Bigger bugs in BART?

Six months in partial service have raised questions about BART's automation and its safety features

Gordon D. Friedlander Senior Staff Writer

When we prepared the three-part series* on the Bay Area Rapid Transit System (BART), the system had not yet been opened for limited revenue service from Oakland to Fremont. Thus, before the inaugural day, September 11, 1972, we could only report on what the sophisticated and complex automatic train-control (ATC) system, and other equipment and components, were *supposed* to do. It was only after a backlog of operating experience that we and the general public discovered what some of the actual capabilities—and deficiencies—were.

In all candor, however, we did receive a forewarning (following the publication of Part I) from Holger Hjorstvang, a former systems engineer with BART, that all was not well with the ATC. His letter, and a rebuttal to it from W. A. Bugge of Parsons Brinckerhoff–Tudor–Bechtel (PBTB), the prime contractors and consultants to BARTD, were published on pp. 16–17 of the December 1972 issue of *IEEE Spectrum*.

Last stop: a sandpile

On October 2 of last year, a southbound BART train operating under the computer-controlled ATC overshot the Fremont terminal and plunged the lead car onto a sand embankment. The train's "attendant" (BARTD's term for train operator, or its "sometime" motorman) barely managed to override the ATC manually before impact. In those final desperate seconds he may have realized that no *deus ex machina* would come to his aid and that all remaining divinity lay within himself. Fortunately, there were no fatalities or even serious injuries as the result of this incident. Although most of the passengers were just "shook up," the repercussions of that accident are a continuing subject of rather heated debate . . . .

At the time, David G. Hammond, BART's assistant general manager and chief engineer, told us that the cause of the accident was

". . . A malfunction of a crystal oscillator on board the lead car . . . This oscillator controlled the commands for a 27 mi/h [43.5 km/h] speed which was the [speed] zone in which the train was approaching the Fremont Station. Examination and detailed tests showed that there was an intermittent short in this crystal oscillator due to its mounting within its case which caused the oscillator to give an incorrect speed signal. Various tests showed that this ranged between 40 and 70 mi/h [64 to 113 km/h] instead of the correct speed of 27 mi/h . . . It was further verified by X-ray examination, which showed that an intermittent short was possible because the crystal was not in the proper location within its case . . . ."

The gist of this explanation was carried in "Spectral Lines," in the November 1972 issue of *Spectrum*. (We shall pursue Hammond's reply later in this piece.)

*See *IEEE Spectrum's* September, October, and November 1972 issues.

The incident of October 2, 1972. Lead car of BART train overshot the terminal station at Fremont and came to rest on a sand embankment following a failure in the ATC system. (Photo courtesy Lonnie Wilson, *Oakland Tribune*.)

The state hearings and report documents

According to a memorandum to "Bechtel Senior Management" from the San Francisco office of Bechtel Incorporated (one of the principals in the PBTB joint venture), dated November 27, 1972, events leading up to the State of California Senate Public Utility and Corporations Committee hearings—convened during that month—had their origins in 1971 (or earlier), when several BARTD engineering employees were dismissed after publicly objecting to certain BART policies. Subsequently, the Walnut Creek Chapter of the California Society of Professional Engineers backed this dissident group, drew up a bill of particulars, and submitted it to State Senator John Nejedly. Nejedly convened the 16 legislative representatives of BARTD and requested an investigation of BART's operations by the state's legislative analyst, Alan Post.

The Post report. Post's report, released on November 9, consists of 106 pages of comments (leading to 31 recommendations), which, in essence, alleged that BART was unsafe as it was being operated as of that date. The two principal stipulations of the report were that

- PBTB and BARTD allowed BART's service to begin last September without adequate checks and with train-control deficiencies that jeopardize public safety.
- PBTB overcharged BART for the system engineering and construction-management services rendered.

According to Post, every statement in his report is based on information from BART, PBTB, and Westinghouse sources—plus opinions of outside technical consultants. His report emphasizes that the ATC is the key to passenger safety. In this context, the document stresses that BART selected an untested Westinghouse system on the basis that the company presented the lowest bid and because it offered the most advanced circuitry as a spinoff of the missile industry. Further, the report alleges that, prior to the award of the $26 million contract (additional costs have raised the total bill to about $35 million), the California Public Utilities Commission (PUC) informed BART that previous experience of ATC bidders should be taken into account before the award of contracts. Nevertheless, it is contended in the Post report that BARTD accepted the proposal of the lowest bidder without requiring prior demonstration of the system before giving the go-ahead for final design and installation.

Post's investigative team also delved into the Fremont Station incident, and recommended that, because the crystal oscillators may transmit erroneous commands, the speed-control element should be redesigned. The report states in this context: "Contrary to the public position of BART and PBTB, all evidence available to us indicates that the speed-control circuits on all transit cars . . . do not possess required fail-safe features and have not been adequately qualified for reasonable assurance of passenger safety."

The report explains why the present system is unsafe:

Signals are transmitted through a low-power circuit in the tracks. But when there is rust or dirt on the track, the presence of a train may not be detected. When this occurs, protection circuits do not take the necessary action to slow other trains and thereby avoid a collision. (In a later section, we will discuss the remedial measures taken by BART to eliminate this defect.)

The report also warns that the present system involving the use of personnel relaying information by telephone is not foolproof and claims that, on two occasions, communications errors have placed two trains within the same block.

This method was called "only slightly more sophis-

I. Subsystems identified in the Battelle analyses of the BART system in which an oscillatory condition of a circuit may result in an unsafe condition

Report Page Number	System	Circuit	Drawing Number	Remarks
54	Train protection	Bit-by-bit comparator	209P188	Can the latch circuits oscillate?
63	"	Occupancy driver	209P583	Can the occupancy driver oscillate?
72	"	Vital-relay driver	209P282	Can the relay driver oscillate?
73	"	Gate-violation detector	209P584	Can this circuit of fail-safe AND, OR, and TRANSFER gates oscillate?
187	Vehicle	P-signal generator and power amplifier	209P493 and 203P528	Can the p-signal generator, or the power amplifier, or the combination of the two, oscillate?
198	"	Power/brake-relay driver	2698A98 Sh. 61	Can the power/brake-relay driver oscillate?
199	"	P-signal decoder	203P523	Can the power amplifier that produces the FAC and FSR signals oscillate?
219	"	Relay circuit board	39-9315G (Hurst-Airheart)	Can the relay driver oscillate?

ticated than having a man with a red flag walk in front of each train" by *Newsweek*'s William J. Cook.*

Unfortunately, spatial constraints do not permit a summary of the Post report's 31 recommendations; however, some of the salient observations were that

- BART is unsafe as it is presently operating and that the remaining sections of the mass-transit line—including service through the Transbay tube to San Francisco (scheduled for September)—should be delayed until all the bugs in the ATC system are swatted.†
- Emergency restraining structures plus track extensions be built at the terminal ends of each line in the network.
- The Public Utilities Commission should augment its staff so that it can do an efficient job of monitoring the train-control system.
- Modifications be made in the ATC system to ensure that all trains will center and stop at station platforms without manual override by the on-board attendant.

The Battelle Institute report. During its extensive research, Alan Post's staff of legislative analysts and engineers apparently discovered the text of a two-volume study prepared for BART by the prestigious Battelle Memorial Institute in 1971. The summary of that report is contained in the box on the facing page; also see Table I.

Reactions to the Post report

Parsons Brinckerhoff-Tudor-Bechtel. In response to the question dealing with train control, PBTB contends it provided the *performance* specifications for BART's ATC system. Westinghouse, as the successful bidder for supplying the system, is *obligated* to meet these specifications. As of last December, Westinghouse met the required *safety* tests for extending revenue operations to the Hayward–MacArthur Line, but had not met all the reliability tests.‡

With respect to the Post report's criticism of fee overcharges, PBTB states that Post took the position that PBTB accepted a contract for design and management of construction of the Transbay tube on a basis of 6 percent of construction cost. Thus he reasoned that PBTB should have been able to do the same thing for the overall BART project. PBTB claims, however, that a 13 percent fee is normal, is in accordance with the ASCE manual, and compares favorably with other public projects "of similar magnitude and complexity."

BARTD. The Bay Area Rapid Transit District (BARTD) avers that, since the initiation of service last September, 28 million passenger miles have been run in the "automatic mode, with the manual block system used as backup for train separation." On occasion, manual operation of trains through certain stretches has been used where, for instance, a false track occupancy was indicated but, in actuality, there was no train; manual operation has also been used when a train lost automatic speed codes. According to BARTD, these malfunctions continue to decrease in number so that present operations are in the fully automatic mode more than 95 percent of the time.

Further, the presently scheduled 10-minute train headways have generally provided *full automatic operation,* even with the manual block system, since the block ahead is usually clear. This permits the train to enter and leave the station automatically. Also, the wayside automatic train operation (ATO) is steadily improving, with "false train occupancies" and other malfunctions decreasing to the point of infrequent occurrence. Automatically programmed stop

*In August 1972, before partial system revenue service was inaugurated, the PUC required BART to adopt a "manual block system"—which means that a train cannot leave one station until assured by a telephone call that there is no train between that station and the next station. What actually happens is that BART supervisors telephone ahead to make sure there are no trains for *two stations down the track.* If there are none, the train proceeds to the next station where the telephone clearance procedure is repeated!

† In fact, the report described BART's promised completion date for total system operation as "unrealistically optimistic."

‡ Revenue service was started, from Oakland to Fremont, on September 11, under the provisional approval by the PUC of manual block control. PBTB has yet to approve the system for operation of converging trains on the Concord and San Francisco lines.

Summary of the Battelle Institute report

Scope. *The work conducted in this study consisted of a limited safety analysis of the operation of the automatic train-protection system and the vehicle system portions of the BART ATC system . . .*

The analyses were conducted with the aid of a methodology and safety criteria . . . to reduce the complexity of the required safety analysis. Analyses were limited to considerations of the effect on safety of single component failures . . .

In preliminary analyses of the systems, particular subsystems were identified that are vitally involved in safe operation of the system while other subsystems were identified that are not involved with safety in any way. Those subsystems involved with safety were analyzed further in greater detail under both normal and malfunction operating conditions to determine if any condition could be identified that would result in a condition that would be either unsafe or potentially unsafe. In those cases . . . an estimate was made of the failure rate of those components identified in the analyses whose failure might result in an unsafe condition . . . .

Results. *Under the condition of all subsystems operating normally with no malfunctions, no conditions were found in the analyses of either the train-protection system or the vehicle system that would result in unsafe operation.*

Under the malfunctions considered in the analyses, no clearly defined unsafe conditions resulting from those malfunctions were found. Several circuit conditions were observed, however, in both systems such that, if any one of them should occur, a potentially unsafe operating condition may result . . . .

It appears from the analyses that precautions have been taken in the design of the circuits of the system to provide a high degree of immunity against the occurrence of the potentially unsafe conditions observed. However, documentation as to the degree of immunity actually provided was not available. A list of the subsystems in which the potentially unsafe conditions have been identified appears in the section of the report titled "Questions for Further Investigation" **(see Table I, p. 34).**

Although fail-safe circuitry is used in some subsystems of the vehicle system, redundant circuits play a large role in performing safety functions. Analyses of these redundant circuits indicate that they perform their intended function in a safe manner if only a single malfunction at a given time is considered. However, multiple malfunctions were identified that, should they occur simultaneously, a potentially unsafe condition may result . . . .

Conclusions. *The conclusions that can be drawn as the result of the limited safety analysis of the BART ATC system are*

1. Under normal conditions, the system appears to operate in a manner that is not unsafe.

2. Under conditions of single malfunctions (not multiple) no clearly defined unsafe operating condition was identified. However, circuit conditions were identified that, should they occur, a potentially unsafe condition may result.

3. The operating safety of the vehicle system depends upon redundant rather than fail-safe circuits. Simultaneous multiple failures in these circuits can result in unsafe operating conditions.

Recommendations. *As a result of the . . . analysis on the BART ATC system it is recommended that:*

- *Further investigation be made concerning the immunity of the subsystem circuits to the potentially unsafe conditions identified in the analyses and listed under* "Questions for Further Investigation."
- *A more detailed safety analysis be made of the vehicle system, with more emphasis on the propulsion–braking portion of the system than was possible in this limited analysis.*

Comments of a BART director

Daniel C. Helix, mayor of Concord, Calif., has been a BARTD director since November 1971. The following are excerpts from his remarks at the Contra Costa Mayors' Conference on January 4:

. . . There are many things of a positive nature that might be said about BARTD. First and foremost is that BARTD will be meeting the need for a viable operating mass transportation system and I will continue to be supportive of the concept and what it will mean for the Bay Area. However, during this past year a number of things have occurred which have not engendered a feeling of confidence toward top management on the BARTD staff . . .

. . . In December 1971, there was collision wherein a moving test train hit a stationary train. At a board meeting, the directors were presented with the final report of the Board of Inquiry convened and dismissed by the BARTD general manager. Some of us . . . had additional questions which had not been presented to the Board of Inquiry and related directly to the possibility of a breakdown of the ATC. The board of directors advised the general manager to reconvene the Board of Inquiry . . . To my knowledge, the Board of Inquiry was never reconvened . . .

Also in December 1971, the chief engineer of BARTD was asked specifically whether or not there were any serious problems with the ATC. He responded that there were a few "bugs" . . . but that there were no serious problems. This statement was made after the September 1971 Battelle Institute Report which pointed out the train-detection problem . . .

In January [1972], three BARTD engineers approached me and other directors expressing concern about the reliability of the ATC system and the need to involve lower-echelon staff engineers in the testing phase. They retained an engineering firm which prepared a summary of the ATO problems. The report was rejected out of hand and no action was taken; yet, today, in rereading the report, we find many of the concerns expressed by the Battelle Institute, and many of the predictions supported by actual occurrences. The three engineers were summarily fired . . .

Currently, the PUC has authorized revenue service on the A–N [East Bay] line in a modified manual-automatic mode. We are still experiencing technical problems . . . but it seems to me that the number of problems is excessive (100 deficiencies noted in a two-day period) . . .

Finally, a very large question about the safety of the system is thus far unanswered and that relates to the need for an independent backup system, either manual or automatic, which would provide for protection in emergency situations. Electrical experts are studying this problem and I will accept their judgment as to whether a backup system is necessary . . . .

failures (trains running through a station) have been virtually eliminated—partly due to additional training and experience of on-board attendants relying on automatic operation.

Finally, the performance of the vehicles—including the on-board ATO equipment—is also improving; this provides greater availability of vehicles for revenue service and fewer occasions on which cars are removed from passenger-carrying operations. Investigations of the various ways in which to provide train detection for completely "dead" cars (this is the only train-detection problem existing) have been made. BARTD believes a solution has been found by using conventional "wheel scrubbers"—or shunt shoes—to remove foreign particles from the wheels. A description of this technique is presented on p. 37.

Westinghouse. At a press conference last December, Dr. Woodrow E. Johnson, vice president and general manager of Westinghouse Electric's Transportation Division, defended his company's position in no uncertain terms. Here are some excerpts from his statements:

"... First, I think we have accomplished the single most important objective: we have provided a train-control system as safe or safer than any other designed and operating anywhere in the country. We believe the concept of our system was the best that BART could have chosen [and] I think we have made that concept a reality.

"So why is there so much controversy over the system and its safety? One [reason] is an honest difference of opinion among technical people. We don't say that the system BART selected is the only one it might have chosen. We do think it is the best of several possible systems ... The other reason for the controversy is simply a matter of slipshod reporting by those who prepared the Post report. I'm sure you know that the best way to get facts is to go to the best possible source—Westinghouse—[if] you are going to write a report on the BART train-control system.

"I don't say that Westinghouse is the *only* source of information, but certainly ... the company building and installing the system was one of the logical places to go for information ....

"... The most important single matter is ... how to meet the PUC requirement concerning train detection ... As far as we have been able to determine, no other state has felt that this requirement was necessary to operate to a safe mass transit system.

"When the requirement was imposed, BART had no choice but to adopt the manual block procedure—having an attendant at every other station checking ahead to see that the track was clear ... In three months of operation, there has not been a single report and instance of a train not being detected.

"I'm not sure that it is clearly understood... that BART trains are operating every day under full automatic control. Occasionally a train is held manually at a station and then returned to automatic control ...I hope we all understand that manual block procedures do not replace automatic controls."

The PUC hearings

Last November 27, PUC conducted a two-day field inspection of BART train operations during which more than 100 instances of failure of equipment to function properly were noted. The most frequent defect in the rolling stock was that trains, running under ATC, attempted to run through stations and the attendants had to press "stop" buttons to halt them. Also, other trains would accelerate unexpectedly and then, for no apparent reason, decelerate. Occasionally, a train would travel at only half speed; and there was sporadic difficulty with doors that would not open or close. These incidents, and numerous minor operational flaws, led PUC Commissioner J. P. Vukasin to state for the record: "As long as there is one scintilla of evidence that raises a doubt of the safety of the passengers ... it must be reconciled."

On the matter of faulty crystals. Wayne Keithley, an engineer-analyst in Alan Post's office, testified on the Fremont accident of October 2. He alleged that BART engineers were using "nonvalid" data in calculating the speed of the runaway train at 26 mi/h (42 km/h) when it struck the sand barrier. In his testimony, Keithley also commented on BART's "faulty crystal" oscillator explanation. Crystals, said Keithley, are subject to many environmental influences, such as air pressure, temperature, vibration, shock, and the way in which they are mounted.

Holger Hjorstvang testified that, as an electrical engineer, he considers BART's ATC system to be unnecessarily complex. He regarded the crystal malfunction explanation, however, as an "incredible coincidence" that might never occur again. Nevertheless, he felt that the complexity of the system made it much more probable that other failures will take place. BART, he contended, would have been wiser if it had adopted the less complicated train-control systens used on other transit lines.

Wheel scrubber may solve train-detection problem

BART's train-detection scheme* requires the shunting of a low-voltage signal from one rail, through a car's wheels, to another rail so that a following train will receive a signal not to approach the train ahead at less than safe-braking distance. As we have previously noted, corrosion or dirt on the wheels has insulated the wheels from the rails and, thus, has prevented the shunting action necessary for train detection. But in mid-December BART fitted off-the-shelf cast-iron mechanical wheel scrubbers† to a BART vehicle and tested them on a section of track not yet in revenue service. The scrubbers have apparently scraped off the electrically insulating dirt film from the wheel surfaces successfully enough to permit the signals to be shunted adequately.

Westinghouse's Woodrow Johnson believes that the scrubbers offer the best solution to the "dead" train detection problem.

Spiking the switches

BARTD has verified the report carried in the news media that 29 of the 49 switches on the Oakland–Fremont line have been spiked shut because BARTD discovered the switches sometimes derail the vehicles by unexpectedly opening while trains are passing over. Because of the spiking, all of the sidings along the line have been blocked off, thereby making it inconvenient to use a siding when necessary.

Blue ribbon panel reports

On December 19, 1972, a special three-man panel appointed by the California State Senate Public Utilities and Corporations Committee began its study of the alleged deficiencies in the BART system. The panel members were: William Brobeck, a Berkeley mechanical engineer; Bernard M. Oliver, vice president of R&D for Hewlett-Packard Co., Palo Alto; and Clarence A. Lovell, a Fairfax, Va., consultant who has designed a number of electronic systems.

The panel concluded its study on January 31, and as this issue of *Spectrum* goes to press, we are in receipt of the panel's final report.‡ Among its salient findings are that the present restricted mode of operation of BART is reasonably safe and represents a suitable interim measure. However, (1) the present design of the BART Automatic Train Control system will not provide adequate passenger safety under full-scale operation; and (2) modifications can be made and back-up added to the present design that will provide adequate passenger safety under all service conditions. The modifications fall into the following classes: (a) modifications needed to make the ATC system adequately safe for full-scale automatic operation; (b) additional safety features needed to make the system adequately safe under full-scale operation in the manual and mixed manual-automatic modes of operation; and (c) further modifications of and additions to the system that, combined with the present hardware, will permit a new standard of safety to be achieved in public transportation.

Recommendations for such modifications related to each of the aforementioned categories were given in the report. We shall examine these in detail in the April issue of *Spectrum*.

Fail-safe concepts with reference to the BART ATC system

The following excerpts are from a paper by Dr. Willard H. Wattenburg, an electronics expert who testified at the PUC hearings:

During the last 15 years we have learned from ... experience that even the most complex electronic control systems—including computers—have unpredictable failure characteristics which force the use of independent fail-safe systems whenever human lives are safeguarded by the electronic system in the primary mode. Furthermore, there is no such system routinely operated which does not utilize [human personnel] *as the final backup in cases where all levels of electronic or automatic control fail or disagree ...*

The electronic-control systems are utilized to constrain man's error-making capability. They are not designed to eliminate his essential error-correcting capability ...

The concept used in the BART train-control system design falls short of satisfying ... these conditions ...

BART management and engineering staff has declared publicly that their intent was to completely automate train control and eliminate the man from the loop ... to prevent human error ...

I believe they have overlooked numerous opportunities for independent fail-safe checks on train operation in the automatic mode, unnecessarily eliminated essential information required by the human operator, and placed a degree of confidence in the electronics they are using which far surpasses the degree of reliability which would be placed in this circuitry by men who have had extensive experience with this technology under actual operating conditions. Furthermore, they have not performed the degree of testing prior to design or prior to operation which would be considered essential before any system such as this would be man rated.

The failure analysis ... to date has been rudimentary ... It has not taken into account the great majority of failures which occur due to external influences and multiple errors ...

... The local station and train-borne electronics now in place comprise a single system. The fail-safe circuitry and logic in the local station control equipment and the train-borne electronics amount to no more than reasonable "error checking" ...But, who in his right mind would stake his life on the operation of a single computer over a long period of time ...?

The present train-detection communications link is both frail and open loop. [This] *has been utilized in the past with some success because high-power, reliable track circuits and components have been used ...*

The train-detection communications loop must be closed and fail-safed. This requires active communication and signaling by the trains as well as a substantial improvement in the signal-to-noise characteristics of the present low-power track circuits.

Under full-schedule operation, intermittent failure of the track circuits and speed-command communications can become dangerous ... even though error-detecting circuits always bring trains to a stop whenever anomalous conditions occur. Frequent stopping of trains on a high-speed, high-traffic system begs conditions which can lead to disaster.

I claim that the reliability of the low-power signaling system now being used will create a frequency of anomalous events a thousand times greater over the long term than would be the case with high-power track-detection circuits ....

[The initial BART staff reaction to the Post report was to challenge the competence of Post's engineers who prepared the critical report. Post then produced Wattenburg as an expert witness before the state senate hearings. Wattenburg corroborated the Post findings on the ATC system and referred to them as "minimal and conservative." He then proceeded to explain to the senators how the open-loop system was designed to operate, concluding that the "previous statements made by BART witnesses would indicate that none of them have direct, personal knowledge of what they say."

Asked for comment on the BART and Westinghouse technical responses to the senate committee's questions, Wattenburg suggested that "technical pablum" would be an appropriate description.

In another development, David Hammond, BARTD's assistant general manager, submitted his resignation late in January, effective March 1.]

***Train detection by means of track shunting** is the most critical parameter in a train-control system design. **The** first careful measurements **of BART's low-voltage shunting were made** only *after* the system was built.

†It should be emphasized that the original design and purpose of the ATC system was to eliminate "old-style" mechanical and electromechanical devices.

‡Meanwhile, on January 29—despite a number of unresolved operational problems—BART opened revenue service between Oakland and Richmond, to complete the full-route length along the eastern margin of San Francisco Bay.