

Failure Modes and Effects Analysis and Minimum Headway in PRT

J. Edward Anderson, PhD, P. E.

To achieve safe and reliable operation at small headways in an optimized PRT system, it is necessary to perform careful failure modes and effects analysis and to follow the recommendations thereby discovered. A major recommendation is that the on-board and wayside computers be dual redundant. In this paper, possible failure modes are analyzed, the mean times between major failures including collisions are estimated, and a series of recommended design features is given. An important conclusion is that, by use of the features recommended, the distance traveled in PRT between incidents that may lead to collisions will be about 10 trillion times longer than in the U. S. automobile system.

Contents

	Page
1. Introduction	2
2. Externally Induced Failures	4
2.1 Power Failure	4
2.2 Truck Hitting Post	5
2.3 Tree Falling Across Guideway	5
2.4 Lightning Stroke	5
2.5 High Wind	5
2.6 Earthquake	5
2.7 Vandalism or Sabotage	5
3. Minimum Safe Headway	6
4. The Requirement of Low Maximum Failure Deceleration	7
5. Mean Time Between Vehicle Failures	8
5.1 Computer Failure	8
5.2 Communications Failure	9
5.3 Encoder Failure	10
5.4 Propulsion-System Failure	10
5.5 Other Vehicle-Borne Components	10
5.5.1 Switch Actuator	11
5.5.2 Auxiliary Brake	11
5.5.3 Power Pickups	11
5.5.4 Push-Mode Actuator	12
5.5.5 Door Actuator	12
5.5.6 Hydraulic Bumper	12
5.5.7 Wheels	13
5.5.8 Air Conditioning, Ventilation, and Heater	13
5.6 MTBF for Vehicle Failures	13
6. Mean Time Between Zone Controller Failures	14
7. Mean Time Between Vehicle-to-Vehicle Collisions	14
8. Potential for Sudden Stops	15
9. Diverge-Junction Collision	16
10. Merge Collision Between Two Vehicles	19
11. Run-Away Vehicle Entering Station and Crashing into Stopped Vehicle	21
12. Summary of Design Features Required for Minimum Safe Headway	22
13. Conclusions	23
14. References	23
A. Truck Hitting Guideway Support Post	24
B. Tree Falling Across Guideway and Stopping a Vehicle Instantly	25

1. Introduction

Notwithstanding great expenditures of public money, urban transportation continues to frustrate planners and citizens everywhere. Wider roads, wherever they are politically possible, quickly fill up; and, even at enormous expense, conventional rail systems do not attract enough riders to make much difference. Even the introduction of new automated transit systems using large vehicles and conventional service concepts, as they do now, are not much better – the mere substitution of automatic control for drivers is not enough. New ideas have been needed, and to find them has required the investigator to step back and examine the urban transportation problem as a *field* of requirements and characteristics *without prejudice*. After several decades of intuitively based research and development by many investigators, Anderson [1984] found that it is possible to start with a system-significant equation for the cost per passenger-mile of any means of urban mobility and from it discover a set of characteristics that minimize cost per passenger-mile subject to requirements on safety, reliability, and environmental protection.

Why is minimization of cost per passenger-mile so important? Because attempts to minimize cost per passenger-mile leads to discovery of system characteristics that both minimize system cost and maximize ridership. Because no urban service can, in the long run, require costs in excess of benefits. Because minimization of costs while maximizing ridership leads to minimization of the land, material and energy required for adequate mobility. Because the search for sustainability requires optimization.

It may not be surprising that the above-described process leads to a set of system characteristics that differ markedly from existing mobility modes. Adequate safety and reliability at average speeds that will attract riders requires an exclusive guideway away from the street system, but minimum guideway cost requires minimum loading, which requires that people ride in the smallest practically sized vehicles, which permits people to ride alone or with their own traveling companions at times of individual choice regardless of any imposed schedules. Adequate throughput at the highest practical average speed requires nonstop trips, which requires that the stations be placed on bypass guideways, and safe minimum headway between vehicles lower than the headways between automobiles operating manually on freeway lanes. But, by placing stations on bypass guideways (off-line stations) the vehicles wait for people rather than requiring people waiting for vehicles. Thus trip time is both minimum and predictable. Moreover, adding off-line stations does not reduce the average speed, so many more stations can be used, which increases accessibility, which increases ridership. By providing reliable in-vehicle switching, vehicles can travel from line to line, thus avoiding transfers, which are a major deterrent to ridership. With fully automated vehicles the operating costs are minimum and safety is maximum. With minimized guideway cost, an extensive network of guideways becomes practical, which conforms to the fact that cities cover areas – travel “corridors” only separate areas. They are not the places where people live, work, and play.

It is not surprising that the system that results from the above-described optimization process is different from all existing modes. It differs from the automobile-highway system markedly in land required, safety, noise, air pollution, and congestion avoidance. It differs from bus and rail systems in the markedly improved level of convenience, security, and timesavings provided for the rider. It differs markedly from large-vehicle automated systems now called “People Movers” in customer convenience, system cost, and control sophistication. It differs in the lack of institu-

tional constituencies that support it. In the latter sense the new, optimized mobility mode is a *disruptive technology* – it will require rearrangement and possibly disruption of institutions and likely some discomfort for some of the people that work in them. But the new mobility mode is sorely needed.

What to call it? Calling it a mode of “transit” conjures up visions of conventional transit modes that must be heavily subsidized because so few people use them. Calling it a form of automated highway brings in the vision of problems of transition to them that may never be solved. Calling it a type of taxi – an automated taxi – may be closer, but even here the image of “taxi” is a vehicle that one must wait for and that gets bogged down in traffic. The new mode has been called generically “personal rapid transit,” but that term has been corrupted by many visions of what it is not, and brings with it the baggage of classification with larger transit vehicles, which are subject to standards that no longer apply. The optimized mobility mode is now new, but is so superior to existing modes that once the institutional problems are solved it will no longer be new. The ultimate, achievable with the optimized mode of mobility, is that moving from place to place in a city will no longer be a topic of conversation; it will no longer be frustrating, time wasting, and money wasting. The name must not classify the new system with any existing mobility mode – it is a new species all by itself.

The specific design of the new mobility mode has been a complex process. Hundreds of decisions had to be made related to tradeoffs between alternative possibilities, and these decisions required years of study to produce satisfactory resolution. The problem of safe control of such a system of vehicles has had to be solved completely, and it has been necessary to show from comprehensive failure modes and effects analysis (FMEA) that the resulting system will be safe and reliable. Evolving the new mobility mode has required the best of engineering science and practice, much of which has evolved in technical fields that have been foreign to highway and transit designers, and that is one reason for resistance.

The real future of the new mobility mode depends on safe attainment of fractional-second headways, which are lower than the stopping-distance headway. The rationale for and the means of achieving safe, small headways in these systems has been the subject of many papers particularly during the 1970s. Such papers are contained in *Personal Rapid Transit II*, the proceedings of the second international conference on PRT, in Irving [1978], Anderson [1978], and in studies sponsored by the Urban Mass Transportation Administration. More recently Anderson [1988] updated and summarized the requirements for safe operation of PRT systems, refined them [Anderson, 1998a] by describing a PRT control system, by considering the question of capacity and comparing it with demands for service [Anderson, 1998b], and later by providing further detail in Anderson [2000]. Much further work was done in 1990-91 a \$1.5 M Phase I PRT Design Study sponsored by the Northeastern Illinois Regional Transportation Authority (RTA). During the 1990s the American Automated Highway System Consortium, after extensive research and development, tested the operation of a group of automobiles traveling down a freeway at headways under half a second. A movie of the test and backup information on it can be seen on

<http://www.gigascale.org/pubs/talks/1997/path/path/>

Thus the practicality of fractional-second headways has been demonstrated in an environment much more demanding than found in PRT.

To attain fractional-second headways safely, the analysis of failure modes and effects is primary to the design, and such analysis shows the power of redundancy in reducing failure frequency. Every failure possibility had to be rigorously and exhaustively explored, and the results used to define the criteria for design. Anderson [1978] and Irving [1978], as well as others, treated this topic; and it was treated in more detail in the above-mentioned RTA study. The purpose of this paper is to describe such analysis and to show that it results in specific conclusions about the design features of the new mobility mode.

In addition to the work of analysis and design, safe short-headway also requires frequent inspection of vehicles in service as well as routine maintenance.

A PRT deployment strategy should be to begin with non-controversial headways and gradually reduce them as they are shown by operational experience and analysis on operational hardware to be safe.

In the next section, externally induced failures are discussed. The remaining sections are devoted to consideration of failures of components of the system and how redundancy can reduce consequences. Of particular concern are common-cause failures that would take out both elements of a redundant system. They can and must be eliminated by isolating the redundant elements.

An important point is that optimized PRT economics show that it can be built and operated as a private for-profit business. As a result, the company has the strongest incentive to make the system safe, for public knowledge of failures will be the fastest way to lose business.

2. Externally Induced Failures

Failures of concern in designing any transit system can be caused either by an external agent or by the failure of a system component. Externally induced failures could be due to a failure in the external power supply, a truck hitting the post of an elevated system, a tree or other object falling across the guideway, a lightning stroke, a high wind, an earthquake, or an act of sabotage or vandalism. All external causes of failure are subject to local building codes and prudent design.

2.1 Power Failure

To minimize the consequences of a power failure, it is necessary to provide backup power through an alternate utility, a motor-generator set, wayside batteries, fuel cells, or flywheels. The method used will be determined during the site-design phase and may vary due to local conditions or technology advances. A key requirement is that it is necessary to switch power sources virtually instantaneously. Thus, if motor-generator sets are used as backup, a practical means of providing instantaneous back up is by means of wayside batteries designed to fill the transient while the motor-generator set gets up to speed.

2.2 Truck Hitting Post

To minimize the consequences of a truck hitting a post, the remedies are to place the posts as far from a roadway as possible, to shield the post by a common highway barrier, or to place the post on a concrete pedestal. In Appendix A it is shown that a 10-ton truck would have to hit the post head on at slightly less than 30 mph to shear a post designed for a maximum wind speed of 120 mph.

2.3 Tree Falling on Guideway

Trees rarely fall unless pushed by a high wind, so it is expedient to suspend operation in winds above about 25 m/s, and in some cases it may be prudent to hold a tree of particular concern back by means of a cable, or prevent it from falling by installing a lightning rod in it. This failure mode is analyzed in Appendix B, where it is shown by a comfortable margin that if the line speed is 30 mph or less and if vehicles are following the vehicle hit by a tree at headways down to half a second, the people in the vehicles behind the unfortunate vehicle hit by the tree will not be injured.

2.4 Lightning Stroke

To minimize the effects of a lightning stroke on the system, the guideway must be adequately grounded. We have consulted several lightning experts and have been assured that this is sufficient to prevent damage.

2.5 High Wind

For urban systems, the sum of the wind speed and the line speed should not exceed about 70 mph. Thus, if the wind speed exceeds 40 mph, the line speed should be no more than 30 mph; if the wind speed exceeds 50 mph, the line speed should be reduced to a maximum of 20 mph; etc. Since the incidence of trees falling usually implies high wind, this precaution should all but eliminate injury to people in the vehicles due to wind. PRT should be designed to operate at speeds that may be different in different segments of the guideway, and the system is designed to be able to reduce and later increase these line speeds.

2.6 Earthquake

The local code for earthquakes must be taken into account in the design and that is easier the lower the weight of guideways and vehicles. Design of the foundations in an earthquake-prone zone must be done by or in consultation with experts.

2.7 Vandalism or Sabotage

During the design of my PRT system, engineers were assigned to act the role of vandal or saboteur. During the Phase I Study for the Chicago RTA, police captains and lieutenants were consulted on issues of security, vandalism and sabotage. No system can be completely immune to such damage, but with people spread out as they are in PRT it is not a likely target for malicious damage.

3. Minimum Safe Headway

Minimum safe time headway is given by the following formula:

$$T_{\min} = \frac{L}{V} + \tau + k \left(\frac{V}{2a_e} - \frac{V}{2a_f} \right) \quad (1)$$

in which L is the vehicle length, V is the line speed, τ is the time interval from start of deceleration of the vehicle ahead to full application of the brakes, a_e is the minimum emergency braking rate under the most extreme conditions, a_f is the maximum possible deceleration due to a failure, and k (≥ 1) is a dimensionless factor. The quantity a_f can be reduced by careful design as described in Anderson [1988]. In traditional railroad practice, in which trains can derail and cross traffic can interfere, it is necessary to assume that $1/a_f$ is zero, and that k is at least 2; however, the conditions in a properly designed PRT system are substantially different. In Figure 1, T_{\min} is plotted as a function of a_f for $L = 2.6$ m, the length of a PRT vehicle, for three values of line speed, and for $a_e = 0.4g$, $\tau = 0.1$ sec, and $k = 1$. The assumption of a response time of 0.1 sec is very short for those familiar with railroad practice, but long for engineers who have developed the control systems used in automated highway vehicles, where time constants of only a few milliseconds are routine. Thus the assumption of 0.1 second is conservative in contemporary practice. In Figure 1 the safety factor k is taken as one, but the emergency braking rate is taken as only 0.4 g, whereas the APM Standards permit 0.6 g. So with $1/a_f = 0$ the same results would be obtained if we assumed $k = 1.5$ and $a_e = 0.6g$.

It may be seen that to attain the short headways desired to realize the potential of PRT, the system must be designed so that a_f cannot under any reasonable circumstances be much greater than the emergency braking rate, and that it be possible to apply constant-deceleration braking. For the smallest values of a_f , which are less than a_e , the minimum possible headway is L/V , which is independent of a_f .

To attain safe, minimum headway, emergency deceleration must be predictable. If the vehicle is braked through wheels, the deceleration possible is variable. It depends on traction, tailwind, grade and gross vehicle weight, therefore an optimized PRT design uses linear electric motors for both propulsion and normal braking, which can be controlled to provide constant-deceleration braking in all emergencies in which an obstruction may appear ahead.

A problem with using electric-motor braking in large-vehicle automated people movers is that they brake by regeneration, i.e., the power generated is fed back into the line. But then they face the problem of "receptivity" of the line. If for any reason power can't be fed into the line, electric braking is not effective, so spring-loaded mechanical brakes must be applied. On the other hand, when small, lightweight vehicles travel nonstop between off-line stations, most of the energy goes into overcoming air drag and road resistance. The kinetic energy at the end of the trip that must be dissipated in stopping is a small fraction of the total energy used. The energy that must be added to the vehicle at the beginning of the trip to overcome inertia is the cruise kinetic energy divided by the efficiency of the propulsion system, and only a fraction of the kinetic energy can be recovered at the end of the trip through regeneration. So in systems using offline stations and nonstop trips, regeneration generally brings too small a return to be worthwhile. As a result, when linear motors are used to brake the vehicle, the extra energy is dissipated in on-

board resistors. This assures that constant-deceleration electric braking is always available. If it were not, the auxiliary brake described below would have already been applied to stop the vehicles.

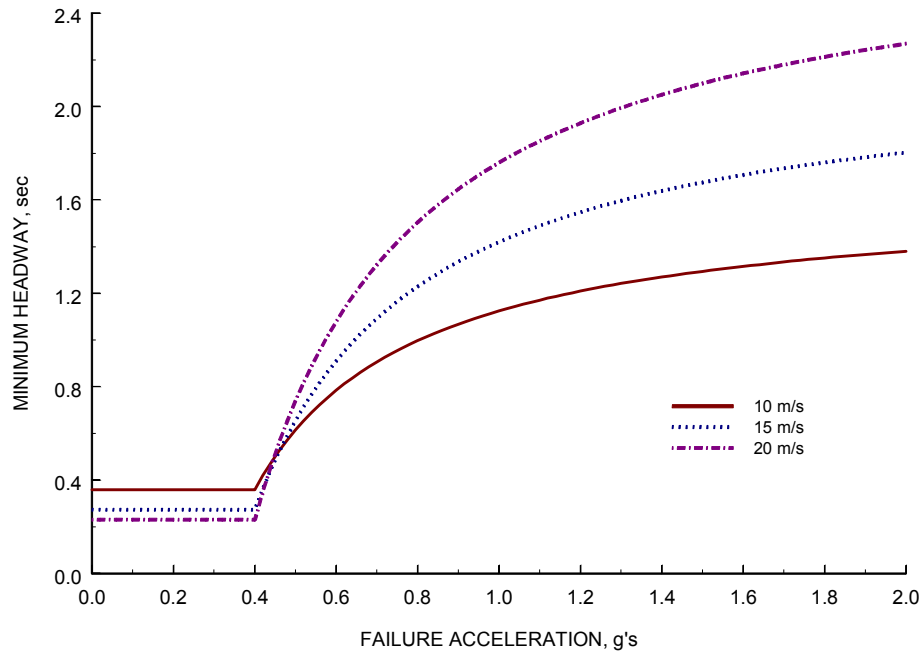


Figure 1. Minimum Headway for a PRT System with Vehicles 2.6 m long.

4. The Requirement of Low Maximum Failure Deceleration

It follows from Figure 1 that, to attain fractional-second headways, the *system* must be designed in such a way that sudden stops are practically impossible. This means that a sudden stop must not be possible unless at least two independent highly improbable events occur in such a way that they produce their effects in close proximity in both space and time, i. e., these events must be virtually simultaneous within the range of influence of each other, and there can be no reasonable common cause whereby both could fail simultaneously. This design criterion is consistent with railroad practice where collision avoidance depends on a functioning *vital relay*, the failure of which in the presence of another failure may result in a collision. In large-vehicle automated guideway transit systems, collision avoidance depends on the functioning of special emergency brakes and no one can guarantee that these brakes cannot fail, only that their failure requires the occurrence of at least two simultaneous failures so improbable that the level of risk involved is accepted.

Each operating PRT vehicle is in one of three states: rest, cruising at constant speed, or following a predefined maneuver profile. A wayside zone controller (ZC) commands the line speed in its zone; and, when needed, at one of several command points the ZC may command a maneuver

profile, in which case, to watch for anomalous behavior, the ZC follows precisely the maneuver profile being performed by each vehicle in its zone.

Each vehicle reports its position and speed to the ZC at an interval of about 40 milliseconds (called the time-multiplexing interval, TMI), and the ZC is connected to wayside sensors that independently report the position and speed of each vehicle as it passes a series of fixed points. If the ZC detects a predefined anomaly in speed, it removes the speed signal for the anomalous vehicle and all those behind, and reports the action to the upstream ZC. Each vehicle controller must be designed so that it detects the speed signal every TMI in order to continue normally, otherwise the on-board speed controller commands the vehicle to creep speed.¹ Examination of the maneuver profiles in all cases shows that, by thus commanding creep speed for all vehicles upstream of the failed vehicle, *a single vehicle failure cannot cause a collision.*

If a wayside ZC fails, it cannot produce the speed signal, in which case all vehicles in its zone command themselves to creep speed. The lack of the speed signal is detected by the upstream ZC, which then causes the vehicles in its zone to slow down to creep speed. Thus no collision occurs. See Section 9 for a discussion of a possible diverge-junction failure.

5. Mean Time Between Vehicle Component and Vehicle Failures

5.1 Computer Failure

A vehicle failure is a situation in which a vehicle slows down or speeds up anomalously in a way that may set up conditions for a collision. Based on work by Boeing in the Advanced Group Rapid Transit (AGRT) Program [Milnor and Washington, 1984], the on-board computer system should be dual redundant. In each pair of these computers, the necessary calculations are performed independently on two motherboards and are checked with each other every TMI. In the following discussion, such a computer with a pair of critical elements and with cross-checking software, will be called a “computer².” If the two calculations do not agree, a failure is reported. Suppose the MTBF of each board is only 5000 hours, which is low for state-of-the-art computers, and suppose the TMI is 0.04 sec. Then, on the average once every 2500 hours a failure can be expected to occur in one or the other of the two boards, and will be reported. The consequence would be that the failed computer² would be switched out. Using the good computer², the vehicle would be permitted to finish its trip and then would be routed empty to the nearest maintenance facility.

A serious problem occurs if the same failure occurs on both boards during one TMI so that no failure is reported when in fact a failure has occurred. In 5000 hours there are $5000 \text{ hrs} / (0.04 / 3600 \text{ hrs}) = 450$ million intervals. Since failures occur randomly, after the first board fails the second board may fail in any one of the 450 million intervals, in only one of which no

¹ Standard practice, derived from railroad practice has required that in such emergencies, the creep speed be zero. This has the unfortunate consequence of stranding and delaying passengers unnecessarily, thus increasing anxiety and possibly inducing heart attacks. With state-of-the-art microprocessor control, commanding a safe creep speed of about 1 m/s (selected to prevent injury in a collision) for a vehicle with no fault is no less reliable than commanding zero speed. Moreover, in large-vehicle automated systems, in which there are standing passengers and no protection for them, the consequences of a low-speed collision are far greater than in a system in which all passengers are seated and protected.

failure is reported when in fact a failure has occurred. Thus the mean time between simultaneous failures in both boards is $2500(450)(10)^6 = 11,250(10)^8 \approx 10^{12}$ hrs. If it is assumed that each computer² is functioning all of the time, even in storage, then, since there are $24(365) = 8760$ hrs/yr, the MTBF of one of the computers² is $11,250(10)^8/8760 \approx 128$ million years, or virtually never.

But, during every TMI the output of each of the computers² is compared with the other. If no failure has been reported but these two outputs don't match, then the highly unlikely situation described in the previous paragraph has occurred. Now arises the necessity of knowing which board failed. During the 1980s software was developed that continually checks the calculations and can detect where the failure occurred. It is also possible that the source of the failure can be determined by continuity with previous calculations. A vehicle failure occurs only if the second computer² experiences a failure after the first computer² experienced such a failure and the vehicle is on its way to the maintenance shop. It is reasonable to assume that after a failure, the time to reach the maintenance shop is less than 10 minutes or 1/6th hr. Based on the above calculation, either one or the other of the computers² may fail twice as often, i.e., once in $5625(10)^8$ hrs and the second similar failure may occur randomly in any one of $11,250(10)^8/(1/6) = 6.75(10)^{12}$ intervals. Thus the mean time between vehicle failures is $5625(10)^8 \times 6.75(10)^{12} = 3.8(10)^{24}$ hrs or $4(10)^{20}$ yrs, which may be compared with the estimated duration of the universe of $13.6(10)^9$ years.

5.2 Communications Failure

Based on the calculations of Section 5.1, it can be assumed that a vehicle failure as defined at the beginning of this section will not be due to a computer failure. Consider other possible failures. The vehicle computer receives its commands from a local zone controller through a communications device, the signals from which are read by a redundant pair of transmitter/ receivers. The protocol is that the ZC sends its command and the on-board controller returns the command. If the returned command does not agree with the sent signal the ZC resubmits the command. If it does not come back correct the second time, the ZC removes the speed signal, which must be received by the vehicle controller in order to proceed normally. Otherwise, the vehicle controller is programmed to decelerate to creep speed and the consequence of this kind of failure is a slow-down in the traffic, not a collision. In the Phase I PRT design study with the Chicago RTA, available data² showed that the MTBF of the communications device was at least 20,000 hours. Using the logic for redundant systems derived above, the MTBF of a system consisting of a pair communications devices aboard each vehicle, each having a mean time to failure of $MTBF_d$, is

$$MTBF_s = \frac{MTBF_d^2}{2\tau_{shop}} \quad (2)$$

As before, assuming the time to reach the shop is $\tau_{shop} = 10$ min or 1/6 hour, the communications systems MTBF is $(20,000)^2/2(1/6) = 12(10)^8$ hours, or $12(10)^8/8760 = 137,000$ years.

² MTBF data in the Chicago RTA study was taken either from industrial sources or from a data base maintained by the Reliability Analysis Center, Griffiss Air Force Base, Rome, New York.

5.3 Encoder Failure

Next consider that the vehicle receives its actual speed and position from a system of digital encoders, consisting of one encoder in each of the four wheels. The front pair and the rear pair are each averaged to give the correct output in turns. Each encoder transmits a pulse every time the vehicle has advanced a very small increment in distance. By means developed in the Boeing AGRT program [Lang and Warren, 1983], both vehicle speed and position can be derived from this signal. The digital encoder consists of a small wheel that turns with one of the vehicle's support wheels and is marked alternately, for example, with black and white spaces. By means of a light source, a pulse is sent to the computer each time one of the white spaces is reached. If one of the encoders fails to send its pulse, a failure is reported and only the output of the other pair of encoders is used. Simultaneously, the vehicle commands itself to finish its trip and then travel to the maintenance shop, taking, as estimated before, 10 minutes. Equation (2) gives the MTBF of the encoder system. The data found in the sources given in Section 5.2 gave the MTBF of an encoder as 25,000 hours. Thus this MTBF is higher than estimated for the on-board communications device by the ratio $(25/20)^2$ or 1.56, which gives for the encoder system MTBF 214,000 years.

5.4 Propulsion-System Failure

The output of the computer system in terms of a voltage command at a given frequency is sent to each of *two separate propulsion systems*, each consisting of a Variable Frequency Drive (VFD), which sends a variable-frequency voltage to a linear induction motor (LIM). In the Phase I study for the Chicago RTA, the MTBF of the VFD is reported to be 50,000 hours and the MTBF of the LIM 60,000 hours. The LIM itself consists of imbedded copper windings that would fail only if they overheated due to excessive current, but the VFD provides the necessary current limiter and temperature sensors are imbedded in the motor to shut off the current if it were to overheat. The reciprocal of the MTBF of one series of VFD-LIM is the sum of the reciprocals of the unit MTBFs. Thus

$$MTBF_{VFD-LIM} = \frac{1}{\frac{1}{50,000} + \frac{1}{60,000}} = 27,300 \text{ hrs.} \quad (3)$$

Then, using equation (2), the propulsion-system MTBF is therefore $(27,300)^2/[2(1/6)] = 22(10)^8$ hrs. Assuming the average vehicle operates 10 hrs per day and 320 days per year it would operate 3200 hours per year, so the propulsion-system MTBF would be 700,000 years. If the propulsion system fails, the vehicle cannot move under its own power and must be pushed by the vehicle behind.

5.5 Other Vehicle-Borne Components

In the above-mentioned Chicago RTA Program, data on the MTBFs of all components were found from the above-mentioned sources. This data was gathered in 1991 before there was great emphasis on 6-sigma manufacturing; however, improvements made since 1991 have not been taken into account.

Table 1. Component Mean Times to Failure

Component	Single-Component MTBF, hrs	Redundant System MTBF, hrs
Switch Actuator	4800	69 million
Auxiliary Brake	4600	
Power Pickups	10,000	300 million
Push-Mode Actuator	50,000	
Door Actuator	4600	
Hydraulic Bumper	5000	
Wheels	45,000	
Air Conditioning Unit	1900	
Ventilation Fan	5000	
Heater	5000	

Following are comments on possible failures of the components listed in Table 1, all of which must be inspected and serviced regularly.

- 5.5.1 Switch Actuator: To improve reliability, a pair of back-up solenoid actuators will be used to throw the switch in each direction. Failure of both actuators may require that the switch be thrown manually, and the design permits manual actuation. The mean time between such incidents is estimated to be 69 million hours, or assuming vehicle operation 10 hours per day and 320 days per year, about 22,000 years.
- 5.5.2 Auxiliary Brake: It is necessary to have a separate braking system aboard the vehicle that will engage when primary power fails. Primarily because 1) the probability of needing such braking is remote in a properly designed and well-maintained system, and 2) it is possible to design the system so that the consequences of a low-speed collision are slight, the parking brake has been designed to fulfill this function. Such a brake must not be applied through the wheels; it must be a no-power-on, no-power-off device; and it must be possible for the vehicle behind to release it. The device that meets these criteria is a brake shoe that presses down on the running surface and is actuated by a ball-screw actuator powered by a small on-board battery, with a circuit designed to turn the actuator on if power fails. By proper design of the brake shoe, it can be made to cut through any residual ice on the guideway, and it can be made of very-high-friction material. The running surface is a copper sheet overlaid on a steel angle, a design required for operation of the LIMs. Tests during the RTA Phase II Program showed that the wear characteristics of a reasonably hard copper alloy are adequate for this task. This brake serves as a parking brake and an emergency brake. It is applied each time the vehicle stops in a station and is released each time the vehicle is ready to leave, so it is tested many times a day. If a vehicle leaves a station with an auxiliary brake that has worked, which is the only way it will be permitted to leave with passengers aboard, and the trip time is 1/6th of an hour, then in only one trip in $4600/(1/6) = 27,600$ would a failure occur sometime during the trip. The MTBF between incidents in which the auxiliary brake must serve as an emergency brake is estimated in Section 5.5.3

- 5.5.3 Power Pickups: In merge and diverge sections of the guideway, there will be power rails on both sides. Study during the Phase I Chicago RTA Project resulted in the conclusion that power-rail reliability is sufficiently high that power rails are not needed on both sides of the guideway away from the merge and diverge sections. There is, however, a pair of power-pickup assemblies on each side of the vehicle. If both assemblies on one side were to lose contact, the vehicle would lose primary power and the auxiliary brake would actuate. It is possible that both power-pickup assemblies would fail at a time when the auxiliary brake could not function. But the auxiliary brake is actuated every time the vehicle comes to a stop, and if it does not actuate then the vehicle will be dispatched to the maintenance shop. A typical trip time will be less than 10 minutes, but assume as before it is that long, i.e., $1/6^{\text{th}}$ of an hour. Then during the 4600 hours between failures of the auxiliary brake only one time in $4600/(1/6) = 27,600$ would the brake not be working when it was needed to stop the vehicle as a result of dual power-pickup failure. Thus, using data from Table 1, the meantime between incidents in which the auxiliary brake could not stop the vehicle due to a power-pickup failure would be $300(10)^6(27,600) = 8(10)^{12}$ hrs/3200 = 2.6 billion years. But, even in this case, there will be enough on-board battery power to slow the vehicle to a halt by action of the LIMs.
- 5.5.4 Push-Mode Actuator: The push-mode actuator will be tested every time the vehicle enters the maintenance shop for its routine inspection and preventive maintenance. Assuming, as before, operation of an average vehicle ten hours per day, the inspection occurs every 20 hours. With a 50,000-hr MTBF, as found from Table 1, in only one operational period out of $50,000/20 = 2500$ would a specific actuator be expected to fail when needed. This would mean, for example, that in a fleet of 500 vehicles, a push-mode actuator somewhere in the system would be inoperative every $2500/500 = 5$ operational periods. But the chance that the one push-mode actuator needed to push a vehicle ahead was the one that had failed would be only one out of 500. So with a push-mode actuator somewhere in the system out of commission every 5 operational periods, only one time in $5(500) = 2500$ would the actuator needed not be working. Since the mean time between pushing incidents in a fleet of 500 vehicles was estimated in Section 5.6 to be 150 years, the mean time between incidents in which the vehicle behind could not perform the pushing function would be $150(2500) = 375,000$ years. This is an example of the frequency in which people may have to be rescued from a vehicle.
- 5.5.5 Door Actuator: Each vehicle has a door on each side, which is opened and closed automatically by a door actuator. A door is to actuate only in a station. If for some reason the actuator is inoperative, the design is arranged so that the door can be opened manually from the outside, and, with some instruction from an operator in the central control system, it will be possible to talk most people through a procedure to open the door from the inside in a situation in which there is no one in the station who could help. If that were not possible, an indication in the control room that a door did not open would be a signal to send one of the system personnel to the station to assist. Thus a door failure is a nuisance, not a problem of safety.
- 5.5.6 Hydraulic Bumper: The bumper in the rear of each car contains hydraulic fluid and is designed to provide a constant force throughout its stroke. It activates in any collision under 14 mph. To provide energy absorption at higher relative speeds, a friction bumper

is mounted at the front of each car. It is simply a pair of press-fit concentric cylinders with nothing in it that can fail. If the hydraulic fluid in the rear bumper were to leak out, it would provide little shock absorption, thus it must be routinely inspected. From Table 1, in a fleet of 500 vehicles, it can be expected that a hydraulic bumper somewhere in the system will fail every 10 hours, but as calculated in Section 7, the mean time between vehicle-to-vehicle collisions is longer than the life-time of the universe; so, with an MTBF of 5000 hours, the mean time between collisions in which the bumper on the lead vehicle is inoperative is much longer. If the vehicle is inspected every 20 hours, such a combined failure circumstance would occur in only 1 of every $5000/20 = 250$ collisions.

5.5.7 Wheels: Commercially available wheel-axle-bearing assemblies will be used. The main-support tires will be either cushion or the new Michelin airless tire, neither of which can go flat. The side tires for lateral support will be polyurethane. The wheels run on smooth surfaces in the shade. There are no chuckholes or curbs to climb. The running-surface expansion joints are designed so there is no step or slope discontinuity. Temperature sensors will be built into the wheel hubs to sense a temperature rise in the case of an incipient bearing failure. If a bearing were to freeze, which today is almost unknown in automobiles running in a much tougher environment, and the wheel were to lock, the consequence would be minor because it is only one of four wheels, and both the tire and the running surface are smooth. With only about one fourth of the vehicle weight on one wheel and a coefficient of friction of say 0.2, the friction force would be only 5% of the weight, which would slow the vehicle at 0.05 g. The vehicles behind, designed for emergency braking of up to 0.4 g, have no trouble stopping in time to avoid a collision.

5.5.8 Air Conditioning, Ventilation, and Heater. The system will become aware of a failure in any of these units by report at central control of an anomalous temperature, or by complaint of a passenger. The trip is sufficiently short that it can usually be concluded before dispatching the vehicle to the maintenance shop, and if not, the passenger can press a button to stop the vehicle at the next station.

5.6 MTBF for Vehicle Failures

A vehicle failure of concern for safety is an incident that causes a vehicle to depart from its commanded maneuver profile enough so that it could collide with another vehicle. The failure rate for a vehicle thus defined is the sum of the failure rates of the components discussed above that would cause a vehicle to stop. With n components, the mean time for vehicle failures is given by the equation

$$\frac{1}{MTBF_{veh}} = \sum_{i=1}^n \frac{1}{MTBF_i} \quad (4)$$

Substituting the above-derived component MTBF's

$$\frac{1}{MTBF_{veh}} = \frac{1}{4(10)^{20}} + \frac{1}{137,000} + \frac{1}{214,000} + \frac{1}{700,000} = \frac{1}{75,000}$$

So, the vehicle MTBF is 75,000 years or 240 million hours. In a fleet of 500 vehicles, one vehi-

cle would have to be pushed every 150 years.

The question arises as to how often it would not be possible to push a stopped vehicle. No failure in the system could cause such an event. The support wheels are merely rollers. There are no brakes on them. If one bearing were to freeze, as discussed in Section 5.5.7, it would still be possible to push the vehicle with the one behind. If the parking and emergency brake were to stick in the down position, the push-mode coupler would release the brake in a simple, positive way. There are no other system failure modes that could prevent a vehicle from being pushed. Thus the need for walkways to rescue people stranded on the guideway is limited to “Act of God” events such as a tree falling across the guideway, notwithstanding the precautions discussed in Section 2.3. Because the incidence of need to rescue passengers cannot be due to a system failure, it is impossible to calculate a mean time for such an event.

If one vehicle fails by producing an anomalous deceleration, the cognizant zone controller removes the speed signals to the vehicles behind so that they slow to creep speed. If a vehicle could fail in such a way that it results in an anomalous acceleration, it could crash into the vehicle ahead. To do this would require a failure of the on-board computer system, which has an MTBF of $4(10)^{20}$ years, or of the VFD, which has current limiters to prevent overspeed.

6. Mean Time Between Zone Controller Failures

Assume that the zone controller hardware is of the same quality as the vehicle controller hardware. Then the mean time between failures of each of the pair of computers, as estimated in Section 5.1, is $(10)^{12}$ hours. A failure of either of the two mother boards in either of the two computers² would be reported to the central-control station, whereupon a trained maintenance person equipped with spare parts would be dispatched to the fault site. A system failure would occur only if the second computer experienced a similar double failure before a part replacement could be made. Assuming that a series of events slow him down, a reasonably conservative value of the time to repair might be about two hours. Thus on the average only one time in $5(10)^{11}$ hours would the second computer fail before the repair could be made. The calculation is the same as before with the two hour time to repair substituted instead of 1/6 hour to get to the maintenance shop. Thus, from equation (2), the mean time between zone controller failures would be $[(10)^{12}]^2/2(2\text{hrs}) = 2.5(10)^{23}$ hrs or $3(10)^{19}$ years.

7. The Mean Time Between Vehicle-to-Vehicle Collisions

As argued in Section 5.4, failure of one vehicle does not set up conditions for a collision because the system reacts to avoid contact with it. Suppose two vehicles in proximity fail. Let $MTBF_v$ be the mean time between failure of a single vehicle in such a way that it may (not necessarily will) cause a collision if a second vehicle fails within a time interval δt and a space interval δs of the first failure. Let the number of vehicles in the system be N_v . Then the mean time between failures of vehicles in the system is $MTBF_v / N_v$. After one vehicle fails, the conditions for a collision can be set up only if a second vehicle fails within a time interval δt and a space interval δs of the first failure. The probability of any one of the other vehicles failing within the time interval δt and the space interval δs is $(N_v - 1)\delta t / MTBF_v \times \delta s / L$, in which L is the total guideway length. The reciprocal of this quantity is the number of incidences in which the first

vehicle fails for one incidence in which a second vehicle fails within a close enough interval of time and space for the conditions for a collision to be set up. But a collision may occur only if a lead vehicle anomalously slows down while the following vehicle speeds up. There are four possibilities: both vehicles slow down, both speed up, the one ahead speeds up while the one behind slows down, or the one ahead slows down while the one behind speeds up. Only the last of these four possibilities sets up the conditions for a collision. Hence, the mean time between incidents in which at least two vehicles fail close enough in space and time to set up possible conditions for a collision is

$$MTBF_{col} = 4 \times \frac{MTBF_v}{N_v} \times \frac{MTBF_v}{(N_v - 1)\delta t} \times \frac{L}{\delta s} \cong \left(\frac{MTBF_v}{N_v / L} \right)^2 \frac{4}{\delta t \delta s L}. \quad (5)$$

In this expression N_v / L grows slowly with the size of the system because the demand per unit length of guideway will generally increase as the system grows. Therefore the mean time between collisions somewhere in the system reduces somewhat faster than the system size increases, which is to be expected.

Suppose, as estimated in Section 5.6 that with a dual redundant vehicle controller and taking into account all possible failures, $MTBF_v = 120$ million hours. For the proximity time δt , consider that it takes about 6.3 seconds to stop a vehicle from 13 m/s at a quarter g deceleration and maximum jerk of a quarter g per sec. So take $\delta t = 6.3 \text{ sec} = 1.8(10)^{-3} \text{ hr}$, and take δs to be the stopping distance of one vehicle, which from 13 m/s is about 41m. The combined failure could occur any time of day or night. Assume it occurs when there are 15 vehicles per km in the system. Then, from equation (5),

$$MTBF_{col} = \left(\frac{1.2 \cdot 10^8}{15} \right)^2 \frac{4}{1.8(10)^{-3} (0.041)L, km} = \frac{3.5(10)^{18}}{L, km} \text{ hrs} \quad (6)$$

On the average, each vehicle operates about 10 hours a day and about 320 days per year, or 3200 hrs/yr. Thus

$$MTBF_{col} = \frac{3.5(10)^{18}}{3200L, mi} = \frac{10^{15}}{L, mi} \text{ years.} \quad (7)$$

A large urban PRT system could have 1000 km guideway. In this case,

$$MTBF_{col} = \frac{10^{15}}{1000} = 10^{12} \text{ years.} \quad (8)$$

In such a system, it can be expected that the vehicles will average perhaps 45 km/hr, or assuming as before 10 hours per day, say 450 km per day or $450(320) = 144,000$ km per year. With 15 vehicles per km, a 1000-km system would have 15,000 vehicles, so the system would run about $15,000(144,000) = 2(10)^9$ vehicle-km per year. In 10^{12} years the system vehicle-km would be $20(10)^{20}$, which implies one incident in which a collision may occur every $20(10)^{20}$ vehicle-km.

In the U.S. automobile system there are about $130(10)^6$ active automobiles averaging each about

28,000 km per year, or a total of about $36,000(10)^8$ vehicle-km, during which time there are about 44,000 fatalities, or 82 million vehicle-km per fatality. PRT vehicles would travel $20(10)^{20}/82(10)^6$ or $24(10)^{12}$ times as far before an incident in which a collision, not necessarily a fatality, may occur. This is such a large number that it can be concluded that it is not necessary to design for the case of one vehicle colliding with another.

8. Potentials for Sudden Stops

To make further progress, it is necessary to consider the specific situations in which a sudden stop due to a system failure is possible. These are the possibility of:

1. Sudden locking of a wheel, discussed in Section 5.5.7.
2. A collision with the junction point of a diverge section of guideway.
3. A collision between two merging vehicles.
4. A run-away vehicle entering a station and crashing into a stopped vehicle.

The first three of these failure modes could result in a high value of a_f . Thus, only by eliminating their causes can one attain safe headways in the economically viable range. The fourth has been of fundamental importance in the design of PRT because it is the worst failure possibility in the system, and thus must be included in any discussion of potential failure modes.

9. Diverge-Junction Collision

The PRT switch is a mechanical device mounted on the vehicle with no moving parts in the guideway. It consists of a pair of arms with a wheel on each end of each arm that engages either a left or a right channel-shaped rails mounted one on each side of each merge or diverge section of guideway. The switch arm, which has a wheel on each end, rotates about a longitudinal axis so that no position of the switch, under any circumstance, could result in contact with a switching rail. The switch arm is shaped so that the line of force from an engaged switch wheel passes through the axis of rotation, thus making it self-centering.

Normally the vehicle's switch wheels on either the left or right side are positively engaged in the above-mentioned left or right switch rail while the vehicle passes through the diverge section of guideway. For a junction-point collision to be possible, one of three events must occur: 1) the switch rail has come loose, 2) a switch wheel breaks, or 3) the switch arms are not locked in their left or right positions as the vehicle approaches the switch rail. The probability of a collision with the junction point is minimized as a result of any of these events by designing the front of the chassis to be as narrow as possible.

The first two of the above possibilities require structural failure. The switch arms, wheels and rails are of necessity vital elements that cannot practically be duplicated. Assurance against failure requires that they be designed very conservatively. With a lightweight vehicle it is possible to do so. The switch arms must be manufactured out of high-fatigue-strength material, preferably forged. The switch rails will be adjusted and fastened in place at least every five feet. Loosening of one fastener must be detectable, and must, by design, not cause the rail to break loose. The high-stress regions of the switch arms must be free of scratches or other causes of stress concentration, and must be inspected routinely.

To examine the possibility that the switch arms are not securely in the correct left or right position at the moment they reach the flared guideway switch rails, it is necessary to describe switch operation:

- After a vehicle passes either a merge or diverge point, it passes a Switch Command Point (SCP). If the next branch point is a line merge or line diverge, SCP is placed right after the previous branch point, but ahead of the next switch rail by at least a stopping distance plus line speed multiplied by the switch throw time.
- If the next branch point is into a station, the Deceleration Command Point (DCP) must be located a normal stopping distance plus line speed multiplied by the braking time constant ahead of the last stopping position on the station entry queue. As before, the SCP must be placed upstream of the switch rail at least a stopping distance plus line speed multiplied by the switch-throw time, and it must be upstream of the DCP far enough so that the switch throw is complete before the DCP is reached. If the SCP is placed too far up stream, a vehicle may be waved off because the station at that moment was full, but a short time later the last berth may have cleared so that the vehicle need not have been waved off. From study of network simulations, this is a realistic problem. To minimize wave-offs, the SCP should be placed as close to the DCP as permitted by the above-mentioned constraints.
- When a vehicle reaches an SCP, the cognizant zone controller (ZC) interrogates it for its destination, looks up the desired left or right switch position for that destination from a table of switch commands, and sends the switch command to the vehicle. If, however, the last station position is occupied, the switch is thrown to direct the vehicle away from the station.
- If the switch were to become stuck in the wrong position it may direct the vehicle either into or away from the station. If it is directed into the station and the last position is occupied emergency braking must be applied. If it is directed away from the station the vehicle can continue down the guideway. Central control is then alerted that a switch on a certain vehicle is in the wrong position. If the switch cannot be moved by remote control, the vehicle must continue until reaching either a) a station on the side the switch is thrown, in which case the passengers disembark and proceed to their destination in another vehicle, or b) a maintenance facility on the side the switch is thrown. If and only if neither is a possibility and attempts to throw the switch remotely fail, the vehicle must be stopped and a maintenance person must throw the switch manually. This must be a rare occurrence for it causes a line stoppage, and requires that *one important criterion* for switch design be that the switch can be thrown manually in a short time by a maintenance person.
- When a vehicle passes an SCP, about half the time the switch is already in the correct position, so nothing need be done. When the switch must be thrown, the on-board computer commands it to be thrown, and simultaneously issues a command to stop the vehicle a bit more than a switch-throw time later a) if proximity detectors do not indicate that the switch is in either the left or right position, or b) if the switch is in the position to go into a station with no room. Detection of neither of these conditions after the switch-throw

time cancels the command for the vehicle to stop. If the first condition is detected, emergency braking must be applied; and, if the second condition is detected, normal braking would be applied. Obviously the software must be totally debugged.

- Having been thrown, there must be a means to hold the switch in either the left or right position before reaching the next set of switch rails. In the industry, a firm requirement is that *the switch be bi-stable*, so that, by itself, it cannot hang up in a mid position. The switch is held in position by a spring and is designed so that, after the switch wheels engage the switch rail, the contact force holds the switch in position because the line of action of the force passes through the switch-arm bearing axis. An important advantage of use of a spring to hold the arm is that it would be easy for either a) a maintenance person to throw the switch manually, or b) a mechanism on the vehicle behind to throw the switch.
- An alternative holding mechanism would be a solenoid-actuated pin. Its advantage would be that, while engaged, it would be impossible for the switch torquer to throw the switch under any circumstance. Its disadvantage is that if the pin may freeze in position, making it difficult for a maintenance person or a vehicle behind to throw the switch.

The circumstance in which such a switch would not be in either its left or right stable positions at the instant the guideway switch rails are encountered will be rare. The one plausible suggestion is that the switch arm may throw as a result of an “out-of-the blue” freak voltage pulse, probably due to a lightening stroke, even though the guideway would be grounded and the control system shielded. But the probability of such an event occurring anywhere in the system, P_{fvp} , is small. Since the actual switch-throw time is less than one second, the freak voltage pulse, which could occur at any time, would have to occur at almost exactly the right time (with an interval δt) so that the switch would not have thrown to the other side at the instant the guideway switch rails are engaged.

The probability of any vehicle entering the switch rails with the switch arm somewhere in the middle of its throw is P_{fvp} multiplied by the ratio of the distance traveled during the critical phase of the switch throw time $V\delta t$ to the total guideway length L multiplied by the number of diverge points N_{div} and the number of vehicles N_v . Thus, assuming that an "out-of-the-blue" voltage pulse occurs, the probability that it occurs during the critical time δt , so that the switch arms fail to engage on either side is

$$P = \frac{V\delta t}{L} \times N_{div} \times N_v = V\delta t \times \frac{N_{div}}{L} \times \frac{N_v}{L} \times L \quad (9)$$

But the voltage pulse can be assumed to occur at random and would be effective over a limited region, say δl . Therefore the probability P' that the voltage pulse occurs at a time that it may cause the switch to throw, would be the value given by equation (9) multiplied by $\delta l/L$, i. e.,

$$P' = V\delta t \times \frac{N_{div}}{L} \times \frac{N_v}{L} \times \delta l \quad (10)$$

Assuming $V = 13$ m/sec and $\delta t = 0.5$ sec, $V\delta t = 0.0065$ km. Furthermore, assume $N_v/L = 15$ vehicles per km, $N_{div}/L = 3$ diverge points per km, and $\delta l = 10$ m = 0.01 km. Then

$$P' = 0.003 \quad (11)$$

We conclude that *if* one random freak voltage pulse occurs anywhere in the system in such a way as to be able to throw a switch, say due to a lightning bolt, however improbable that event may be, the chance that at least one vehicle will be in position to be damaged is too high to ignore.

It is thus necessary to determine if any possible type of voltage pulse could throw a switch, or if the switch actuator can be designed so that no voltage pulse can cause it to throw. If so, it is necessary to lock the switch in position as it passes an SCP, for example by means of the above-described solenoid-actuated pin. The disadvantage of such a lock has been discussed. Its operation must be checked every time the vehicle enters the maintenance shop for routine maintenance. But, the presence of a locking pin means that the unintentional throw of a switch requires the occurrence of a specially shaped voltage pulse that first releases the locking pin, then roughly 100 msec later causes the main torquer to move the switch. The combination of the voltage pulse affecting the torquers at all in a system in which the critical components are shielded from such events, combined with a virtually impossible pulse shape together make the probability of a junction collision remote enough that it need not be included in estimation of a_f for purposes of calculating minimum operational headway.

It can thus be concluded that, by careful design, the possible causes of a sudden stop at a diverge junction can, for practical purposes, be eliminated. Moreover, if a switch should start to throw unintentionally and the vehicle's control system is operative, the event would be reported to the zone controller (ZC) in the next time-multiplexing cycle, which would cause the ZC to remove the line-speed signal, which would cause the vehicles behind to slow to creep speed, beginning before a sudden stop can occur. If the vehicle's control system is rendered inoperative by the voltage pulse, its failure to report to ZC is the major reason the ZC would remove the normal line speed signal, which will cause the emergency brake to be applied. If the ZC is rendered inoperative by a voltage pulse, it will not be able to transmit the normal line-speed signal and the vehicle controller, requiring such a signal, will cause the vehicle to slow to creep speed.

If, in the virtually impossible circumstance that the vehicle's switch fails to engage, wind or unbalanced passenger load may push the vehicle to a small range of positions, which can be minimized by design, and for which it would impale on the switch junction. If such a crash were to occur, what then is the chance that the power-pick-up shoes will rotate enough to short out primary power? To eliminate this possibility, it may be necessary to modify the design of the pick-up shoes. All transit-proven power-pickup shoes are designed for larger vehicles and much higher power levels. Considering the type of insulated covering over the power rails commonly used, and the design possibilities in the shoe itself, it is difficult to believe that, with some careful design and experimentation, a shoe can't be designed so that it could not short out the power rails. Such design should be a priority item, not only because of the possibility, however remote, of a diverge-junction collision, but because it is unacceptable to have a shoe fall off at any point.

A shoe on one side of the vehicle or the other has to disengage and re-engage every time a merge or diverge section of guideway is passed, so the design has required special attention including bench testing before going into service. Such testing was done during the RTA Phase II program. If the shoe is designed properly, the possibility of loss of line power in a sudden stop via the above scenario need not be a factor in selection of subsystems.

10. Merge Collision Between Two Vehicles

Consider a left stream and a right stream of vehicles approaching a merge junction. The progress of the vehicles is monitored by a wayside zone controller ZC, which is a dual redundant pair of fault-tolerant computers powered by uninterruptible battery power supplies, as previously described. A fault-tolerant computer has a pair of motherboards and checking software capable of detecting failures in either board. Such computers are used in a variety of applications in which interruption of operation has serious consequences. The probability of failure of such a wayside computer system is estimated in Section 6. These computers can be placed in vandal-proof temperature-controlled basement compartments under stations and shock mounted if necessary to reduce the effect of vibrations due to passing traffic. The major cause of failure of such systems is current overload, but the current is limited to well below the critical point.

The vehicle controller (VC) is programmed to maintain line speed only if an active line-speed signal is received every time-multiplexing interval (about every 40 msec). Absent a line-speed signal a second time in sequence, the VC commands deceleration at the normal rate to a predesignated creep speed. If a ZC were to become inoperative, the line-speed signal generated by the ZC would disappear, and the vehicle controllers would command deceleration to creep speed. In this case, it can be anticipated that vehicles approaching the merge may be in various stages of the slip maneuver, some accelerating back to line speed and some decelerating.

The Clearance Point (CP) is the point where vehicles the same distance behind the merge junction just touch each other. Proceeding further downstream would cause the sides of these two vehicles to crush. The Merge-maneuver Command Point (MCP) is selected to be at a distance upstream of the CP enough so that the with the largest slip commanded to space vehicles a minimum of one headway distance apart is completed before the CP is reached. If vehicles on opposite legs of the merge that have passed MCP at the time of the ZC failure are still less than a headway distance apart, the vehicle ahead is traveling faster than the vehicle behind, which is decelerating into its correct slot. If both vehicles are commanded at the same time to decelerate to creep speed, the vehicle ahead, which is going faster, will have a longer stopping distance than the vehicle behind. Thus, the distance between these vehicles will increase.

Consider the state of vehicles yet to pass MCP at the time of the ZC failure. On one of the lines, the vehicles may be slipping to maintain minimum headway behind the vehicle on that line that has reached MCP and is commanded to slip. The vehicles on the other line may be traveling at line speed. In either case, vehicles behind MCP will have ample space to stop before reaching the CP, thus cannot cause a merge collision. The conclusion is that a ZC failure, while causing all vehicles approaching the merge to decelerate, will not cause a collision.

If a collision is to be possible, therefore, it must be caused by failure of one or more vehicles while the ZC is operative. If only one vehicle fails in such a way that it begins slowing down

anomalously, the anomaly is detected by the ZC, which commands the vehicles behind on both legs of the merge to decelerate at the emergency rate to the creep speed. Regardless of where the failed vehicle is along the merging guideway, its reduction in speed, as argued above, will not cause a collision, because all vehicles behind it on both legs of the merge slow down at the same rate.

To account for the possibility of a vehicle speeding up anomalously, its VC software must be designed to cut off propulsive power until speed is reduced, which is of course exactly the function of speed control. Checked redundancy in the VC and its sensors is required to make this possibility sufficiently remote. If the vehicle's behavior does not quickly correct, the VC causes its emergency brake to be applied, and the ZC causes emergency braking of the vehicles behind.

If a vehicle experiences a failure and emergency braking is normally through LIMs, the auxiliary brake, normally used for parking, must be applied. If only one vehicle has failed, it is best not to stop it too quickly, which means that the vehicles behind need not be stopped more rapidly than at the normal rate.

We are left with the case of two vehicles subject to major failures while approaching a merge. The worst case would occur when a leading vehicle on one leg of the merge begins to slow down anomalously while a trailing vehicle on the other leg begins to accelerate anomalously, in just such a range of relative positions so that they reach the CP close to the same time. Such an event requires the occurrence of two major independent failures virtually simultaneous in both space and time. We can estimate the probability of such an event by making use of equation (8), which gives the mean time between collisions anywhere in the network. The MTBF for merge collisions must be longer by the ratio

$$\frac{L}{N_m \delta s}$$

in which there are N_m merges in the system. A reasonable number is in the range of say 2.5 merges per km. Assuming, as in equation (6), that $\delta s = 0.041$ km, the mean time between merge collisions would be

$$MTBF_{mergecoll} = 10^{12} \left(\frac{1}{2.5(0.041)} \right); 10^{13} \text{ years.} \quad (11)$$

Following the argument below equation (8), this is so low that it is not necessary to design the vehicles to withstand merge collisions.

11. Run-Away Vehicle Entering Station and Crashing into Stopped Vehicle

Such an incident is possible in any type of guideway transit system, whether the headway is long or short. If the failure is due to an on-board computer failure, the mean time between vehicle failures has been considered above. In any transit system, braking is initiated at least a stopping distance upstream of the farthest upstream stopping point. If, in monitoring the profile of decreasing speed, speed exceeds expectation, the braking force must be increased. In standard railroad practice, where braking is applied if a train is detected in the block ahead, the question of

failure of the normal braking system cannot be related to the block length—it is too late. Braking is expected to work, and there are so many motors and wheel brakes on a train that if one or more fail, the train still stops.

In contemporary types of automated guideway transit, there is generally a separate emergency braking system on each vehicle that can apply irrevocable, spring-actuated emergency braking that is assumed to work if primary braking, often regenerative, fails. We have needed to consider the type of emergency braking appropriate for optimized PRT. If brakes were to require primary power for actuation, the brakes could fail due to shut off of the power source, which could be either at wayside or on the vehicle. Prevention of wayside power interruption is discussed in Section 2.1. It has been specified that there be a braking system (Section 5.5.2) that actuates irrevocably if primary power is interrupted.

It has been argued that it is absolutely necessary to have backup power that initiates virtually instantaneously in the event of utility failure. Assume this is the case. Next, it has been argued that there may be some cause that would short the power rails on a segment of guideway independent of the source so that the existence of backup power would not help. One scenario, suggested in Section 9, is that a vehicle crashes into the junction point of a diverge section of guideway and in the crash the power-pick-up shoes rotate enough to short out primary power. However, such sections are remote once a vehicle has entered into a station.

Assume that the above recommendations on back-up power and pick-up shoe design are carried out satisfactorily. There is still the nagging concern that, for some unknown reason, power on a section of guideway is lost. The most crucial place would be on the entrance to stations. If this were the case, one solution is to supply the deceleration track with an uninterruptible power source. Another solution is to provide enough on-board battery power for one emergency stop, and to design the propulsion system so that adequate braking can be obtained through such batteries. A third solution is to have a separate wayside braking system in the entry of each station that can be actuated by the zone controller.

Consider the battery requirement for one stop: The gross mass of the PRT vehicle is about 750 kg. Assuming a speed of 13 m/s, the amount of kinetic energy that must be dissipated while stopping is

$$K.E. = \frac{mV^2}{2} = \frac{750kg \times (13m/s)^2}{2} = 63.4kJ \times 1kcal / 4.183kJ = 15.2kcal$$

Assume that the efficiency of braking through the motors is only 40%. Then 38 kcal of energy must be dissipated. This is the amount of energy required to raise 1 kg of water (a cube 10 cm on a side) 38°C. In terms of battery requirements, at $a_e = 0.4g$ the time to stop from 13 m/s suddenly without considering comfort jerk is 3.3 sec. During this time, the average power level would be $63.4/3.3 = 19.2$ kW. This corresponds to 32 amps at 600 volts for 3.3 sec, or 800 amps at 24 volts for 3.3 sec, clearly much more demanding for a low-voltage on-board battery than for wayside power. Thus, to serve as a backup braking system, the on-board battery must be a series of enough plates to obtain enough voltage so that the current is reasonable. If the required on-board current cannot be achieved, an uninterruptible power circuit on the station-input

guideway should be used to supply propulsive power on that critical segment.

12. Summary

Design Features Required for Minimum Safe Headway:

- Checked dual redundancy in vehicle and wayside controllers using fault-tolerant computers.
- Bi-stable, in-vehicle, conservatively designed switch mechanism.
- Switch torquer shielded against stray voltage pulses.
- Virtually instantaneous back-up power for propulsion and braking.
- Carefully designed, non-breakable power-pickup shoes.
- Frictionless propulsion and primary braking, i.e., linear electric motors.
- No-power-on, no-power-off auxiliary braking against the primary running surface.

Table 1. Summary of Mean Times to Failure

FAILURE	Mean Time To Event, years
On-Board Computer System	400 billion billion
On-Board Communications System	137,000
On-Board Encoder System	214,000
On-Board Propulsion System	700,000
Vehicle incapable of moving	75,000
Pushing incidents w/ 500 vehicles	150
Zone Controller	30 billion billion
Vehicle-to-Vehicle Collision	1000 billion
Diverge Junction Collision	to long to estimate
Merge Collision	10,000 billion
Life Time of Universe	13 billion

13. Conclusions

The long-term promise of the new optimized means for urban mobility lies in safe, practical use of headways under one second. To achieve such headways, it is necessary to design the system so that the probability of failure acceleration greater than practical for emergency braking is extremely remote. Such design has been achieved through careful failure-modes-and-effects analysis and with use of practical design features that result from such analysis. Such features are described. With them, the collision frequency in PRT will be lower than in the U. S. automobile system by a factor of more than 10 trillion.

14. References

- Anderson, J. E. 1978. *Transit Systems Theory*. Lexington Books, D. C. Heath and Company.
- Anderson, J. E. 1984. "Optimization of Transit-System Characteristics," *Journal of Advanced Transportation*, 18:77-111.
- Anderson, J. E. 1988. "Safe Design of Personal Rapid Transit Systems,"

Journal of Advanced Transportation, 28:1-15.

Anderson, J. E. 1997. "Essentials of Personal Rapid Transit," *Infrastructure*, 2:8-17.

Anderson, J. E. 1998a. "Control of Personal Rapid Transit Systems,"
Journal of Advanced Transportation, 32:57-74.

Anderson, J. E. 1998b. "Personal Rapid Transit: Matching Capacity to Demand."
An Advanced Transit Association Information Paper.

Anderson, J. E. 2000. "A Review of the State of the Art of Personal Rapid Transit."
Journal of Advanced Transportation, 34:3-29.

Irving, Jack H., Bernstein, Harry, Olson, C. L. and Buyan, Jon. 1978. *Fundamentals of Personal Rapid Transit*. Lexington Books, D. C. Heath and Company.

Lang, R. P. and Warren, D. J. 1983. Microprocessor Based Speed and Position Measurement System, 33rd Vehicular Technology Conference, IEEE Technical Paper.

Milnor, R. C. and Washington, R. S. 1984. Effects of System Architecture on Safety and Reliability of Multiple Microprocessor Control Systems. 34th Vehicular Technology Conference, IEEE Technical Paper.

Appendix A. **Truck Hitting a Guideway-Support Post**

Assume the bolts holding the guideway at the bottom are designed for 120 mph crosswind.

$$\text{Crosswind force} = F_w = \frac{1}{2} \frac{\rho g}{g} V_w^2 C_D A$$

$\rho g = 0.080 \text{ lb} / \text{ft}^3 = \text{weight of air per cubic ft}$

$V_w = 120 \text{ mph} (88 / 60) = 176 \text{ ft} / \text{sec}$

$C_D = 2 = \text{conservative drag coefficient. With guideway covers it will be less than 1.}$

$A = 3 \text{ ft deep} \times 90 \text{ ft span} = 270 \text{ ft}^2 = \text{area of one span of guideway}$

$$F_w = \frac{0.080}{64.4} (176)^2 (2)(270) = 20,780 \text{ lb}$$

Moment at base = $F_w(\text{Post Length} + 0.5 \text{ Guideway depth}) = 13,860[16 + .5(3)] = 364,000 \text{ ft-lb}$

Assume the post is held in place by four bolts spaced at four corners 2 ft apart.

Then the lifting force on one of the two bolts that would be in tension is

$$242,550 \text{ ft-lb} / (2 \text{ ft})(2 \text{ bolts}) = 90,910 \text{ lb.}$$

From Marks Handbook, the bolt diameter required to resist this load is 3 ½ in.

What truck momentum is required to knock out a post?

The impulsive force = mass × acceleration = ma = Weight × a/g.

The stopping distance at constant deceleration a is $S = V^2 / (2a)$ or $a = V^2 / (2S)$.

For example, assume a 10-ton truck hits a post at 30 mph or 44 ft/sec and stops after crushing a distance of 4 ft.

Then

$$F = \frac{20,000lb}{32.2ft/s^2} \times \frac{(44ft/sec)^2}{8ft} = 150,300 lb$$

Per Marks Handbook, the shear strength of the 3 ½ in bolt is 70,750 lb, or for four bolts 283,000 lb.

So to shear the bolts, the 10-ton truck speed would have to be

$$30 mph \times \sqrt{\frac{283,000}{150,300}} = 41 mph.$$

On the other hand, if the truck weighed a legal limit of 80,000 lb, at 21 mph it would shear the bolts.

The posts will be octagonal and tapered with 20-in diameter at the base and 10-in diameter at the top, and will be fabricated from 5/16-in-thick structural steel. They will be difficult to crush. To make it more difficult to crush the post, it could be filled with concrete, at least near the base. Testing will be required to determine if this would be desirable.

The conclusion is thus that in almost every reasonable case, the consequence of a truck hitting a post head on is that the truck will be demolished with no damage to the post. A glancing blow, more likely, would cause less damage. If there is a possibility of a truck or car hitting a post, the prudent course is to place an ordinary highway barrier on the street side of the post to provide a greater degree of safety for the car or truck. In addition, a cable of suitable strength could be placed inside the guideway to take up the load if one post were knocked out.

Appendix B Tree Falling Across Guideway and Stopping a Vehicle Instantly

As soon as the system registers a sudden anomalous speed reduction of any vehicle, the vehicles behind are commanded to stop at a suddenly applied braking rate a_e a braking time constant t_c after sensing slowdown. The distance to slow down from line speed V_L to speed V is given by the equation

$$D = V_L t_c + \frac{V_L^2 - V^2}{2a_e} \quad (B-1)$$

Consider a stream of vehicles each of length L moving at speed V_L spaced a distance $V_L T_h$ apart, where T_h is the time headway. Then the nose-to-tail spacing between these vehicles is $V_L T_h - L$. So the close-up distance of the first vehicle behind the one stopped suddenly by the tree falling across the guideway is $V_L T_h - L$. The close-up distance available to the second vehicle is $2(V_L T_h - L)$, to the third $3(V_L T_h - L)$, and to then n -th vehicle $n(V_L T_h - L)$. Thus, substituting $D = n(V_L T_h - L)$ into equation (B-1), the speed V_n at which the n -th vehicle behind collides with the vehicle that is stopped instantly is

$$V_n = \sqrt{V_L^2 - 2a_e[n(V_L T_h - L) - V_L t_c]} \quad (B-2)$$

Garrard, Caudill and Rushfeldt³ studied the conditions under which people unfortunate enough to experience a collision while in a PRT vehicle will survive without serious injury. In so doing they made use of the extensive literature available on automobile safety in a yearlong study that included visits to Ford and General Motors proving grounds.

³ W. L. Garrard, R. J. Caudill, and T. L. Rushfeldt, "Crashworthiness and Crash Survivability for Personal Rapid Transit Vehicles," *Personal Rapid Transit III*, University of Minnesota, June 1976.

They found that the criterion to estimate possible injury used by the automobile companies is called the Severity Index (SI), which is given by the equation

$$SI = \int_0^{\Delta t} a(t)^{2.5} dt \quad (B-3)$$

in which $a(t)$ is the acceleration of the occupant's chest in g 's, t is time, and Δt is the duration of the collision of the passenger with a padded surface, which could also be an airbag or a seatbelt. With time in seconds, SI has units of seconds. Anderson [1978], on page 190, showed that the acceleration profile during the collision is such that equation (B-3) can be integrated to give

$$SI = 0.74V_{cp}^{2.5} \quad (B-4)$$

in which V_{cp} is the speed at which the passenger collides with the padded surface in meters per sec.

We assume that the passenger in the n -th vehicle collides with the padded dashboard at the speed V_n . Use of equation (B-4) implies that the vehicle is equipped with adequate energy-absorption devices, and for extreme cases, a crushable nose. Reference 2 reported that from data obtained in the Automobile Safety Programs, if $SI < 500$ sec "only minor injuries will occur." From equation (B-4), $SI = 500$ sec corresponds to $V_{cp} = 13.8$ m/s = 30.3 mph. V_n from equation (B-2) and the corresponding SI from equation (B-4) are shown in Table B-1 for $L = 8.5$ ft (the length of the vehicle), $t_c = 0.1$ sec (appropriate for the type of control system used in PRT), $a_e = 0.6$ g (a generally accepted emergency braking rate), and $V = 30$ mph. Note that if the headway is 0.5 sec, four vehicles behind the one stopped collide at successively smaller speeds; if headway is 0.6 sec three vehicles behind will collide; if headway is 0.7 or 0.8 sec, two vehicles will collide; and for larger headways only one vehicle will collide. Further analysis shows that, if headway is 1.5 sec or greater, no vehicles will collide. It is seen that in this extreme case in which a tree limb large enough to stop a vehicle instantly falls across the guideway, a conservative conclusion is that if the line speed is 30 mph or less, only the people in the car hit by the tree will be injured.

Table B-1. The Collision Speed and Severity Index for Vehicles Behind a Vehicle Suddenly Stopped.

Headway	n	Collision speed	SI
sec		mph	sec
0.5	1	27.1	379.5
0.5	2	22.2	230.5
0.5	3	15.9	99.3
0.5	4	3.1	1.7
0.6	1	25.6	329.3
0.6	2	18.3	142.5
0.6	3	3.9	3.0
0.7	1	24.1	280.7
0.7	2	13.4	64.5
0.8	1	22.4	233.6
0.8	2	4.5	4.3
0.9	1	20.5	188.4
1.0	1	18.5	145.3