AATC Implementation Project for AATC, 1999

BART's AATC Program Will Revolutionize Train Control – by Katie Harrar

Imagine trains moving through the BART system faster, closer together, and more smoothly. Now picture these trains being controlled by a network of radios located on the trains and along the track. This is not a theoretical technology for the distant future; it's Advanced Automatic Train Control (AATC)—a project currently in development at BART.

BART began work on AATC more than five years ago, and is currently in the middle of Phase 2, which is the design and safety certification phase. Below is a brief description of the project and how it will affect BART.

What is the basis for the Advanced Automatic Train Control (AATC) technology?
The AATC system is based on an extremely reliable, completely wireless data radio network known as the Enhanced Position Location Reporting System (EPLRS), which was originally developed by Hughes Aircraft for the U.S. Army. The system utilizes spread spectrum radios to maintain point to point communication between mobile units and base stations.

How is BART adapting this technology?
A unique aspect of the EPLRS technology is its ability to accurately determine the position of mobile radio units by measuring the time required for the radio waves to travel from a radio transmitter to a radio receiver. Radios will be installed on trains and along the track and will communicate vital information to and from control stations. It will be the first system of its kind in the world.

How will AATC benefit BART?
BART will be able to run trains at higher speeds and more closely together while maintaining all safety requirements. This will enable BART to increase train and passenger capacity on AATC-equipped lines without adding tracks or vehicles. Since trains will also take less time to complete each trip, the system will be able to carry more people with the same number of cars.

What is the AATC project team?
The AATC team consists of BART and its prime contractor, Harmon Industries, Inc. BART's multi-disciplinary team is made up of staff from nearly every department at BART as well as outside consultants. The project began at BART in the R &D Department and is currently coordinated by Transit Systems Development. Harmon, a leading supplier of signal and train control products, licensed the EPLRS technology from Hughes and is adapting the radio technology to the train control world. The BART/Harmon team is a unique partnership because the parties are jointly developing the software applications, testing the equipment, and implementing the system. BART and Harmon are also sharing the system development costs, and BART will receive royalty payments from Harmon on their sales of AATC equipment to other railroads and transit agencies.

Where will the AATC system be implemented?
The system will be implemented from Bay Fair to Daly City.

What is happening now?
Currently, project staff are conducting lab integration testing, installing radios and antennas at the Hayward test track and between the Oakland Wye and the Coliseum station. Train operators may already see radios mounted on the ceilings of the Oakland Wye tunnels and antenna platforms on the aerial structure between Lake Merritt and Coliseum stations. Harmon has also set up a project trailer at the test track.

Look for more information about AATC in future issues of BARTalk.

Advanced Automatic Train Control Implementation Project

Monthly Manager's Meeting

March 4, 1999

PROJECT HISTORY

AATC PROJECT HISTORY

TECHNOLOGY SURVEY

91 93

- Contacted 40 + companies
- Preliminary specification / proposals
- Formal RFP
- Selection of Hughes/MK

DARPA PROGRAM

94 96 98 01

Phase 1

Hughes/MK

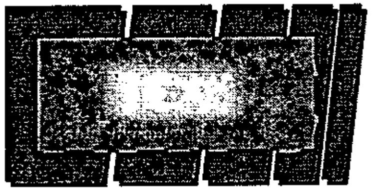
- Prototype design
- Test Track demo

Phase 2

Harmon Industries

- Production design
- Safety Certification

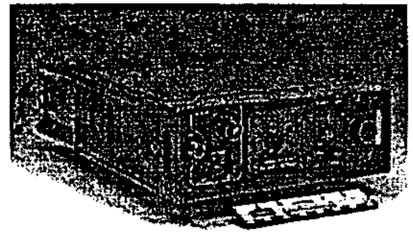
Technology Overview



System Architecture Overview

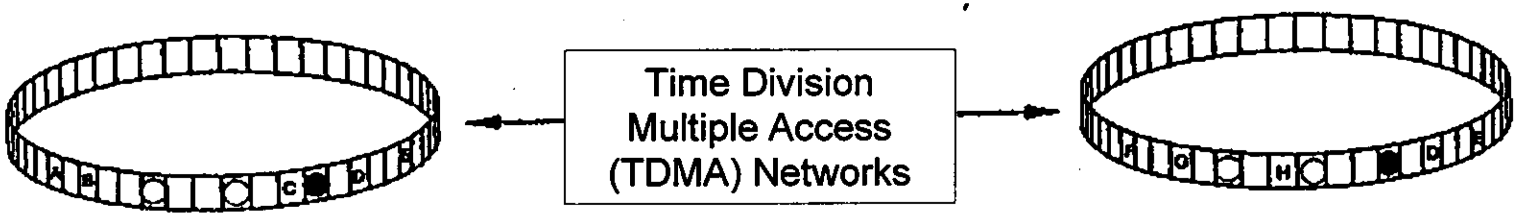
Radio units on end cars

- Communicate with wayside radios
- Determine range to wayside



Wayside Zone Controller

- Determines train position from range reports
- Determines and transmits speed commands to trains

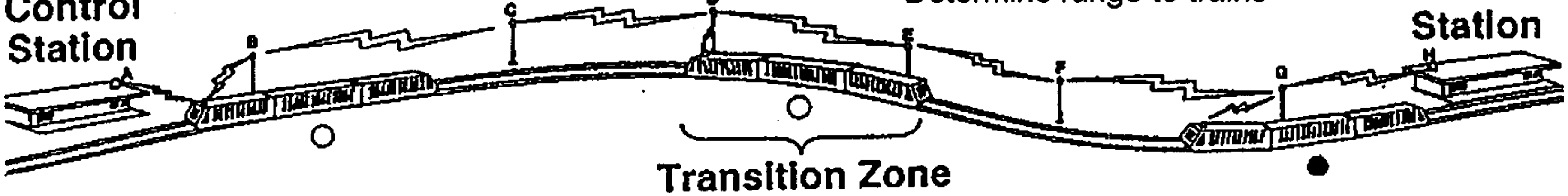


Network management

- Assigns time slots to radios
- Automatically bypasses failed radios

Trackside radio units

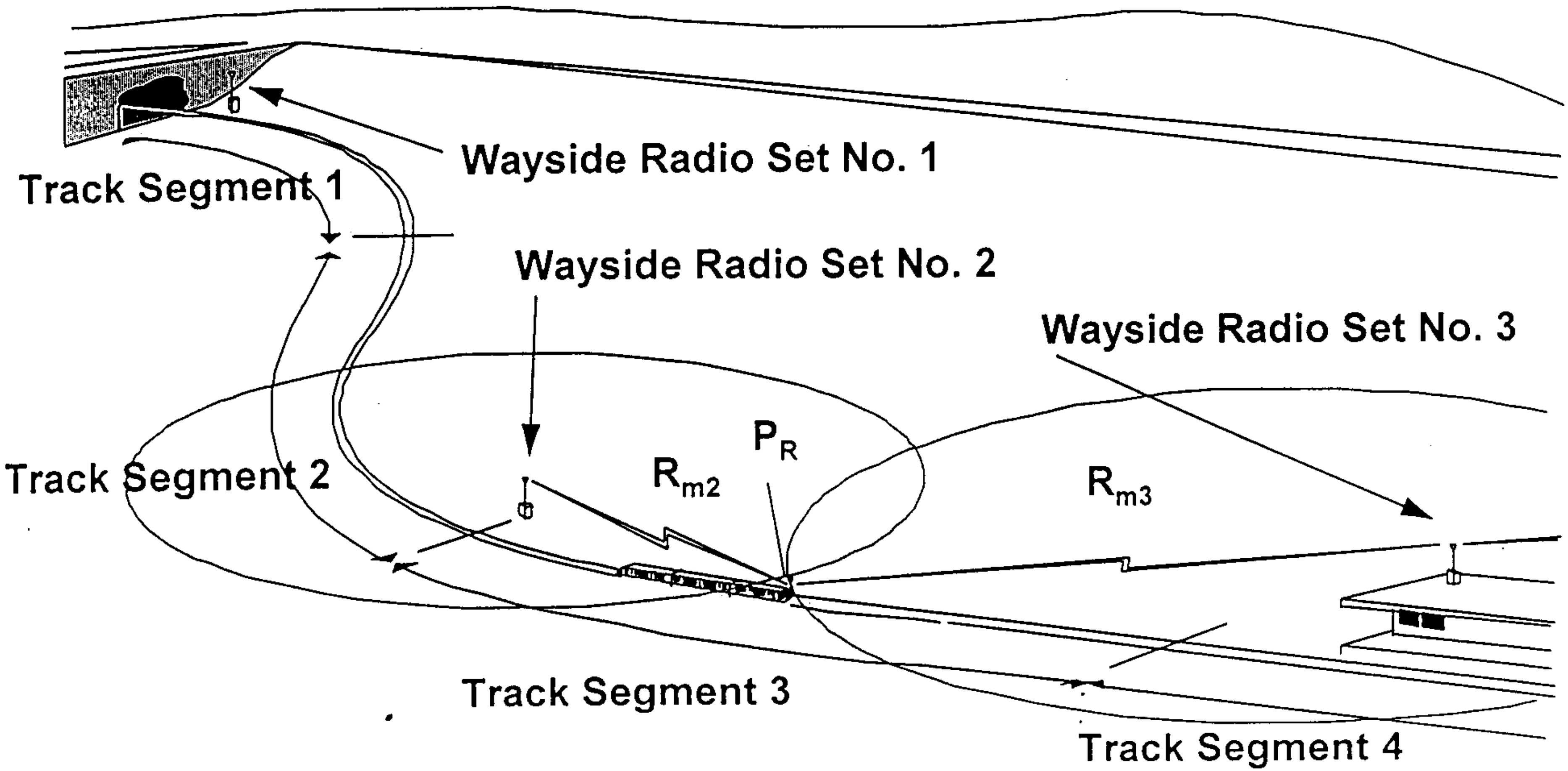
- Form wireless full duplex data bus
- Relay data between trains and station
- Determine range to trains



Spread Spectrum Transmission/Reception

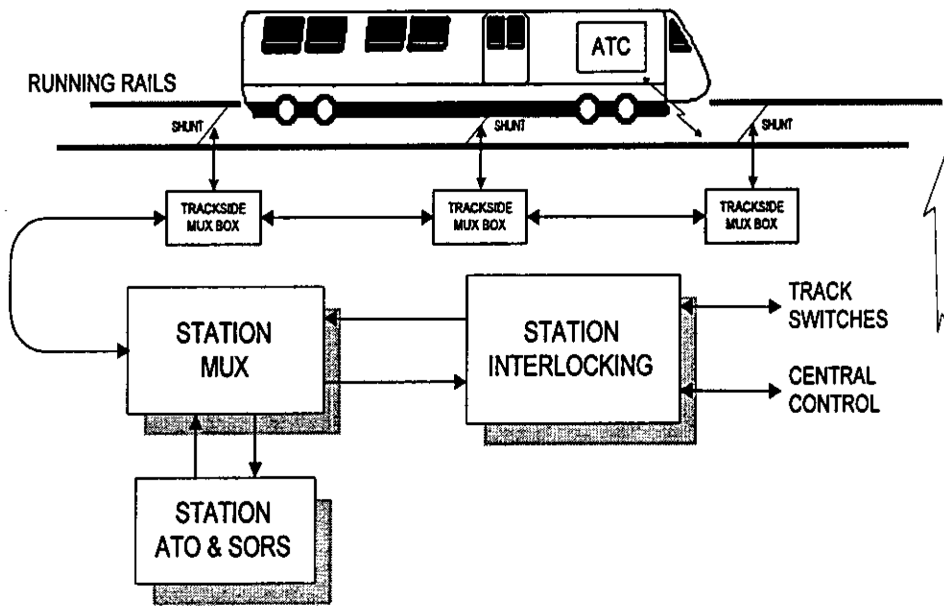
- Spread Spectrum supports:
  - Extremely robust data communication
  - Virtually impossible to counterfeit signal
  - Measurement of distance between radios by measuring radio propagation time (radio ranging)

Initial Train Location

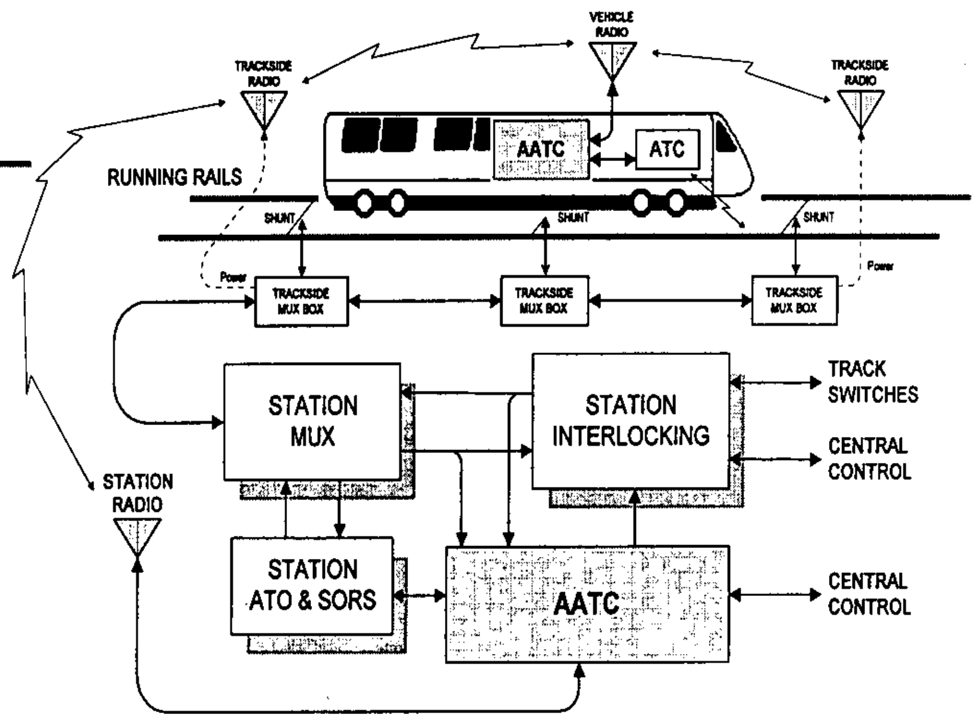


AATC Overlays On Existing System

Existing Train Control

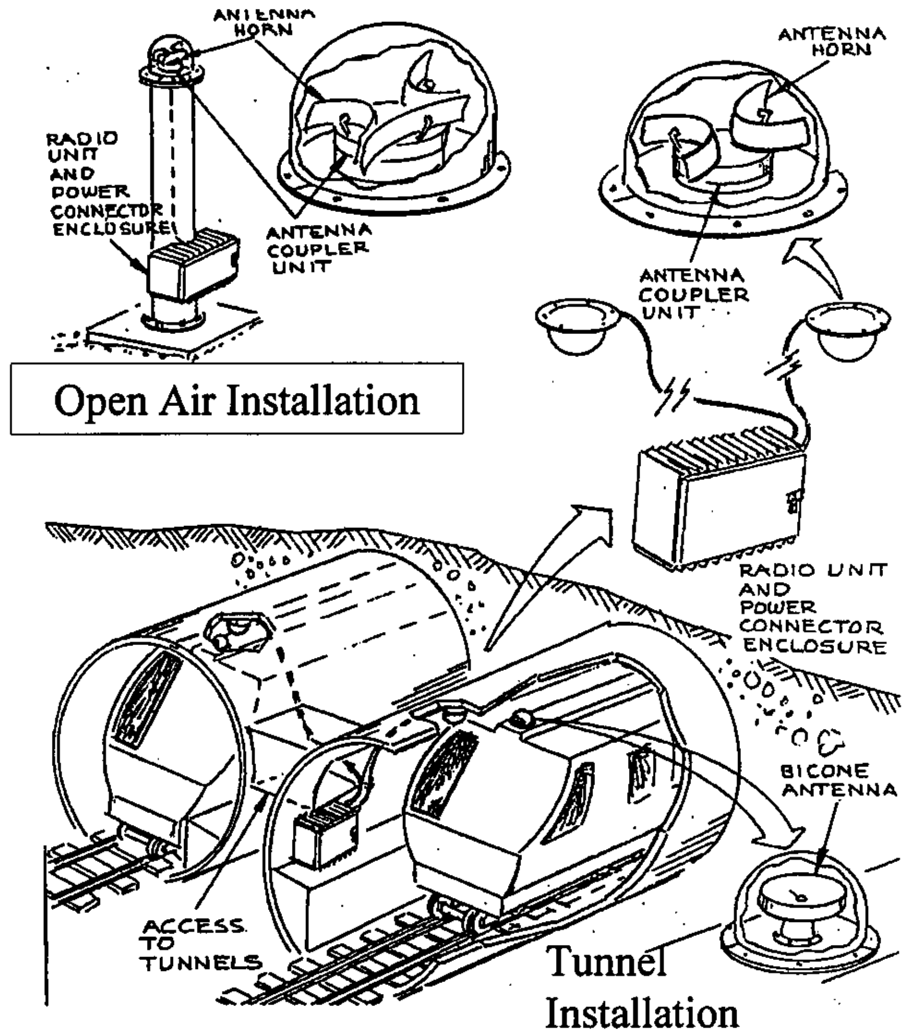


AATC Integration



Ease of Installation

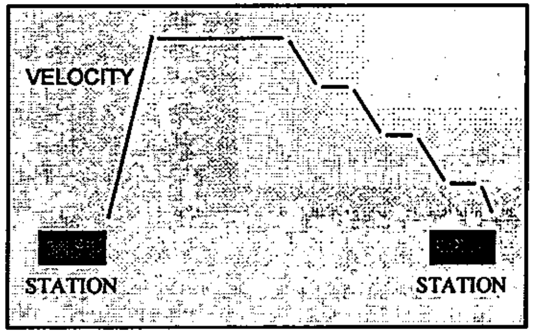
- No wayside signal cabling.
- No Truck mounted equipment.
- Vehicle centric approach will allow installation on 6 to 8 cars per month - 2.8 to 3.7 years to do the fleet.
- AATC approach will allow installation on 30 to 45 cars per month - 6 to 9 months to do the fleet.



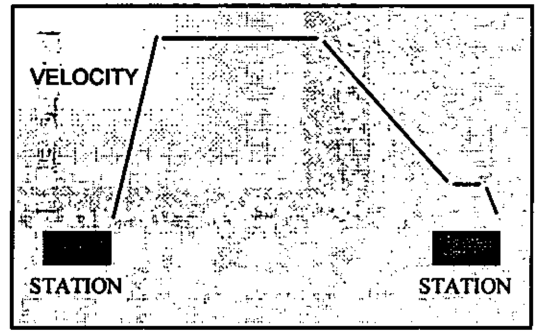
Reduced Brake Rate Saves Energy and Time

- **11% ENERGY SAVINGS AT THE METER**
- **4% FASTER**
- **IMPROVED PASSENGER COMFORT**

EXISTING SYSTEM



AATC SYSTEM

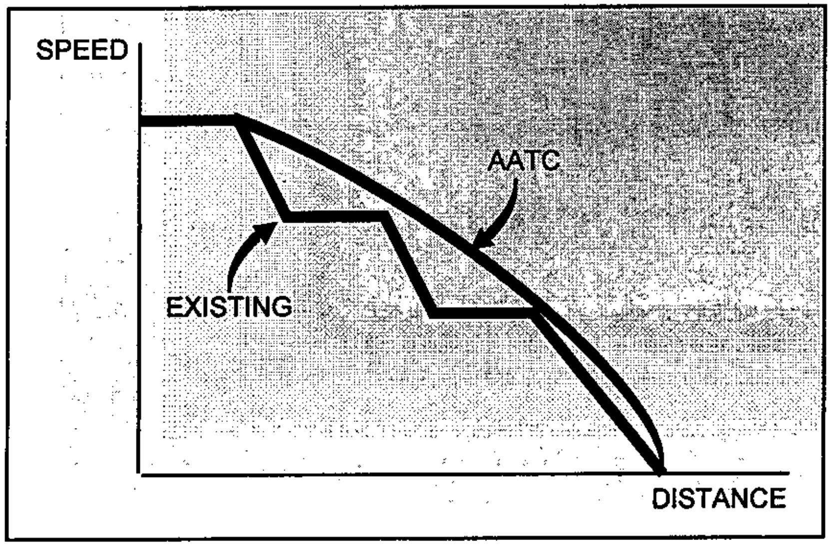


	KWH (Existing System)	KWH (AATC System)
TOTAL ENERGY REQUIRED TO START OF BRAKING	2,945.3	2,945.3
PLUS ENERGY USED FOR STAIR-STEP SPEED MAINTAINING IN BRAKING	+243.8	+81.2
LESS REGENERATED ENERGY USED	-565.4	-685.7
TOTAL ENERGY AT THE METER	2,623.8	2,340.9

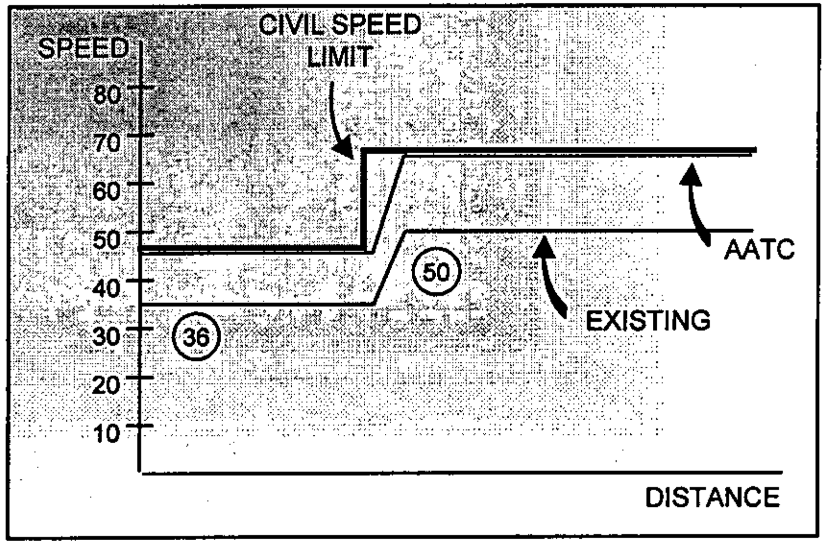
Finer Control of Speed

AATC provides two ways of reducing end to end trip times:

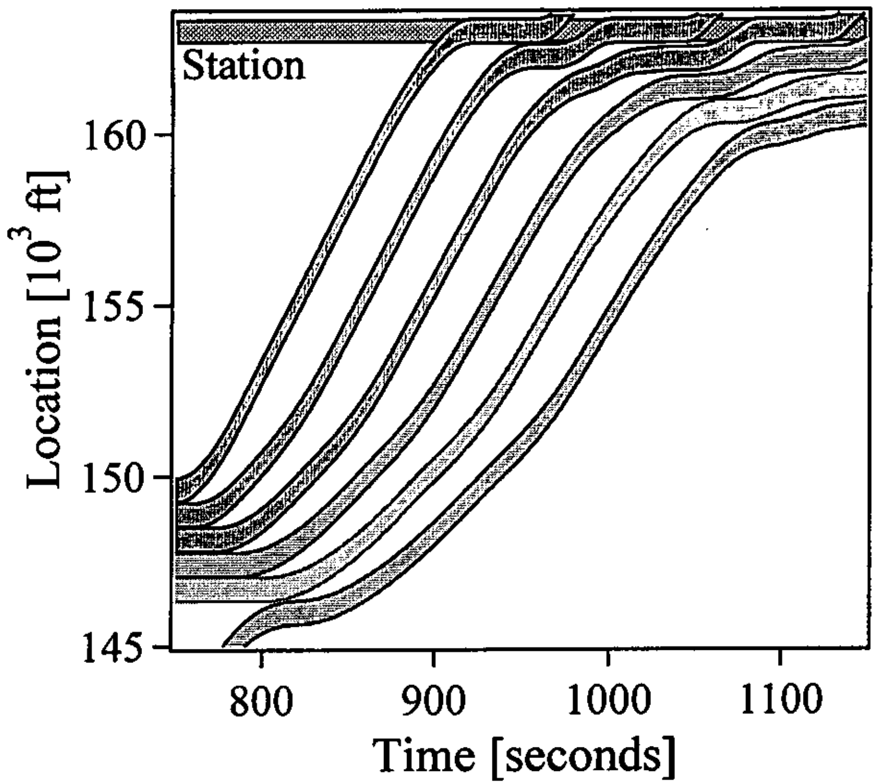
Reduced Brake Rate

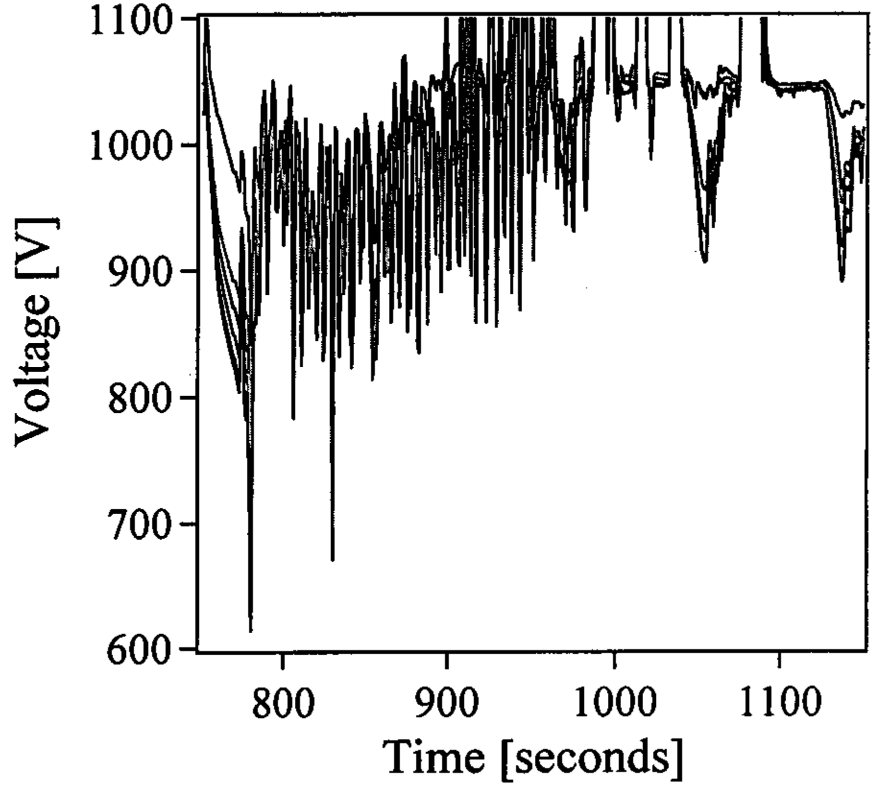


More Speed Codes

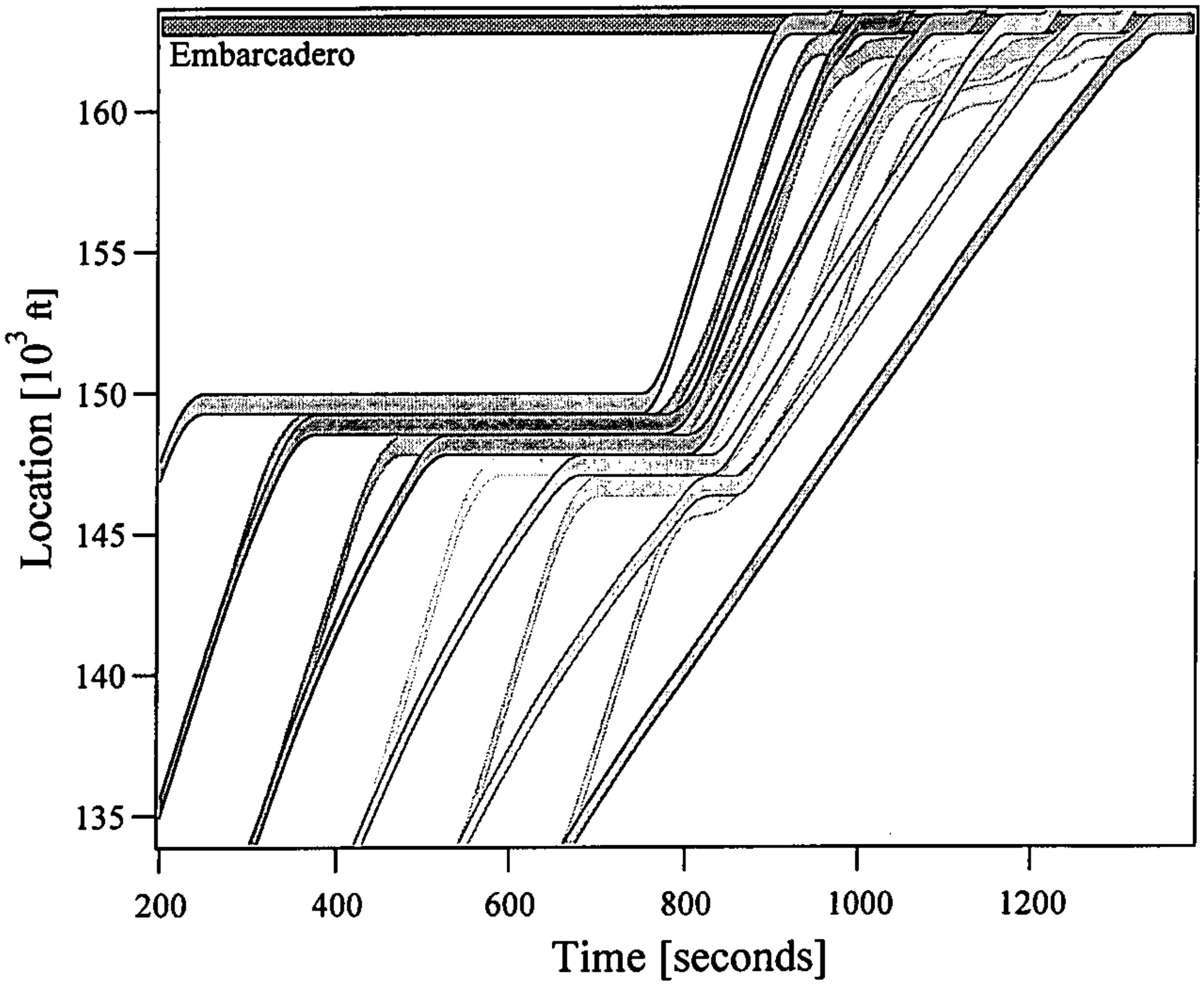


Nominal Control

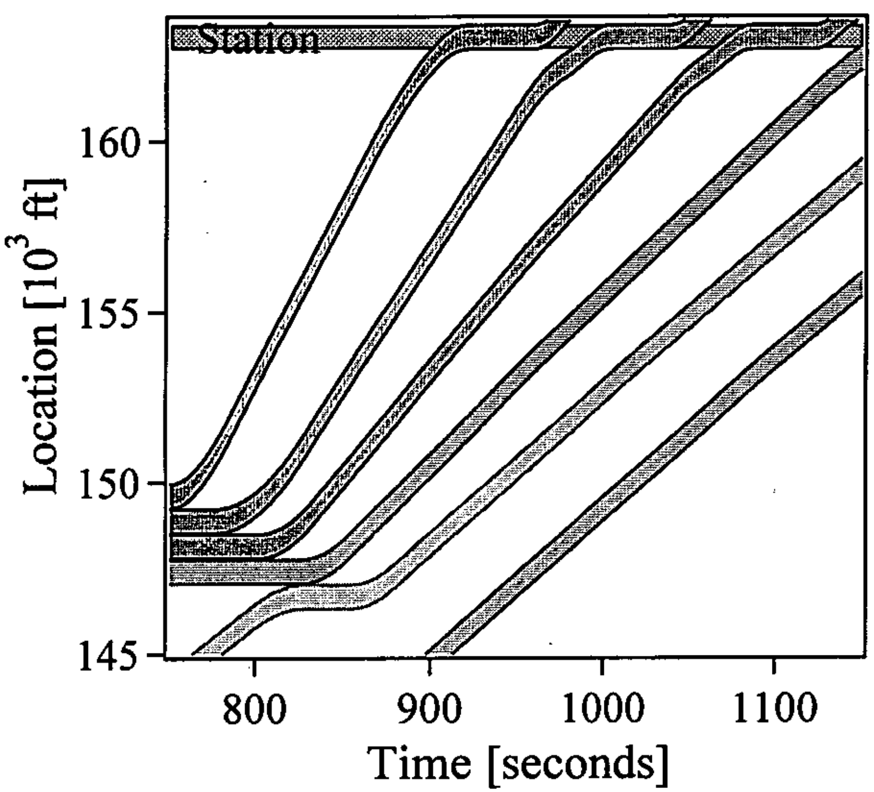


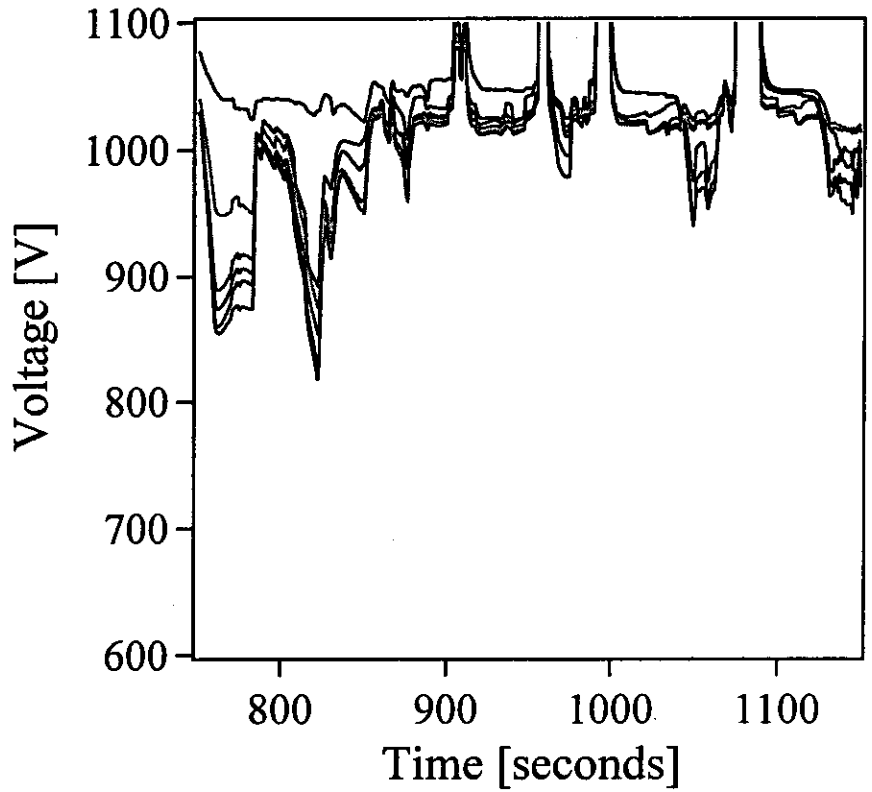


500-Second Delay in Tunnel



Enhanced Control





Operational Benefits

Operational Benefits

System Capacity Improvement Capacity

Increase traffic through Transbay Tube up to possibly 30 trains per hour

Schedule Recovery Capability

Train on-time performance preserved at near current levels

Fleet Size

Significant reduction in required fleet size for future service levels

GREATER OPERATING MARGIN SUPPORTS DENSER TRAFFIC

	Crush Capability	*Operating Margin for 2 Minute Schedule*
Existing A Line	150 seconds	- 30 seconds
Existing M Line	105 seconds	+ 15 seconds
AATC	80 seconds	+ 40 seconds

Calculated Train On-Time for Crush Headway

- Train on-time performance based on 5-minute margin (BART standard)
- Assume number of delays increase by 14.5% during transition from 3.75 minute headway to 2.0 minute headway (car hours will increase 35% and traffic density by 58%)

Scheduled Headway	3.75 min	2.25 min	2.0 min
Existing	93%	85%	73%
AATC	94%	91%	90%

AATC vs Existing Run Times

	AATC on A & M Line Only	*AATC System-Wide*
Daly City to Concord	minus 1:17	minus 4:17
Concord to Daly City	minus 1:58	minus 3:49

Estimated Vehicle Requirements

	FY 02	FY 06
15 Minute Service Intervals		
No AATC	547	563
AATC on A & M lines only	528	543
AATC On Entire Core System	528	533
12 Minute Service Intervals		
No AATC	563	571
AATC on A & M lines only	543	549
AATC on Entire Core System	536	542

AATC HARDWARE

Common in manpack, tactical vehicles and heliborne configurations, EPUUs provide user-to-user data communications, position, navigation and identification services to units both in the air and on the ground.

Lightweight and militarized, EPUUs supply the necessary mobility needed for the rapidly changing and demanding terrain and weather conditions of the battlefield.

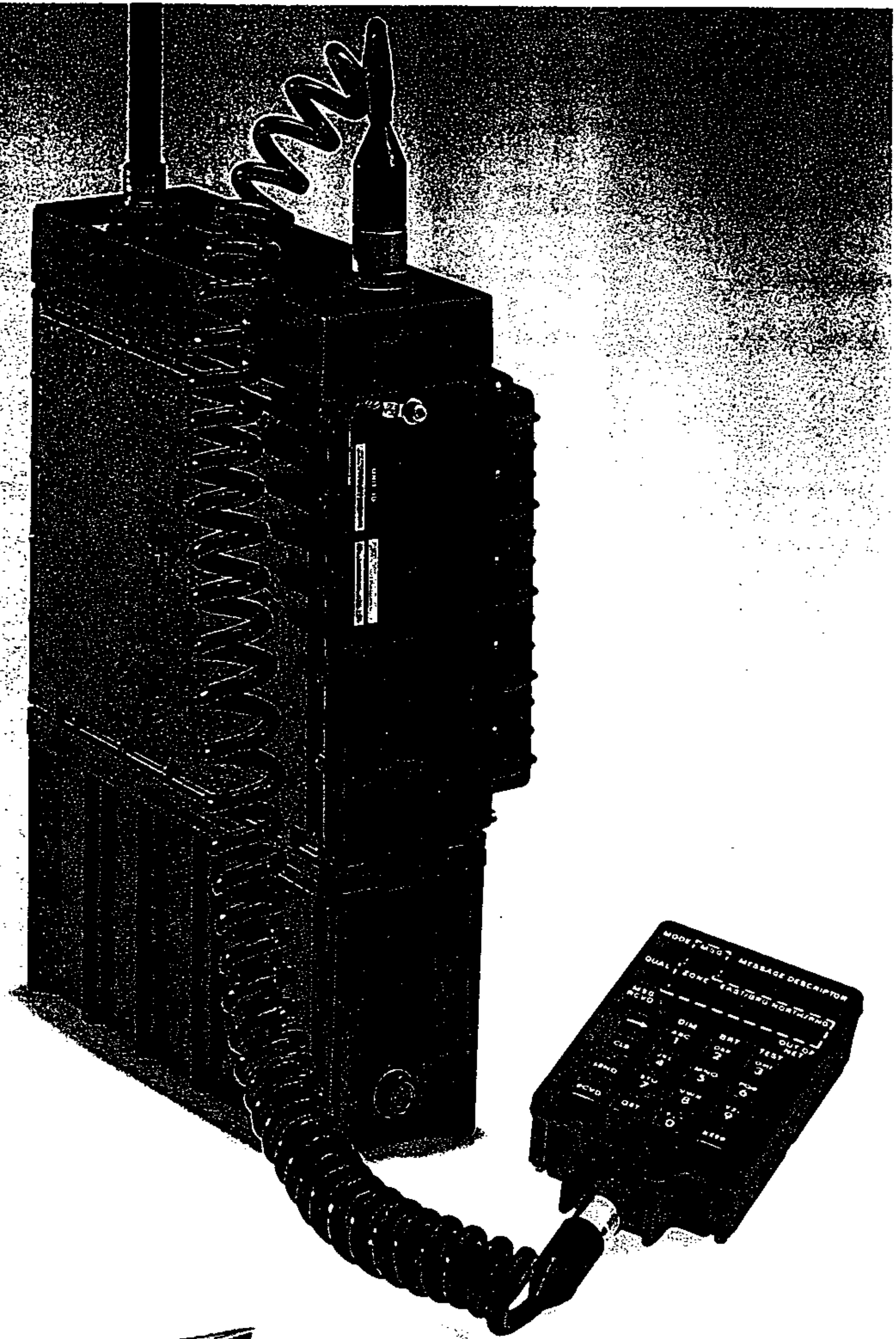
EPUU characteristics:

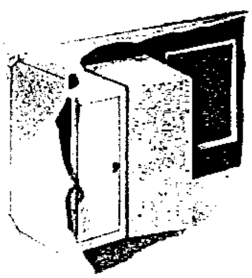
- Dimensions with battery box — 14"x10"x5"
- Prime power — 28 VDC, 16 watts
- Weight (including batteries) — 26 lbs.
- Volume — 660 cu. in.
- Output power — selectable: 100, 20, 3, 0.4 watts

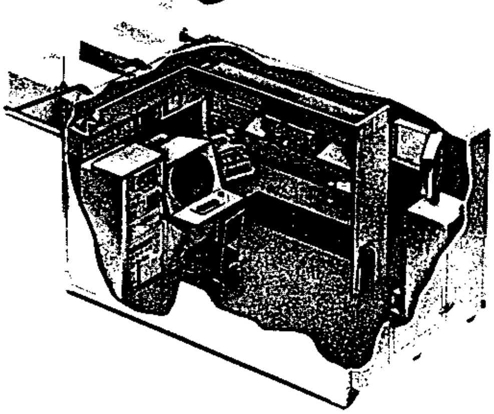
Net control stations, located in each brigade and in division rear, manage the data distribution function and provide position location, navigation and identification services. Data communications requirements, including response time and message traffic requirements for each tactical area, are specified by the NCS operator.

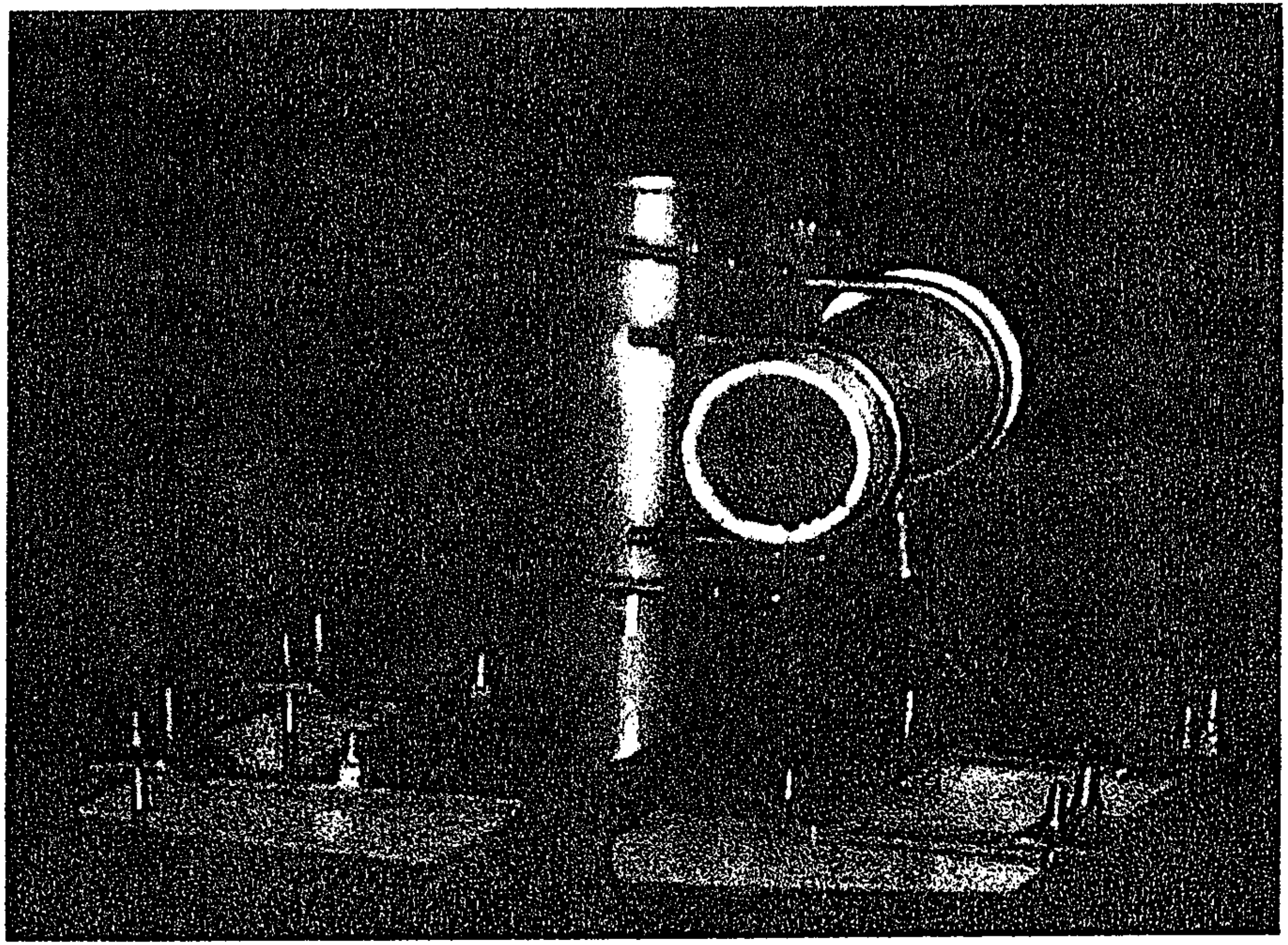
EPLRS system technical characteristics:

- Operating frequency — 420-to-450 MHz
- System architecture — synchronous time division multiple access, frequency and code division, multiplexed
- Typical system size — 500 to 1000 in division deployment with up to five net control stations
- Electronic countermeasures — spread spectrum, frequency hopping, error detection and correction, and automatic rerouting
- Security — embedded crypto, transmission security and dual level communications security
- Terminal data rates — multiple circuits with selectable rates, up to 1200 BPS simplex and 600 BPS duplex
- Navigation aids and services — more than 20 services: positions, navigation, zone alerts, lane guidance, friendly identification, etc.
- Position accuracy — 15 meters CEP









SUPPLEMENTARY TECHNOLOGY NEEDS

Supplementary Technologies

- Broken Rail Detection
- Silent Train Detection
- Station Berthing Control
- Enhanced Control Algorithms

Schedule

- Phase 1: Prototype 1994-1996
  - Initial Design
  - Test Track Testing
- Phase 2: Design and Safety Certification 1998-2000
  - Design Documentation
  - Fruitvale -- Lake Merritt -- Oakland Wye
  - 10 cars
- Phase 3: Implementation 2000-2002
  - Bay Fair -- Daly City
  - 289 cars; all Maintenance Vehicles
  - Training/Manuals/Spares

A Unique Partnership

- Phase 2
  - Harmon's costs shared at 50%-50%
  - Harmon investing in technology development
  - NTE for BART $5M

A Unique Partnership (cont'd)

Marketing

- BART's Interest
- Joint Participation in Conferences
- Technical Papers
- Industry Working Groups

Royalties

- To be paid by Harmon to BART for consideration of technology developed by BART
- Percentage of Harmon's future radios sales
- Fixed amount for each copy of software
- 15 years after completion of Phase 3

A Unique Partnership (cont'd)

The Project Team

- **BART: Staff from 3 Executive Offices**
  - Transit System Development
  - Budget and Business Management
    - R&D
    - System Safety
  - Operations
    - M&E
      - » Train Control Engineering
      - » Computer System Engineering
      - » Track and Structures
      - » Power Mechanical
    - Operations Liaisons
    - Transportation and System Service
    - Rolling Stock and Shops
    - Operations Training and Development

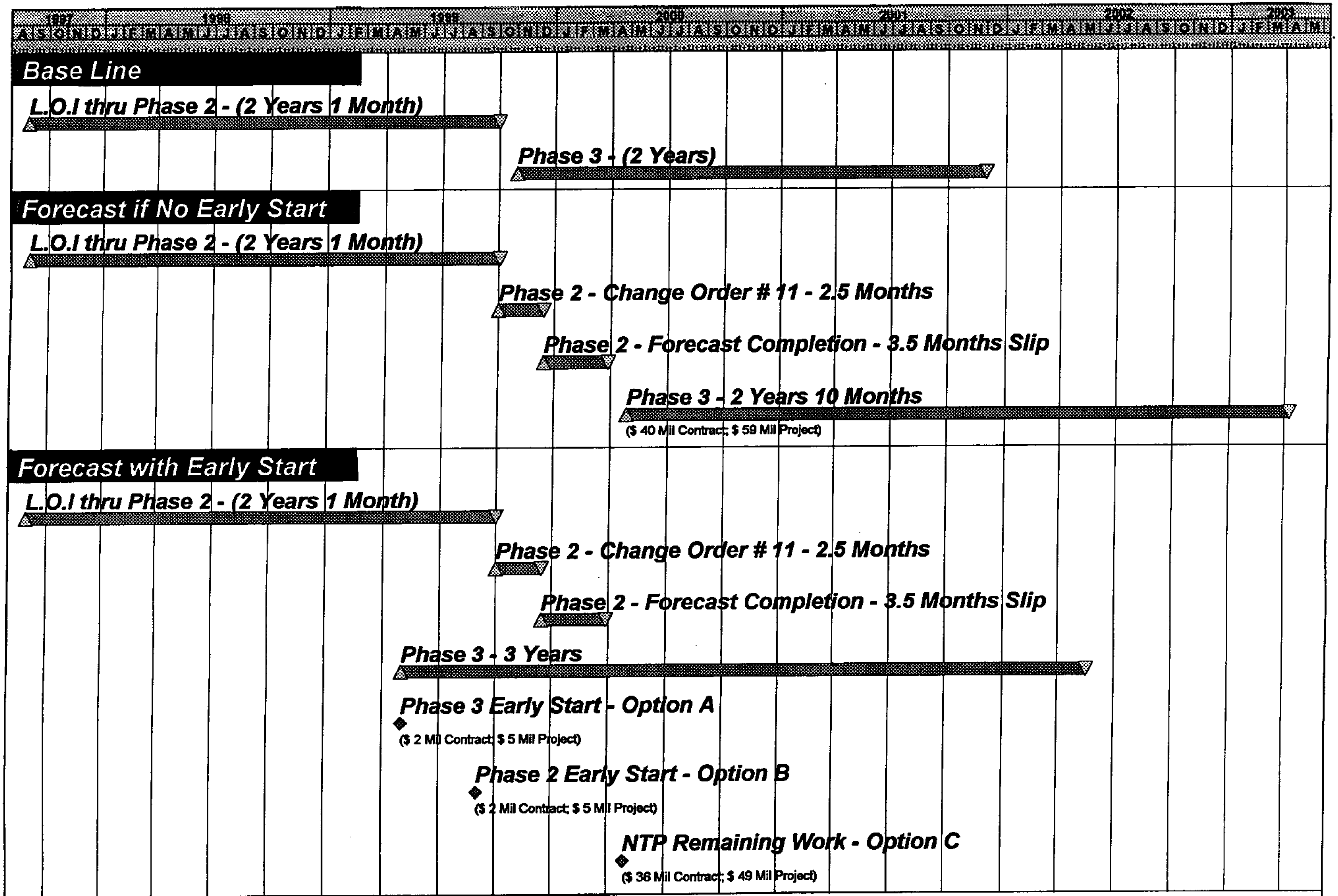
Unique Partnership (cont'd)

The Project Team

- Harmon and Subcontractors
    - Rail Safety Engineering, PC
    - Orthstar
    - Raytheon (formerly Hughes)
    - Design Engineers Group
- Others
    - Sverdrup/Systra (Formerly RTS)
    - Sandia National Lab
    - Lawrence Livermore National Lab
    - Battelle

Integration with Interlocking Replacement

- Unique Opportunity in Mid-98
  - Incorporate Interlocking control function into the AATC equipment, essentially at no extra cost
  - Replace existing relay-based I/L plant with microprocessors provided by Harmon for AATC
  - Accelerate I/L Replacement Project (20LH)
  - Simplify AATC cut-over process
  - Significant savings for District



Project Start	03MAR96
Project Finish	08APR03
Data Date	03MAR96
Run Date	04MAR99

Early Bar
Progress Bar
Critical Activity

ASUM

Sheet 1 of 1

AATC Project
Early Start of Phase 3
March 04, 1999

Project 49GB -- AATC Program
Budget Summary

		Costs ($M)	
PHASE 2			
	Early Phase 2	$	2.7
	Phase 2 Contract w/ Harmon	$	5.7
	BART Staff	$	3.5
	Consultants	$	2.6
	Other Costs	$	0.4
	Reserve	$	-
	Total	**$**	**14.9**
PHASE 3			
	Contract w/ Harmon	$	40.3
	Contingency on Harmon Contract	$	3.0
	Sales tax	$	2.2
	BART Staff	$	5.1
	Consultants	$	3.3
	Installation contract	$	2.5
	Reserve	$	2.8
	Total	**$**	**59.2**
TOTAL		**$**	**74.1**

OPERATIONAL IMPACTS OF AATC

Wayside Work

- Installation and Testing
  - Phase II
  - Phase III

- Installation and Testing Impact
  - Coordination with Revenue Service
  - Coordination with Maintenance
  - Coordination with other Projects

Overlay on Our Current System

- Transportation
- Maintenance and Engineering
- Rolling Stock and Shops

Training and Manuals

- Interdepartmental need in Operations
- Operations Training and Development to provide
- Marketing tool for AATC sales

SAN FRANCISCO BAY AREA RAPID TRANSIT DISTRICT

INTER-OFFICE COMMUNICATION

TO: Mike Healy
Media & Public Affairs

DATE: June 15, 1998

FROM: David Lehrer
Research & Development

SUBJECT: FYI -- Reference to BART activities on the world-wide web

Dear Mr. Healy:

Gene Nishinaga asked me to send you the following "heads up" about a positive reference to BART on the Internet.

In support of the AATC project, Sandia National Laboratories has been collaborating with BART staff in the development of a new safety-critical software testing methodology. The attached presentation outlines the methodology and its initial application at BART. This presentation will be available for viewing on the Internet world-wide web in July of this year via Sandia's "Albuquerque Software Processing Improvement Network" at http://www.abqspin.org/.

Take care,
David Lehrer
BART R&D
x4725

Testing for Software Safety in BART

presented by

Dwayne L. Knirk

Sandia National Laboratories
PO Box 5800, MS 0638
Albuquerque, NM 87185-0638
505.844.7183, dlknirk@sandia.gov

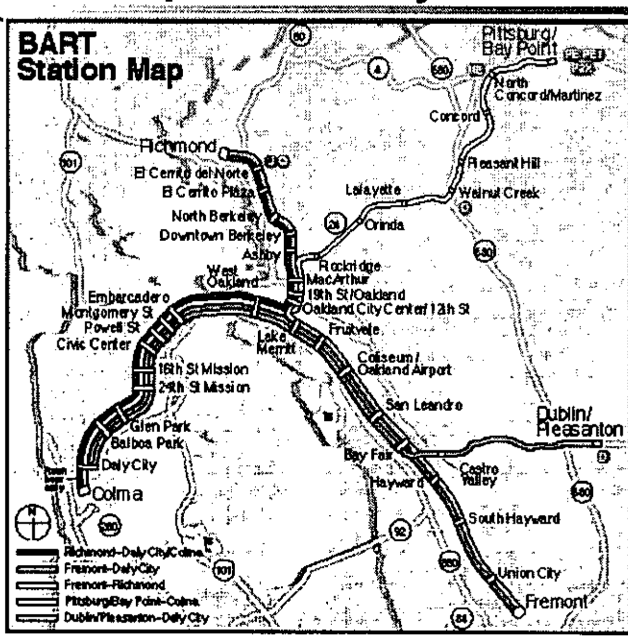
Topics

- Bay Area Rapid Transit System
- Advanced Automatic Train Control Project
- Sandia's Role
- BART's Software Problem
- Software Quality Engineering Approach
- Accomplishments

Web References

- **General Information**
  - http://www.bart.org/frames/public_affairs/system_facts.html
  - http://www.bart.org/frames/public_affairs/historical.html
  - http://www.webcom.com/petrich/transit/yard.html
- **BART Project**
  - http://www.tsd.org/49GB-110.html
  - http:///www.amcity.com/kansascity/stories/011397/focus2.html
- **Communication-Based Train Control**
  - http://www.harmonind.com/news/hughes.html
  - http://www.tsd.org/communic.htm
    Many reference links to projects, standards, suppliers, training, consultants, conferences, and technical documentation

Bay Area Rapid Transit System



Bay Area Rapid Transit System

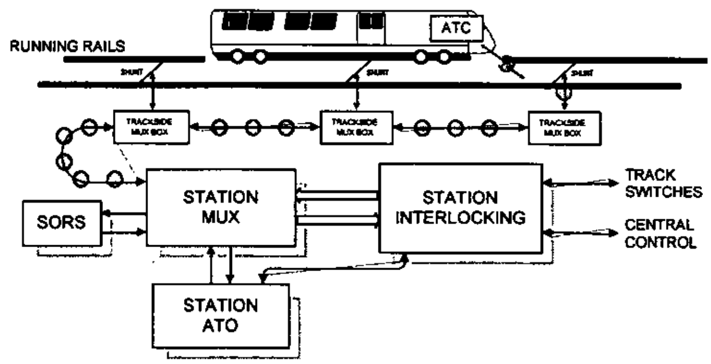
- **General Statistics**
  - 81-mile automated rapid transit system through the San Francisco bay area and inland, 37 stations along four lines of double track
  - 3¾ minute intervals on merged lines in Oakland,
    7 minute intervals on branch lines, 20 second stops
  - 250,000 passengers on an average weekday on 35-47 trains (4 a.m. to midnight)
  - 150 hp motor per axle, 4 axles per 70' car, third rail supplies 1000 volts DC
  - Regenerative braking supplemented by all-wheel hydraulic disk brakes

Advanced Automatic Train Control Project

- **Harmon Industries**
  - Project management
  - system design coordination, system integration
  - System test, reliability, maintainability, QA, CM programs
  - Station computer, interface hardware and software
- **Orthstar**
  - Non-vital station computer software, train interface controller
- **Rail Safety Engineering**
  - Vital station computer software, system safety assurance
- **Raytheon**
  - Radio system, network management services

Knirk: Testing for Software Safety in BART 28 May 1998

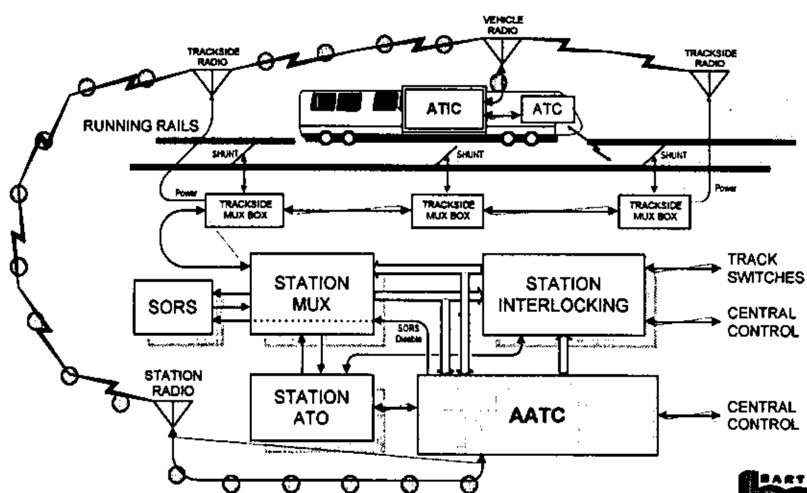
BART Automatic Train Control



Page 7

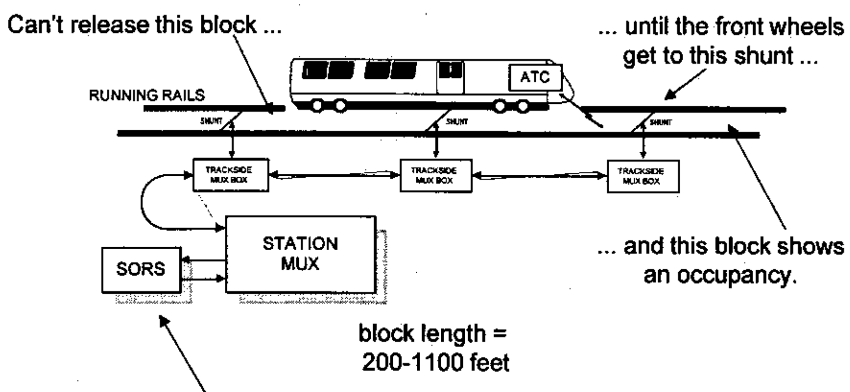
Knirk: Testing for Software Safety in BART 28 May 1998

BART Advanced Automatic Train Control



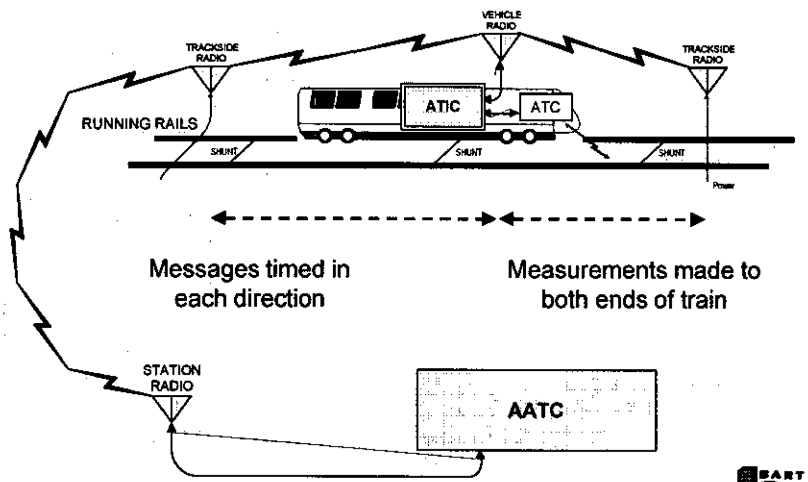
Page 8

BART ATC collision avoidance



Sequential Occupancy and Release System

BART AATC collision avoidance



Radio Ranging System

BART Advanced Automatic Train Control

- **Station Control Responsibilities**
  - Monitor train position
    wayside radio ranging good to 15 feet
    previously used track circuits good to 200-1000 feet
  - Command speed
    fully selectable
    previously limited to discrete set
  - Command brake rate
    fully selectable
    previously limited to on/off
  - Hand-off control to adjacent stations

BART Advanced Automatic Train Control

- **On-board Control Responsibilities**
  - Speed command decoding
    receive and verify speed commands
  - Over speed protection
    brake if train is above commanded speed, allow coasting
  - Braking
    maintain brake rate when in closed loop braking, or apply full service braking
  - Door operation
    open doors automatically on correct side and only when stopped in a station
  - Fail safe operation
    stop train upon detection of error

BART AATC Project Goals

- **Business Goal**
  - Increase throughput in the most congested lines
  - Improve energy usage efficiency (long term)
- **Operational Goals**
  - Top speeds of 80 mph, headways of 90 sec.
  - No less safe than current system
- **Deployment Goals**
  - Dual and mixed-mode operation with old system
  - Ultimately replace former system

BART AATC Safety Concerns

- **Assured Communication**
  - ½ second between train commands
  - No more than 2 seconds without command
- **Accurate Position Determination**
  - Use derived and computed
- **Appropriate Safety Envelope around Train**
  - Grades, train position and speed, rail surface condition
- **Fail-Safe: Stop Train and Yield Control**
  - 1 billion hours mean time between hazardous conditions
  - Specification calls for no software errors that could lead to unsafe condition

Sandia's Role

- **Cooperative Research And Development Agreement identified three areas of collaboration**
  - System safety planning
  - Independent technical review and analysis
  - ★ Software assurance
- **Initial focus on BART's algorithms and software**
  - Role has expanded because of trust and value added

BART Software Problem

- **Vehicle Automated Train Control System**
  - On-board control system, operator monitored
- **Situation**
  - Embedded in Intel 8086 microprocessor, 48K ROM, 8K RAM
  - No operating system
  - Software coded in assembly language, inherited 12 years ago
- **Objectives**
  - Safety: approval by California Public Utilities Commission
  - Reliability: on-time operation tied to revenue
- **First time BART has handled train software**

BART Software Problem

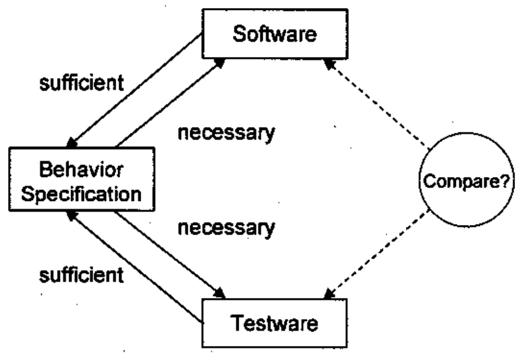
- **Working Materials**
  - 57 modules
    - 4 new
    - 24 modified
    - 9 safety-critical
  - Documentation is sketchy
  - Previous test results are voluminous but unenlightening
- **Their Initial Questions**
  - What kind of testing do we have to do?
  - How can we do it?

Sandia's Solution

- **Options**
  - Hired gun – do it for them
  - Scoutmaster – help them do it for themselves
- **Areas**
  - Software Specification
  - Software Testing
  - Software Configuration Management

Specification-Based Software Testing

❖ **Test for three-way agreement**



Specification-Based Software Testing

❖ **Software**

- Necessary all specified behaviors are realized by the code
- Sufficient all implemented behaviors are desired

Behavior Specification ⟷ Software

❖ **Testware**

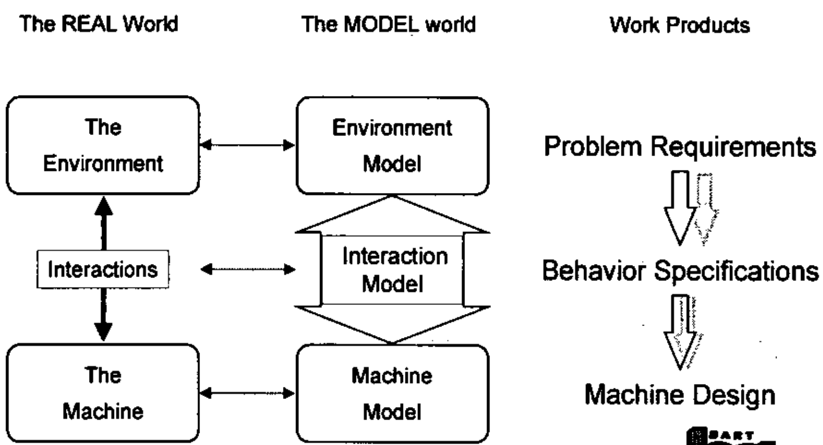
- Necessary all specified behaviors are demonstrated in tests
- Sufficient all demonstrated behaviors are desired

Behavior Specification ⟷ Testware

Specification-Based Software Testing

- **The SBUT Process ('sbutting', 'sbutters')**
  - Create behavior specification tables
  - Design test cases from behavior specification information
  - Execute tests on *instrumented* code
  - Examine test outcomes for behavior pass/fail
    missed services, missed state transitions, incorrect retained data updates
    wrong boundaries, violated constraints
  - Examine execution trace for structure coverage omissions
    missed segments, missed branches, missed branch sequences
    missed units, missed call-return pairs, missed data paths (def-use)
  - Quit when all behaviors pass and all structures are executed
  - Otherwise, fix specification, code, or test cases and iterate

Requirements, Specifications, Designs



Requirements, Specifications, Designs

- **Subject of Problem Requirements**
  - Given environment
  - Required effects
- **Subject of Behavior Specification**
  - Environment interactions
  - Observable behaviors
- **Subject of Machine Design**
  - Architectures, code and data structures, algorithms
  - Computer operations

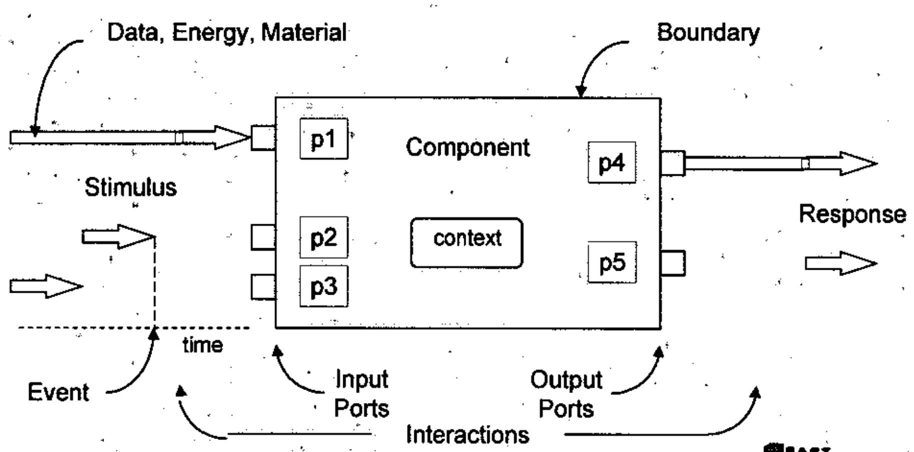
Problem Requirements

- **Vocabulary**
  - Things in the environment
  - Relationships between things in the environment
  - Events that change things or relationships
- **Contents**
  - What is given in the environment
  - What is to be achieved in the environment
- **Source**
  - Application domain expertise

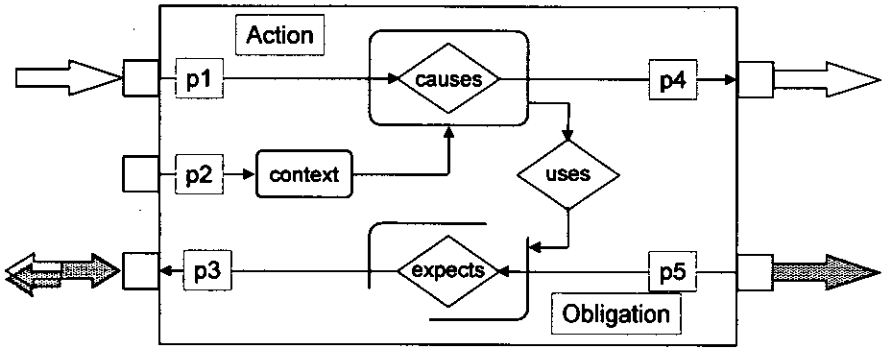
Behavior Specifications

- **Vocabulary**
  - Interactions with the environment
  - Relationships between interaction occurrences and contents
- **Contents**
  - Specification of interactions
  - Specification of behaviors
- **Source**
  - Problem Requirements

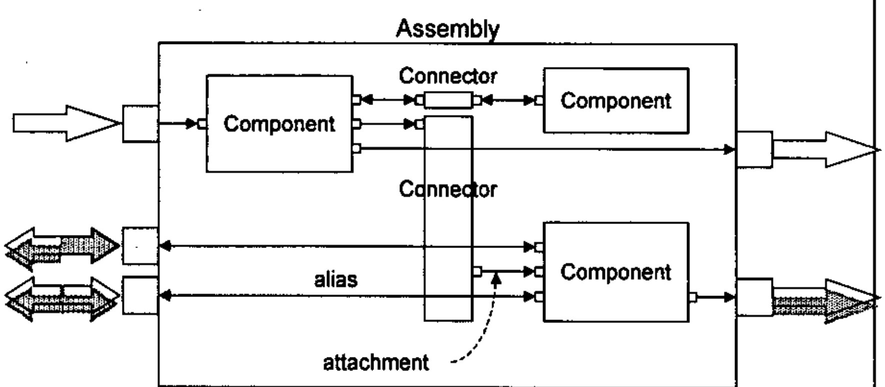
General BS Model - Interfaces



General BS Model - Behaviors



General BS Model - Assemblies



Specification-Based Test Design

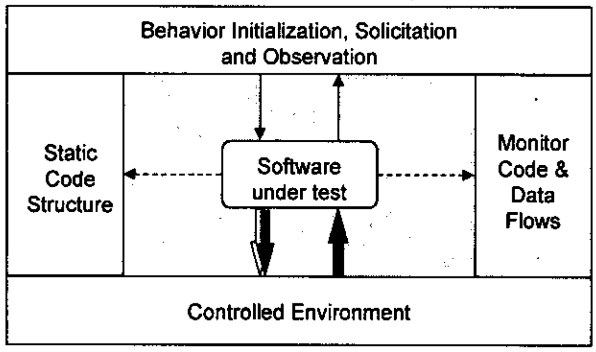
- **Software Description File**
  - Behavior specification (ASCII file)
  - Standard templates for
    components, connectors
    interactions, data, events
    states, actions, obligations
  - Representative data samples
    added clauses in data statements
- **Test Design File**
  - Meaningful combinations
    standard sets
    special cases

Testware

- **Test Execution Inputs**
  - Test case server offering combinations of data samples
- **Test Harness**
  - Modified **gdb** (GNU debugger)
- **Test Execution Outputs**
  - Control flow during execution
  - Data flow during execution
- **Expected Outputs**
  - Original code – regression
  - Alternate implementation in C – new functions, regression check

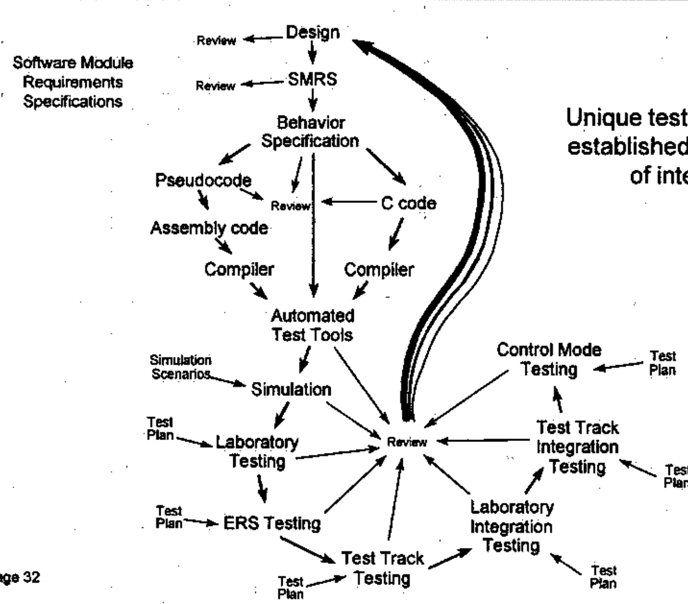
Software Unit Testing

- ❖ **Controlled environment**



- ❖ **Instrumented CPU**
  - instruction pointer (sequences, jumps)
  - memory references (reads, writes)

BART's Integrated Testing Approach



Unique testing objectives established at each level of integration

Accomplishments

- **Demonstrated SBUT Method**
  - Representative module from current system selected
  - Developed specification, test cases - found unknown fault
- **Developed Standard Templates for Specification**
  - Concurrent work for IEEE Std 1175
- **Held Workshop on Vehicle ATC Modeling**
  - Control system architecture, standard component forms
  - Standard templates for test design and execution
- **Developed Automated Process for Unit Testing**
  - Defined activities and work products
  - Identified software tools to support process

Software Process Improvement?

- **Accomplishing Change**
  - Listen to **their** problem
  - Identify **mutual** objectives
  - Construct a **reasoned** approach (keep asking questions)
  - Demonstrate – **do** an example
  - Deal with **details**
  - Automate **sparingly**
  - Build consensus to **realistic** benefits (manage expectations)
- **Change from Outside**
  - Keep **their** best interest at the fore
  - Be **credible**, trustworthy, helpful, clean, kind, humble, . . .
  - Be **competent** to do – but only guide them to their solution

Finis