions of the design also have general application possibilities on a standalone basis.



The jerk and acceleration limiter is one portion that has potential applications both within and outside of the transportation industry. There are many controls applications that require placing limits on the first and second derivatives of a signal where this algorithm could be used to advantage.

The concepts used in the speed and position measurement system could be used to advantage in any system using a wheel odometer as the basic control system sensor. The techniques used to meet safety requirements, in particular, should be of interest.

Finally, the emergency stopping concept has general application possibilities in the transportation industry. The use of a closed-loop mode with an open-loop backup optimizes the trade between performance and safety and does so without significantly increasing system complexity.

## 6.2 Safety

The ultimate requirement for the Vehicle Control Unit is safety. All operations must be performed in a safe manner; all malfunctions affecting safety must be detected promptly and must result in a safe reaction. Given that the performance requirements mandated the use of microelectronics in general, we chose to use microprocessors as the most cost effective implementation. Microprocessors, in turn, imply associated software (or firmware, once committed to read-only-memory).

### 6.2.1 Safety Design Constraints

The AGRT program requirements limited our design options to three basic categories: fail-safe, safe life, and checked redundant.

Fail-safe components consist of devices that rely on physical properties such that failure modes can be absolutely analyzed. (Brass cannot become magnetic, pressure cannot become a vacuum, gravity is always present to release a relay armature, etc.) The American Association of

Railroads "VITAL RELAY" is such a device; remove the electrical excitation and gravity will always release the armature (opening the front contact). If the relay has been correctly applied, any failure of the device in the overall system will be safe (result in a safe condition).

Safe life components are typically structural members. Given that the original design properly considered the operating stress and number of stress cycles, the safe life of the component can be predicted. The application remains safe if the component is repaired or replaced on a predetermined schedule.

Microelectronic devices are neither fail-safe nor safe life. The design was, therefore, limited to a checked redundant configuration. Although the designers were initially concerned with the loss of design freedom, it was realized that a single-thread microelectronic implementation could not be rigorously analyzed for safety. Such a (single-thread) design would have represented a significant cost, schedule, and technical risk. Hence, a dual-redundant configuration was chosen for the Vehicle Control Unit.

Malfunction or loss of either redundant channel, however, reduces the Vehicle Control Unit to a single thread device and by design results in an open loop stop. The open loop reaction is required under the AGRT Program ground rules; these rules prohibit closed loop operation with single thread microelectronic designs.

A prime goal in both the hardware and software design was simplicity. Logic dictated the need for a design that was straightforward to analyze. To this end, the hardware architecture consists of two identical channels with a common clock. The software design consists of a cyclic executive calling applications routines that run within a time framework defined by a hardware clock. Safety critical calculations are performed with redundant, dissimilar routines.

### 6.2.2 Safety Evaluation Constraints

As noted earlier in Section 3.2, the safety evaluation techniques levied against the AGRT contract differed from normal aerospace practice. The contract approach was comparison of the final design to an approach using conventional approach using conventional vital elements. Each component or element that performed a safety critical function was required to have a Mean Time Between Unsafe Failure (MTBUF) equal to or better than an equivalent vital component (one million years).

This evaluation technique proved to be a much greater problem to the designers than did the design constraints noted previously (in Section 6.2.1).

The system designers were unable to allocate failure rates among the various subsystems. The individual hardware designers had no guidelines during the design process; they were unable to effectively use the available statistical data on microelectronic devices. They were instead forced into a circular process of creating a design and submitting it for evaluation, then modifying it if it was determined to be unacceptable. Given this circular design process, managers were hindered in accurately predicting engineering development costs and schedules.

Although it was concluded that the final design is technically sound in addition to meeting the Program criteria, it is believed that the work could have been achieved in a more efficient manner. These experiences with the Vehicle Control Unit design taught or reinforced several lessons; the recommendations below are based upon these lessons.

### 6.2.3 Safety Recommendations

These recommendations relate to design approach rather than to implementation; none of them would result in a change of the basic hardware or software architecture. In truth, they merely reflect good design and management practice.

1. Assign quantitative safety requirements and use the associated quantitative analysis techniques.

Qualitative safety requirements leave the designer concerned as to when he is finished. In contrast, quantitative probability requirements allow evaluation of the ongoing design, and allow flexibility in allocation of safety criticality.

Qualitative assessments, made after the design is complete, are not cost effective and may not result in the desired level of safety. The costs of redesign can be neither predicted nor tolerated. Qualitative requirements ("as safe as a vital relay") cannot be used during the design process.

Quantitative requirements and techniques, applied before the detailed design process, result in a subsystem MTBF (Mean Time Between Failure) allocation. Electronic part failure rates are characterized in terms of MTBF hours adjusted for the intended environment. The designer can choose parts and check times that meet the allocated requirement. (The allocation for each subsystem is based upon a fault tree analysis, a proven technique for identifying critical functions or elements.)

2. Allocate safety requirements early in the design cycle.

Although this seems an obvious corollary to the use of quantitative requirements and techniques, it is repeated here to emphasize the importance of trading the costs of safety analysis with the costs of design and fabrication. The final design must lend itself to analysis and must be producible at reasonable cost.

Of course, the design trades must also include safety, reliability, maintainability, and cost.

3. Use checked redundancy for safety critical microelectronic implementations.

It was concluded that single thread microprocessors cannot be used in safety critical applications. Although state-of-the-art microelectronics are very reliable, not enough is known about microprocessor failure modes to support a rigorous safety analysis. (Indeed, detailed device design data is typically proprietary.)

In a device that relies on thousands of reverse-biased junctions for isolation, it must be assumed that any pin or element could be shorted to any other pin or element. It seems unlikely that many intrinsically safe failure modes could be identified even if the microchip design and implementation details were available for analysis.

4. Exercise safety critical hardware and software functions.

Safety critical functions in a checked redundant system must be exercised frequently. Dynamic self checks meet this need and are essential unless normal processing automatically exercises all logic paths. Integral self checks, performed as a part of normal processing, are more powerful than checks that set aside the main stream processing. These integral self checks, however, are more difficult to implement and analyze.

For the case of a safety function or system implemented with microprocessor components, the actual emergency code must be exercised with data representing a failed condition.

5. Develop specific evaluation criteria for microelectronic hardware (and associated software) within the transit community.

It is recommended that the transit community develop specific evaluation criteria for microprocessor based designs. The use of quantitative safety requirements and techniques is a valid start toward meaningful evaluation criteria. It is impossible to "certify" a microelectronic design as safe for revenue service by proclaiming that it uses "fail-safe" (vital) components applied in a failsafe manner.

Systems engineering design approach and statistical safety techniques have been developed and thoroughly proven across several disciplines, including aerospace, nuclear, and transportation (Morgantown People Mover). These techniques include Failure Modes and Effects Analyses, Worst Case Analyses, Sneak Circuit Analyses, and Fault Tree Analyses. The outstanding safety record of the U.S. space program is proof of the effectiveness of these techniques.

### 6.3 Hardware

As stated at the beginning of this section, the VCU hardware described in this report is a microprocessor based system employing advanced technology. As an example, each channel of the VCU contains nine microprocessor/microcomputer integrated circuit devices, plus one additional microprocessor in the Propulsion Torque Command Data Conversion Unit (PTCDCU); this is a total of nineteen such devices for the dual channel configuration. It was concluded that these devices are necessary for the VCU to perform within the timing and performance constraints of the AGRT requirements and to fit in an acceptable package size.

Section 6.3 discusses what is believed are the innovative hardware design features of the VCU, the conclusions or what could be done differently based on design experience, and what might be done in future designs based on recent advances in technology. Also included is a discussion of possible applications for similar high technology hardware within the transportation industry.

#### 6.3.1 Design Features

Within the design of the VCU there are a number of unique and/or innovative circuits that should be highlighted as possible candidate solutions in future transportation system designs.

#### 6.3.1.1 Dual Channel Configuration

As previously discussed in this report, it was concluded that the checked redundancy approach is necessary to achieve safety in systems using high technology devices. Not enough is known about microprocessor failure modes to establish safety of single channel systems; it is unlikely that microprocessors can be used in safety critical systems without checked redundancy.

The checked redundancy approach is a feasible design solution in circuits as simple as a monitor of a safety critical sensor or in systems with complex control functions such as the VCU discussed in this report.

#### 6.3.1.2 Dual Channel Timing System

The timing system is designed so that all functions of the circuitry are continually being exercised; if a failure occurs it is detected and a safe reaction initiated. The timing system employed uses a single Master Oscillator output to provide timing signals to each channel with an additional oscillator in each channel monitoring the Master Oscillator. If any of the three oscillators fails or drifts outside the tolerance limits the condition is detected and the system initiates a safe reaction. By using a single Master Oscillator the two channels operate synchronously with respect to each other. The synchronous operation provides several software design advantages that would be very difficult to achieve in an asynchronous system. One very important advantage is that cross channel checks are required to match bit for bit; this saves a very difficult task of determining what tolerance or limit is needed at the instant the check is performed.

Another important advantage is that all timing and integration rates used by the control laws are determined by the accuracy of the Master Oscillator. If different timing sources were used the timing measurements and integration rates would differ and errors would immediately be introduced between the two channels. Even frequent resynchronization of the channels would not solve the problem; it would require more complex

software algorithms to compensate for any frequency difference between channels.

A timing system using the principles developed in the VCU design could be adapted to other multi-channel designs.

#### 6.3.1.3 Data Exchange Unit

The VCU Data Exchange Unit (DEU) is the communications artery by which each channel exchanges data with the other channel and then uses the data to make safety critical decisions. The design of this unit is based on failsafe operation. Both hardware and software techniques are employed to make the design failsafe. A Failure Mode and Effects Analysis was conducted on the DEU and the conclusion was that all failures hypothesized resulted in a safe reaction.

It is our conclusion that the DEU is a fast, efficient (minimum parts), and safe method for exchanging data between two synchronous microprocessor channels operating with extremely fast reaction time requirements.

#### 6.3.1.4 FSK Digital Receiver

A study was conducted to determine the type of noise most likely generated by an AGRT type propulsion system; the study concluded that impulse noise would be the dominant interference. Previous FSK receiver designs utilized analog bandpass filters to detect spectral energy within the FSK passbands. Such designs have an inherent problem in severe impulse noise environments because impulses are composed of an infinite number of spectral components.

It was thought that a different type receiver was needed for the AGRT program. This led to a receiver design utilizing a unique method of digital frequency demodulation. The front end of the receiver is still an analog design that amplifies and bandpass filters low level input signals. The demodulator section is an all digital design and consists of an up-down counter, programmable array logic, and an 8-bit microcom-



puter. (The theory and operation is contained in Section 4.1.1.1.1). Laboratory tests on the Digital Receiver show that the design is very effective in the presence of a high impulse noise environment and could easily be adapted to other systems with a similar noise environment.

#### 6.3.1.5 Odometer Preprocessors

The VCU's Main Processor computes the vehicle's centerline speed and position. This is accomplished by processing digital pulse train data that originates from odometers attached to each wheel of the vehicle. Between each odometer and a Main Processor, the pulse train is input to the VCU and preprocessed in an 8-bit microcomputer.

The preprocessing function consists of counting the number of incoming odometer pulses received and also keeping a count on a 200 KHz reference clock. The reference clock provides time base information between odometer pulses to the Main Processor over the time interval between samples taken from the preprocessors; this information is used to compute the speed and position data.

Also implemented in the preprocessor microcomputer is an algorithm used to detect missing and extra pulses in the odometer pulse train. This algorithm is required to ensure the integrity of the speed and position calculations.

#### 6.3.1.6 Fiber Optic Propulsion Data Link

The propulsion data link is the interface between the VCU and the vehicle propulsion controller. For any low power level digital processing equipment, such as the VCU, the propulsion unit poses a threat as a high power electrical noise generator. The use of a fiber optic link eliminates electrical noise interference on the connecting cables from being coupled into the VCU, thus enhancing electromagnetic compatibility.

Our conclusion is that systems employing microelectronic circuits in electrically noisy environments, such as transit systems, must be designed with emphasis on keeping the noise levels within tolerable limits. Fiber optic data link interfaces are necessary to meet the design requirements and will be used more as microelectronics increase within the transit industry.

### 6.3.2 Conclusions Based on Design Experience

This section will delineate what we would do differently in the design of the hardware based on our current design experience.

The design of the VCU was carried on over several years and during this period the electronics industry continued its fast technological advancement. If existing parts could be replaced with new parts the present ten program storage memory chips, on the main Processor card, would be replaced by two larger capacity memory chips. Also, the use of programmable logic devices would be used more extensively on the Communications Processor card and the Main Processor card. These refinements would allow the Main Processor and the Communications Processor to be combined onto one card.

The non-volatile RAM presently used is the one circuit that would be replaced; a CMOS RAM with battery back-up is a much better choice. The non-volatile RAM performs the function it was designed to do but it takes two memory chips to provide 256 bytes of data storage, plus a significant amount of additional circuitry to generate a store and recall pulse (see Section 4.2.1.5) to operate the non-volatile function. A single CMOS chip would provide 1k bytes of storage with minimal additional parts required for battery back-up.

There are several areas where design changes have been suggested; however, on analysis these changes offer no advantage over the present design. The VCU hardware as designed and tested performs the AGRT Command and Control functions very adequately and is deemed to be a good design.

### 6.3.3 Future Design Considerations Based on Advances in Technology

The VCU design is based on NMOS/Bipolar TTL (N-Channel Metal Oxide Semiconductor/Bipolar Transistor Transistor Logic) integrated circuit chip technology. These technologies were the industry standards through the 1970's and early 1980's. Today, one of the oldest MOS technologies, CMOS (Complementary Metal Oxide Semiconductor) has emerged as a leading candidate for any new design consideration.

The early drawbacks that discouraged development of CMOS (slow speed and high fabrication costs) have been overcome and CMOS devices are in direct competition with NMOS/Bipolar TTL parts. Today CMOS microprocessors compete in functionality, complexity, and speed with NMOS; most popular NMOS microprocessors have direct CMOS replacements available.

Two significant advantages are provided by a CMOS design. The first is that typically, noise immunity of CMOS devices is considerably greater (on the order of 50%), which is very attractive in electrically noisy environments. The second advantage is the reduction in the power requirement; a reduction factor of ten or greater is realizable.

Lower power decreases operating temperatures, which results in higher reliability. It also minimizes the need for cooling equipment and power supplies. This reduces system parts count and cost, and again increases reliability. Lower temperatures and lack of the need for cooling ports allows the use of sealed enclosures, which in turn improves noise immunity and further increases the reliability of the system.

### 6.3.4 Applications for High Technology Hardware in the Transportation Industry

The basic VCU architecture, with distributed processing and software control, can handle virtually any job requiring the processing of input data, storing the data, making calculations and decisions, and outputting signals based on past and present information.

A high technology design, as applied to the AGRT VCU, could be utilized in many areas of the transportation industry. These are a number of applications for which the design is suited: the obvious being an automated train system, but in addition a single channel could monitor and supply warnings and prompts to the operator of a manually controlled train. A train line diagnostic system could be installed on a train to pinpoint present and predict future problems. With the addition of a non-volatile memory, status and events prior to an accident could be saved for post accident processing. Another device of this type could be implemented as an automatic tester of a train system. Maintenance personnel would plug the unit into a diagnostic connector on a train car; the unit would provide stimuli, and then display a readout of the train's status.

It should be noted that each application suggested would require some hardware changes and software written for the specific application, but the basic technology is developed and available.

#### 6.4 Software

This section highlights the areas of the VCU software that enhance or detract from important features such as: reliability, operability, maintainability, testability, expandability, and safety.

##### 6.4.1 Design features

###### 6.4.1.1 The Executive

The fixed rate cyclic executive of the VCU main processor has been demonstrated as safe and reliable. Design simplicity, resulting from the cyclic timing and sequencing functions, has resulted in an executive with enhanced testability as it allows full analysis of failure modes, detection schemes, and reaction to such failure modes. While a cyclic executive does not easily allow modification of task execution rates it does allow simple addition of new tasks (at allowable rates of 10 or 40 milliseconds).

Confidence provided by the timing and sequence clarity more than offsets the reduced flexibility resulting from the fixed rate cyclic executive design chosen. The present design now utilizes less than half of the available time for performing control functions, thus allowing program expandability. This also permits the use of high order language as timing is not as critical as with an interrupt driven system.

#### 6.4.1.2 High Order Language

Using a high order language, "C" in this case, for coding of the design enhances testability and maintainability. Most high order languages allow both static and dynamic analysis of code, which simplifies module testing. The software tools available in the "C" programming environment catch most coding errors, which are a large part of what module testing is intended to flush out. Relief from the checking of mechanical details allows more time to check the design of the module against higher level requirements, in conjunction with module integration testing.

The design is commented, cross referenced, and documented. Every logic step is explained in the source code, statements are commented, module functions are described, and complex cross module functions are explained. Variable usage and type are explained in the code.

#### 6.4.1.3 Emergency Code Exercisers

The VCU simulates emergency conditions in background to verify the hardware's ability to process safety critical code. These continual checks

enhance safety. There appears to be no other way to gain the same confidence that the system will not fail when needed. The cost of this confidence comes at the expense of cross-coupled code; that is, the emergency code and the exercisers are intimately related and changes in one affect the functionality of the other. This is a maintenance and operability headache.

Future developments in hardware and software technology should be studied for ways of eliminating the need for this type of feature.

#### 6.4.1.4 Dissimilar Software

The enhancement of safety by continually demonstrating that the code in the system is generating commands that are correct is important. The VCU does this by using a secondary algorithm to keep checks on the primary algorithm. There is technology emerging today which can prove the correctness of code. So far these techniques have been applied only to very simple logic. As that methodology is developed, the need for dissimilar software (to assure that there are no unsafe errors in the code) will disappear. Until then the use of dissimilar software is necessary.

#### 6.4.1.5 RAM and Register Checks

The VCU checks the integrity of its CPU registers and RAM cells on a continuing basis in background. Most microprocessor based control systems do these checks only during initialization. Such continual checks enhance the safety of the VCU. The only negative aspects to these continual checks of RAM and registers are:

- 1) The need to assure that dynamic memory checks will not conflict with checks by other processors that access the same memory cells, as is the case of the Data Exchange Unit in the VCU. This reduces maintainability and reduces confidence in operability.
- 2) The added exposure to EMI noise that could spoil any use of the system bus. Modern technology, however, has reduced this vulnerability to negligible significance.

#### 6.4.1.6 Fault Queue Management

The concept of a fault recorder in software is a good one. The implementation could be expanded to include a wide range of data to be recorded under certain conditions. The recording in the present system is limited to anomalies and the order in which they are detected. With a simple real time clock a variety of events could be recorded with corresponding time tags.

The fault queue concept has proven to be of great value in system testing and would be of equal value in system maintenance.

#### 6.4.2 Conclusions Based on the Design Experience

This section delineates what we would do differently in the design of the VCU software based on our current design experience.

A design drawback is the lack of integration of safety features with operability features. Safety and operability requirements evolved as the design advanced. The early emphasis was on safety. We did not fully consider the effect on system operability of incorporating new safety requirements into the software design. Subsequent considerations of recovery from detected errors or recognition and recovery from false alarms were found to require a major reorganization and design of the safety features. Anomaly management was outside the AGRT software task scope. However, design for safety without consideration of safety's effect on reliability and operability is not realistic. Operability and safety are not separate features of a control system. They must be integrated aspects of the control system design dealt with at the onset of the basic software architecture design. It is recommended that future design processes incorporate more safety/operability trade-off analyses to avoid such problems.

Lack of ability to turn off the emergency code exercisers, that is, the background selftests, proved to be a hindrance during some phases of testing as occasionally a test would fail and stop the CPU. It would be

desirable to have some way of preventing the execution of these tests or preventing the halting of the CPU, at least during the test phase. It is not clear whether such a capability would be present in a deployed system.

There are trade-offs between maintainability and testability with respect to the scope of variables. Good software design practice includes information hiding which means using local variables when possible. However any variable that needs to be output as a testpoint has to be a global variable, for access by the testpoint module. There are some instances in the code where local variables are used that in hindsight would be made global to assist in the debug/test portions of the project. In the "C" programming environment, any module using an external, global variable must explicitly declare that variable. The static code checking tool flags any variables not so declared, or incorrectly declared. These features lessen the potential negative impact of using all global variables.

## 6.5 Test

Subsystem level testing of the VCU generally went smoothly. The number of problems encountered was small for equipment of this complexity and most problems were minor in nature. The lack of significant conceptual problems is, in large part, due to the amount of analysis and simulation conducted early in the program. The significant problems that were encountered tended to be in areas involving interfaces or interactions between functions. The emphasis on peer code review and on module testing further helped to keep the number of problems to a minimum.

### 6.5.1 Built in Test Points

The ability to test a microprocessor-based controller depends in large part on the ability to monitor internal variables during actual operation. The VCU design recognizes this need and includes 8 test points per



channel. Any 8 variables can be output and they are output in both analog and digital form. Which 8 variables are output is controlled via a built in software function.

The test point capability described above proved invaluable during checkout and testing. It also provides a valuable maintenance feature and ultimately could serve as the basis for the design of automated test equipment. This feature should be carried forward in any future design effort.

#### 6.5.2 Real-Time Closed-Loop Testing

Because of the many safety interlocks in the VCU, some of the functions can 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. An extensive test set was developed to allow real-time closed-loop testing of the VCU in the laboratory. While this approach is expensive, the resulting capability proved invaluable. Performing a similar check-out on a test track would be much more expensive and time consuming.

The need for closed-loop laboratory testing was initially underestimated. In hindsight, we feel that less effort should have been spent on software module testing and more on the closed-loop effort. As noted in paragraph 6.1.2.3, future efforts should also consider the possibility of off-line closed-loop testing of the actual VCU code.

The VCU test set was used in both developmental and formal testing. Not only was it valuable in discovering and troubleshooting problems, it also forced a logical build up of the VCU. 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 troubleshoot a large number of problems at one time.

### 6.5.3 Digital Data Acquisition and Processing

The closed-loop VCU test set includes a digital data acquisition and processing capability. This capability was not originally planned but was added as a logical extension when the decision was made to go with a digital rather than an analog computer for purposes of simulating the vehicle.

The ability to record the actual sequences of numbers produced by the VCU proved to be a significant time saver. It allowed the quick identification and resolution of a number of problems that would have possibly taken months to resolve using conventional analog troubleshooting methods.

The digital data acquisition and processing system also allowed a more precise verification of compliance with requirements during formal testing than would have otherwise been possible. The accuracy afforded by the system allowed the identification of small discrepancies that might otherwise have been missed.

### 6.6 Availability

Early in the program the contract was modified in a form that deleted consideration of system availability (freedom from service interruption). As a result, emphasis was placed on features necessary to provide an acceptable level of safety in a microprocessor-based system, without regard to requirements for availability. This section treats the question of how availability may be enhanced in such a system. The subject was treated in more detail in the technical paper: "Effects of System Architecture on Safety and Reliability of Multiple Microprocessor Control Systems" (see Bibliography, Section 7.0).

Several configurations of microprocessor-based control systems are shown in Figure 6.6-1. The "duplex" configuration in the left-hand sketch is

that which was developed in the C&CS development program described in previous sections. The other sketches illustrate the use of additional

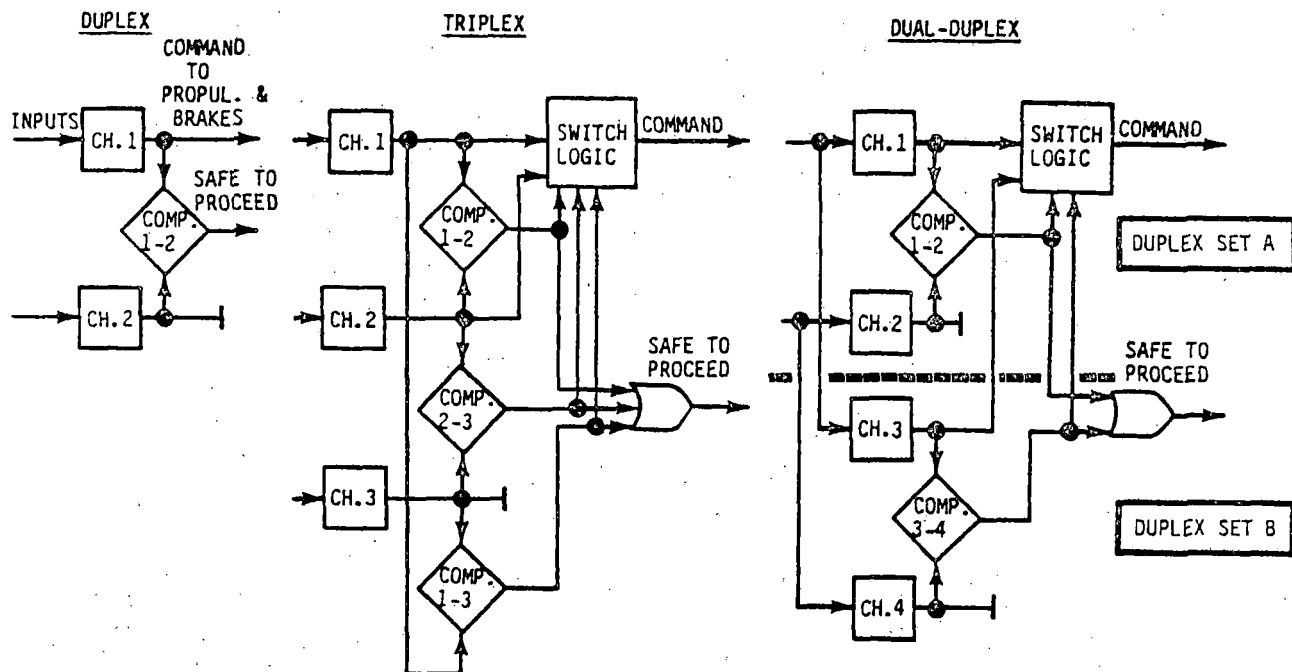


FIGURE 6.6-1: COMPARISON OF CONTROL SYSTEM CONFIGURATIONS

microprocessors to provide a backup in case one microprocessor channel fails. Control would be switched to a pair of working channels, retaining redundancy for safety in the pair used for control.

In the "triplex" system, continuous comparisons are made between the outputs of each pair of microprocessor channels. Motion would continue as long as any pair of channels indicates no discrepancy, i.e., "safe to proceed." Any discrepancy detected by a comparator would indicate that one of the channels had failed. Control would then be switched by the "switch logic" to whichever pair of channels does not show a discrepancy between their outputs. The output of one of the two channels would then be used for command of the propulsion and braking system.

The "dual-duplex" system uses two "duplex" configuration sets in parallel. As long as one of the comparators indicates no discrepancy, it is safe to proceed. Control would be switched to the working set. This configuration uses the same hardware and software as the "duplex" configuration.

The effect of the configuration selection on the Mean Time Between Service Interruptions (MTBSI) is shown in Figure 6.6-2 for several examples of microprocessor channel failure rate and number of microprocessor-based elements in a transportation system. If the channel failure rate is low, say 0.0001 failures per hour (MTBF = 10,000 hrs), and a small number of vehicles or elements is used, say 10, then the system can expect to operate an average of 500 hours between service interruptions. This would generally be considered acceptable, and no additional redundancy would be required. However, if higher failure rates are encountered or if more elements were used, the MTBSI would be 5-50 hours; this would probably not be acceptable, and additional redundancy for availability should be used.

Once an additional microprocessor channel is installed, either in a triplex or dual-duplex configuration, the MTBSI increases to such a high

level that the control system is no longer a factor in system availability. Service interruptions due to mechanical factors or other causes (not illustrated here) would probably dominate. The use of redundant channels has an additional advantage: the failure of a microprocessor channel would be signalled to system operators, who could then divert the impaired vehicle to a maintenance area for repair of the failure. Maintenance would be performed in a suitable work environment, rather than on the guideway. Therefore repairs, although more frequent than with a duplex system, would probably cost less to perform. A considerable time can be permitted to elapse before the impaired vehicle is removed from service without risking a second failure that would shut the vehicle down. A "vehicle removal time" of one hour was assumed in the calculations for Figure 6.6-2; larger values would not significantly affect the conclusions.

The choice between a triplex and a dual-duplex configuration, if additional redundancy is required, should be based on convenience rather than on any precise measure of performance. If a system was implemented using two or more completely packaged minicomputers, then a triplex system would be less costly than a dual-duplex system. If, however, the control system is built up from individual chips, as was demonstrated in the AGRT C&CS program, then a dual-duplex system would use fewer components and would be preferable to a triplex system. A comparison of system complexity is shown in Figure 6.6-3 (see referenced technical paper for more details of component configuration).

Using the estimated configuration complexities above, the principal performance measures have been calculated for each configuration and are shown in Figure 6.6-4. They may be summarized by saying that either the duplex, triplex, or dual-duplex configuration would provide adequate time between unsafe failures (MTBUF; the goal is  $10^6$  years or more) and substantially greater MTBSI than that of a duplex system. Both would have less time between failures requiring maintenance actions (see Mean

Time Between Failure, or MTBF) than the duplex system and thus should be installed only when required to meet MTBSI goals.

Channel Failure Rate Hr <sup>-1</sup>	No. of Vehicles or Elements	MTBSI - Hrs, For Indicated Config.		
		Duplex	Triplex	Dual-Duplex
.0001	10	500	$1.67 \cdot 10^6$	$1.25 \cdot 10^6$
	100	50	$1.67 \cdot 10^5$	$1.25 \cdot 10^5$
.001	10	50	$1.67 \cdot 10^4$	$1.25 \cdot 10^4$
	100	5	1670	1250

FIGURE 6.6-2: TYPICAL INTERVALS BETWEEN SERVICE INTERRUPTIONS

Configuration	Duplex	Triplex	Dual-Duplex
Components:			
Microprocessors	2	3	4
External "And" Gates	1	3	2
Timing Check Devices	2	3 or 6	2 or 4
Shared Memory Units	1	3	2
Input Sensor Sets	2	2 or 3	2
Total No. of Components	8	14 - 18	12 - 14
Overall Hardware Complexity Ratio	1.0	2.0	1.8
Overall Software Complexity Ratio	1.0	1.0+	1.0

FIGURE 6.6-3: COMPLEXITY COMPARISON

Configuration	Duplex	Triplex	Dual-Duplex
Hardware Complexity Ratio (per Fig. 12)	1	2	1.8
Equivalent Channel Failure Rate - hr <sup>-1</sup>	0.00010	0.00013	0.00009
MTBUF - Yrs.	$4 \cdot 10^8$	$8 \cdot 10^7$	$2.5 \cdot 10^8$
MTBSI - Yrs.	0.6	$1.1 \cdot 10^3$	$1.8 \cdot 10^3$
MTBF - Yrs.	0.6	0.3	0.3

FIGURE 6.6-4: CONFIGURATION PERFORMANCE COMPARISON

It is our view that the dual-duplex configuration can be developed more easily and with less risk than a triplex system and thus is the preferred choice for microprocessor-based control systems.

## 7.0

## BIBLIOGRAPHY

"MPRT Longitudinal Control System Design Summary"

Report No. UMTA-MA-06-0048-75-4

Final Report, December 1975. R. P. Lang

"Morgantown People Mover Inductive Communications System Design Summary"

Report No. UMTA-MA-06-0048-78-6

Final Report, December 1978. T. N. Johnson

"Morgantown People Mover Redundant Computing System Design Summary"

Report No. UMTA-MA-06-0048-80-8

Final Report, September 1980. J. Rucker and B. Hill

"Morgantown People Mover Collision Avoidance System Design Summary"

Report No. UMTA-MA-06-0048-80-9

Final Report, September 1980. R. J. Schroeder and R. S. Washington

"Morgantown People Mover Electromagnetic Compatibility Program"

Report No. UMTA-MA-06-0048-80-10

Final Report, September 1980. T. H. Herring

"AGRT Guideway Communications Unit Design Summary"

Report No. UMTA-WA-06-0011-84-1

Final Report, December 1984. C. W. Colson

"AGRT Odometer Data Downlink Collision Avoidance System Design Summary"

Report No. UMTA-WA-06-0011-84-2

Final Report, October 1984. C. W. Colson, R. J. Schroder, W. B. Chapman

"Programmable Digital Vehicle Control System"

28th Vehicular Technology Conference - IEEE

Technical Paper, March 1978. R. P. Lang, D. B. Freitag

"Digital FSK Receiver Capable of Operating in High Impulse Noise

Environments" 31st Vehicular Technology Conference - IEEE

Technical Paper, April 1981. E. Nishinaga

"Failsafe Synchronization of Redundant Microprocessor Control Systems"

32nd Vehicular Technology Conference - IEEE

Technical Paper, May 1982. D. E. Haberman

"A Vehicle Collision Avoidance System Using Time Multiplexed Hexadecimal

FSK" 33rd Vehicular Technology Conference - IEEE

Technical Paper, May 1983. C. Colson, E. Nishinaga



"Microprocessor Based Speed and Measurement System"  
33rd Vehicular Technology Conference - IEEE  
Technical Paper, May 1983. R. P. Lang, D. J. Warren

"An Implementation of Distinct Software In a Vehicle Controller"  
33rd Vehicular Technology Conference - IEEE  
Technical Paper, May 1983. W. E. Greve, R. J. Schroder

"Effects of System Architecture on Safety and Reliability of Multiple  
Microprocessor Control Systems" 34th Vehicular Technology Conference -  
IEEE Technical Paper, May 1984. R. C. Milnor, R. S. Washington