9 Redundancy, Failure Modes and Effects, and Reliability Allocation

9.1 Introduction

In the previous chapter, an equation for allocation of required subsystem reliability (equation (8.8.3, 8.8.4) was derived, thus providing a basis for allocating reliability requirements of the subsystems of a system in such a way that the system life cycle cost is minimized, subject to the constraint of a specified level of service unavailability. The theory requires classification of failure modes and determination of failure effects in terms of the delay times and the number of people involved in each failure. This task is outlined in the present chapter in enough detail to clarify the general method and to provide some numerical estimates of the reliability requirements.

In classification of failure modes for analysis of system reliability, failures are identified not according to which specific part fails, but according to the consequences in terms of person-hours of delay. Consequently, it is possible to aggregate many components and sub-subsystems into the set of subsystems specifically identified in equations (8.8.3, 8.8.4). For example, the entire vehicle can be considered as a subsystem possessing the failure classes defined in section 8.4. As discussed in section 8.9, if the failure of any one of K components or subsystems causes an m-class failure of the nth type of subsystem, then $MTBF_{mn}$ is given in terms of component failures by equation (8.9.1). This equation simply states that the failure rate of failures of the "mn" class is the sum of the failure rates of components that can cause it, that is, the probability of an "mn" failure is the sum of the probabilities of independent events that can cause it.

Equation (8.9.1) is the series law of failures. The corresponding parallel law is obtained by building redundancy into the system if the required value of $MTBF_{mn}$ cannot economically be achieved by single components or subsystems. The theory of redundancy is developed in the next section. Then, a set of subsystems of a transit system is defined and specific types of failure classes are considered in order to determine for each generally applicable formulas for the number of person-hours of delay. As a point of interest, the theoretical construct is then used to consider the problem of the most appropriate type of mechanism for escape from vehicles in case the need should arise. Finally, the various components of the theory are assembled to give a specific example of its application to the problem of reliability allocation.

9.2 Redundancy

A subsystem is redundant if two or more parallel units (components or subsystems) exist and if each is able to perform the function required of the subsystem without interference from the failed element, but possibly with minor degradation in service. Let $MTBF_u$ be the mean time between failures of ~~either~~ each of the two parallel units. Then, the mean time between failures of either of the two units is $MTBF_u/2$.

Let τ be the time interval following a failure during which the failure of the second parallel unit is critical. If the subsystem is aboard a vehicle, τ is the mean time interval following the first failure required to get the vehicle off the line and into the maintenance shop; if the subsystem is at wayside, τ is the mean time required to fix it or replace it. If the entire system is to operate satisfactorily, it is necessary that

$$\frac{MTBF_u}{\tau} >> 1$$

If predictable failures due to wearing out of parts are eliminated by replacing all such parts at a fraction of their *MTBF*s, the remaining failures occur randomly and $MTBF_u/\tau$ can be interpreted as the number of subintervals τ during which the failure of a redundant element could with equal probability occur within the time interval $MTBF_u$. The failure of the second element of a redundant pair during τ then has a probability equal to twice the failure rate of a single unit divided by the number of time intervals $MTBF_{ss}/\tau$ in which, with equal probability, the second unit could fail. In other words, the *MTBF* of both elements of the redundant pair is increased from $MTBF_u/2$ by the ratio $MTBF_u/\tau$. If $MTBF_{ss}$ is the mean time between failures of both elements of a redundant pair less than τ apart, that is, of the subsystem consisting of two parallel units,

$$MTBF_{ss} = \frac{MTBF_u^2}{2\tau} \qquad (9.2.1)$$

For example, if $MTBF_u$ is 100 hours so that on the average the failure of either of two units occurs once in 50 hours, and τ is 0.1 hour, there are 1000 time intervals each of length 0.1 hour during which the second failure could occur. Only if failure of the second element occurs in the specific interval immediately following failure of the first element, is a double failure of consequence. Thus $MTBF_{ss} = 50(1000) = 50{,}000$ hours.

The benefit of redundancy in systems that can be maintained at frequent intervals is enormously increased over that in systems, such as spacecraft, in which τ is essentially infinite. Thus the economics of redundancy in transit systems with failure monitoring is much different from that experienced in the aerospace field.

Trains

An example of redundancy in transit systems is the coupling of cars into trains so that failure of one car does not cause a line stoppage. In a two-car train, the mean time to failure of both cars within less than τ units of time is, from equation (9.2.1),

$$MTBF_{T_2} = \frac{MTBF_{car}^2}{2\tau} \tag{9.2.2}$$

In a three-car train, the *MTBF* for failure of any of the three cars is $MTBF_{car}/3$. The probability of failure of either of the remaining cars within the interval τ is $2\tau/MTBF_{car}$. Therefore the *MTBF* for failure of two cars within less than τ is

$$\left(\frac{MTBF_{car}}{3}\right)\left(\frac{MTBF_{car}}{2\tau}\right)$$

The second car fails anywhere in the interval τ, therefore at a mean time 0.5τ following the first failure. The third car must carry the train the remaining time 0.5τ to the maintenance depot. The probability of its failure before arrival is $0.5\tau/MTBF_{car}$. Therefore, the *MTBF* of all cars in the train before it can arrive at the maintenance depot is

$$MTBF_{T_3} = \frac{2MTBF_{car}^3}{3 \cdot 2\tau^2} \tag{9.2.3}$$

By a similar analysis

$$MTBF_{T_4} = \frac{(2 \cdot 4)MTBF_{car}^4}{4!\tau^3} \tag{9.2.4}$$

and it follows that

$$MTBF_{T_n} = \left(\frac{2 \cdot 2^2 \cdot 2^3 \ldots \cdot 2^{n-2}}{n!}\right)\tau\left(\frac{MTBF_{car}}{\tau}\right)^n \tag{9.2.5}$$

in which we can write

$$2 \cdot 2^2 \cdot \ldots \cdot 2^{n-2} = 2^{(1+2+\ldots+n-2)} = 2^{(n-2)(n-1)/2}$$

It is of course recognized that the performance of an n-car train in which only one car is operative may be marginal; but the train can be kept moving, thus considerably reducing the passenger delay from the case in which the train stops. If $MTBF_{T_n}$ is given from system considerations (use of equations (8.8.3, 8.8.4)), the mean time to failure of each car must from equation (9.2.5) be

$$MTBF_{car} = \tau\left[\frac{n!\,MTBF_{T_n}}{2^{(n-2)(n-1)/2}\tau}\right]^{1/n} \tag{9.2.6}$$

Trains in Loop Systems

Consider a transit system in which N_t trains of n cars each move between on-line stations around a loop. A failure of any of the N_t trains causes shutdown of the system. Thus, from equation (9.2.5) the mean time between system shutdowns, $MTBF_{S_1}(N_t|n)$, is

$$MTBF_{S_1}(N_t|n) = \left[\frac{2^{(n-2)(n-1)/2}}{n!}\right]\frac{\tau}{N_t}\left(\frac{MTBF_{car}}{\tau}\right)^n \tag{9.2.7}$$

If the loop consists of two counterrotating one-way system, each of N_t trains of n cars, the system mean time between failures is found by substituting equation (9.2.7) for $MTBF_u$ in equation (9.2.1). Thus for a two-way loop,

$$MTBF_{S_2}(N_t|n) = \frac{MTBF^{\,2}_{S_1}(N_t|n)}{2\tau} \tag{9.2.8}$$

Suppose the system is designed so that $MTBF_{S_1} = 3000$ h or approximately one year. Suppose further that the mean time between inspections for failures is $\tau = 10$ hr. Then

$$MTBF_{S_2} = \frac{(3000)^2}{20} = 150 \text{ years} \tag{9.2.9}$$

if we assume 3000 hours of operation per year.

Now consider the problem of estimating the required *MTBF*of a single car in a train of cars. The equation for required *MTBF* is equation (8.8.3, 8.8.4). Let each of the N_t trains be the subsystems. Then, as a first approximation, assume that the N_t trains are the only subsystems in a one-way loop system, and that there is only one class of failure—a train stops. Then there is only one term in the summation of equation (8.8.4) and $\Sigma_{mn} = 1$. For the subject configuration, $N_v = N_t$, τ_{mn} is the mean time to restore service (*MTRS*) when a train fails, and n_{mn} is *MTRS* times the average total flow of people per hour into the system, t_h. Thus equation (8.8.3) becomes

$$MTBF_{T_{\text{req}}} = \frac{t_h(MTRS)^2 N_t T_v}{\epsilon_{\text{spec}} PH_{yr}} \tag{9.2.10}$$

$MTBF_{T_{\text{req}}}$ is the required *MTBF* of a single train. To find the vehicle *MTBF* substitute $MTBF_{T_{\text{req}}}$ for $MTBF_{T_n}$ in equation (9.2.6), in which τ is the time interval between trips to the maintenance shop for inspection. Then the required MTBF of each car in a one-way loop is

$$MTBF_{\text{car}_{\text{req}}} = \tau \left[\frac{n! t_h (MTRS)^2 N_t T_v}{2^{(n-2)(n-1)/2} \tau \epsilon_{\text{spec}} PH_{yr}} \right]^{1/n} \tag{9.2.11}$$

But from equation (8.2.4) PH_{yr} is the number of person-hours of travel per hour multiplied by the number of hours of travel per year. The latter quantity is simply T_v, therefore ?

for demand responsive systems only

$$PH_{yr} = (t_h T_{\text{trip}}) T_v \tag{9.2.12}$$

in which t_h is the number of trips per peak hour, and T_{trip} is the average trip time. Thus, equation (9.2.11) becomes

$$MTBF_{\text{car}_{\text{req}}} = \tau \left[\frac{n!(MTRS)^2 N_t}{2^{(n-2)(n-1)/2} \tau \epsilon_{\text{spec}} T_{\text{trip}}} \right]^{1/n} \tag{9.2.13}$$

In a typical case, assume τ = one day or 10 hours of operation of an average vehicle, $MTRS$ = 1 hr, T_{trip} = 6 min (0.1 hr), and $\epsilon_{\text{spec}} = 0.01$. Then

$$MTBF_{\text{car}_{\text{req}}} = 10 \left[\frac{100 n! N_t}{2^{(n-2)(n-1)/2}} \right]^{1/n} \tag{9.2.14}$$

For comparison, consider two cases: (1) There are five two-car trains (N_t = 5, n = 2); and (2) the ten cars operate as individual units (N_t = 10, n = 1). Then

$$MTBF_{car_{req}} = 316 \text{ hr if } N_t = 5,\ n = 2$$

$$= 10{,}000 \text{ hr if } N_t = 10,\ n = 1$$

As a matter of interest, the meaning of ϵ_{spec} in terms of $MTBF_{S_1}$ (equation (9.2.7)) is found from the equation

$$MTBF_{S_1} = \frac{MTBF_{T_{req}}}{N_t} = \frac{(MTRS)^2}{\epsilon_{spec} T_{trip}} \tag{9.2.15}$$

in which the second expression is from equation (9.2.10) with equation (9.2.12) substituted.

Using the numerical values below equation (9.2.13)

$$MTBF_{S_1} = 1000 \text{ hours}$$

or one failure every 100 days. If τ = 10 hr, as before, equation (9.2.8) gives

$$MTBF_{S_2} = \frac{(1000)^2}{20} = 50\ MTBF_{S_1}$$

The dramatic effect of redundancy on the vehicle *MTBF* required to achieve a given level of service availability is very apparent.

Single Vehicles in Loop Systems

In the above calculations, it was assumed that n is the number of cars per train. Suppose the cars in a loop system operate singly but that each critical subsystem aboard a car is fully redundant. Then N_t is the number of individual cars, N_v, and n = 2. From equation (9.2.13), the required *MTBF* is proportional to $N_v^{1/2}$. In small-vehicle systems, using all of the numerical values in the previous paragraph, $MTBF_{req}$ for each individual subsystem tends to be too high to be practical. The apparent difficulty can be solved, however, by examining equation (9.2.13) for n = 2:

$$MTBF_{r.e.} = (MTRS)\left(\frac{2\tau N_v}{\epsilon_{spec} T_{trip}}\right)^{1/2} \qquad (9.2.16)$$

in which $MTBF_{r.e.}$ is the *MTBF* of the redundant element.

$MTBF_{r.e.}$ can be reduced if the system can be designed in such a way that both *MTRS* and τ are reduced. The time τ the vehicle is on line with a failed redundant element can be reduced by introducing an independent failure-monitoring system, the failure of which will itself signal that the vehicle should be taken off the line. With a failure-monitoring system, τ becomes the time required to get the vehicle off the line and into the maintenance shop following indication of failure of one of the redundant systems or of the failure monitor. In this circumstance, $\tau \doteq T_{trip}$, and equation (9.2.16) reduces to

$$MTBF_{r.e.} = (MTRS)\left(\frac{2N_v}{\epsilon_{spec}}\right)^{1/2} \qquad \text{(loop systems with failure monitoring)} \qquad (9.2.17)$$

MTRS, on the other hand, is the mean time to restore service in the case of failure of both redundant elements. To reduce *MTRS* to an acceptable value, it is necessary to introduce a means of rapid removal of a failed vehicle from the line. In a thoughtfully designed system, the vehicle will be pushable in almost all cases. Therefore, an automated pushing (or pulling) mode activated by the on-board failure-monitoring system should be added to the vehicle. (The availability of microprocessors permits the introduction of such devices on board each vehicle at modest cost.) With such a device, it is reasonable to reduce *MTRS* to the order of one minute, that is, $MTRS = 1/60$ hr. For say $N_v = 300$ vehicles, $MTRS = 1/60$ hr, and $\epsilon_{spec} = 0.01$; equation (9.2.17) gives $MTBF_{r.e.} = 4$ hours. Since this is a very modest *MTBF*, much smaller unavailability is possible. For example, for $\epsilon_{spec} = 10^{-6}$, $MTBF_{r.e.} = 400$ hours required.

Single Vehicles in Network Systems

For network systems using single vehicles, it is necessary to recall that in equations (9.2.10) and (9.2.11), the appearance of t_h in the numerator was based on the assumption that the number of people involved in a failure is $(MTRS)t_h$. This is true in a loop in which *MTRS* is long enough so that all vehicles are stopped. In a loop in which *MTRS* is short, the number of people involved in a failure is more nearly $MTRSf_{av}$, whose f_{av} is the average line flow. Thus, if equation (9.2.17) is applied to cases in which

MTRS is small or to a network system in which only a portion of the flow is delayed, it should be replaced by

$$MTBF_{\text{r.e.}} = (MTRS)\left(\frac{2N_v f_{\text{av}}/t_h}{\epsilon_{\text{spec}}}\right)^{1/2} \tag{9.2.18}$$

In loop systems, $f_{\text{av}}/t_h = 0.5$ if the average trip goes half way around the loop, and the *MTBF* requirement is reduced $\sqrt{2}$.

In network systems, equation (4.5.19) gives

$$\frac{f_{\text{av}}}{t_h} = \frac{L\langle L_t\rangle}{2\beta A}$$

and, from equation (4.5.17),

$$N_v = \frac{\bar{t}_h A\langle L_t\rangle}{p_v f_p V_{\text{av}}}$$

in which $\bar{t}_h$ is the hourly trip density and A is the network area. With these substitutions, equation (9.2.18) becomes

$$MTBF_{\text{r.e.}} = (MTRS)\langle L_t\rangle\left(\frac{\bar{t}_h L}{p_v f_p V_{\text{av}}\beta\epsilon_{\text{spec}}}\right)^{1/2} \tag{9.2.19}$$

From figure 4-18 assume that for a large network

$$\langle L_t\rangle \approx 0.8A^{1/2} \tag{9.2.20}$$

Then, as a specific example, assume $MTRS = 1/60$ hr, $A = 256\ \text{km}^2$, $L = 0.8$ km, $p_v f_p = 1$, $\beta = 1$, $V_{\text{av}} = 50$ km/hr, and $\epsilon_{\text{spec}} = 10^{-4}$. Then $\langle L_t\rangle = 12.8$ km, and

$$MTBF_{\text{r.e.}} = 27\bar{t}_h^{\,1/2} \tag{9.2.21}$$

if $\bar{t}_h$ is the trip density in trips per hectare. From figure 5-7, assume $\bar{t}_h = 60$ trips per hectare (15,000 trips per square mile) is an upper limit on patronage. Then $MTBF_{\text{r.e.}} = 209$ hours. Based on the work of C.L. Olson[1], this is a modest *MTBF*. If, however, a lower requirement is desirable, equation (9.2.19) shows that a lower value can be obtained by reducing *MTRS* below one minute. The work of Bernstein and Schmitt[2] indicates that a value

$MTRS = 15$ seconds may not be unreasonable, thus reducing $MTBF_{req}$ by a factor of four. $MTBF_{req}$ could be further reduced by reducing the ratio of τ to average trip length (see equation (9.2.16)). This can be done by dispersing small maintenance facilities throughout the network, but is probably not needed.

The above analysis shows that in large networks the simple expedients of

1. Redundancy in critical elements
2. Failure monitoring
3. Automated pushing

will reduce the *MTBF* requirements to readily obtainable levels, even if the time delays due to failure are of the order of 0.01 percent of travel time. This figure means that one hour of delay is experienced in 10,000 hours of travel. If the average regular user of the system takes 10 work trips per week of 15 minutes each for 50 weeks a year, the number of hours of travel per year is 125 hours. Assuming on that basis a total of 200 hours travel per year, $\epsilon = 10^{-4}$ means an accumulation of one hour of delay per person in 50 years.

The above analysis is of course preliminary since it neglects all wayside subsystems. Also, note from equation (8.9.2) that the *MTBF* requirements of the various individual vehicle-borne subsystems are higher than the above figures in proportion to the number of them.

9.3 Subsystems and Classes of Failure

In section 9.2, *MTBF* requirements were developed under the simplifying assumption that any wayside equipment is infinitely reliable. In a complete analysis, it is of course necessary to account for the finite reliability of wayside subsystems. As indicated in section 8.9 the subsystems should be defined as the largest units in the system for which meaningful values of person-hours of delay ($n\tau$) due to each class of failure can be defined. Thus define the following types of equipment as the "subsystems":

1. Vehicles
2. Station entry monitoring equipment
3. Passenger processing equipment in stations
4. Merge point equipment
5. Diverge point equipment
6. Central communications and control equipment

For each of these subsystems, the classes of failure have to be defined separately. For the vehicle subsystem, the classes will be taken as those defined in section 8.4. For the remaining subsystems, the classes will be defined below.

The above analysis and that which follows is designed to apply to any type of transit system including systems with manually operated vehicles. In simpler systems certain terms are set to zero, as will be apparent.

9.4 Vehicle Failures

As indicated above, the classes of vehicle failure will be taken as those defined in section 8.4.

Class 1 Failures

In Class 1 failures, the number of persons involved in a failure is just the average number of persons per vehicle. Thus

$$n_{11} = p_v$$

The time delay, τ_{11}, is the time required to stop at a station, wait for a second vehicle, and resume the journey. Thus

$$n_{11}\tau_{11} = p_v\left(\frac{2V_L}{a} + t_{sd}\right) \tag{9.4.1}$$

in which t_{sd} is the station delay time.

Class 2 Failures

In Class 2 failures, the vehicle slows down, therefore all people in a string of vehicles that slows down are delayed. The number of person-hours of delay, $n_{12}\tau_{12}$, can be found by considering figure 9-1.
Assume that a vehicle slows down from line speed V_L to a speed V^* and cruises at V^* for a distance D^* at which time it leaves the main track. At this point, neglect the deceleration period. Then the time at which it leaves the main track is $t^* = D^*/V^*$. The time delay on line is

$$\Delta t_1 = t^* - t_a$$

$$= \frac{D^*}{V_L}\left(\frac{V_L}{V^*} - 1\right) \tag{a}$$

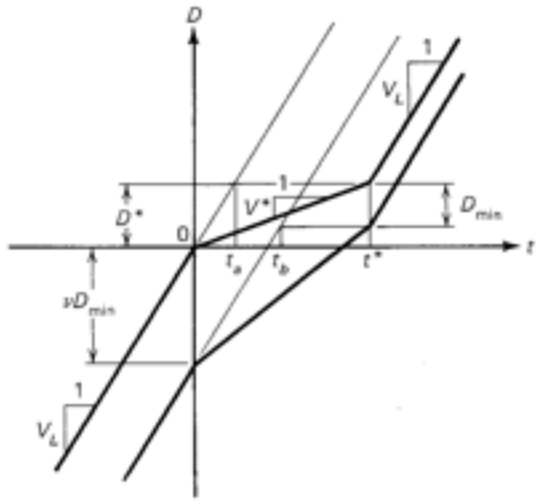

Figure 9-1. Distance-Time Diagram Used to Compute the Time Delay due to Slowdown of a Vehicle

in which $t_a = D^*/V_L$ is the time required to traverse D^* at V_L. In these calculations, neglect of jerk introduces an insignificant error, and the neglect of the acceleration periods can be accounted for by considering V^* to be the reduced velocity in the case of infinite deceleration. In significant cases, the error in neglecting the effect of finite deceleration is small. The passengers in vehicle 1 lose the additional time given by equation (9.4.1).

Assume a second vehicle is travelling a distance νD_{min} behind the first vehicle. D_{min} is the minimum nose-to-nose distance between vehicles and ν > 1. Then, at $t = 0$ (neglecting control lags) the second vehicle slows to a speed such that it achieves the minimum spacing, D_{min}, at time t^*. (The velocity profile is of no consequence.) The time lost by the second vehicle is

$$\Delta t_2 = t^* - t_b$$

$$= \frac{D^*}{V_L}\left[\frac{V_L}{V^*} - 1 - (\nu - 1)\frac{D_{min}}{D^*}\right] \qquad \text{(b)}$$

$$= \Delta t_1 - (\nu - 1)\frac{D_{min}}{V_L}$$

in which $t_b = (D^* - D_{min} + \nu D_{min})/V_L$.

Assume a cascade of vehicles each spaced a distance νD_{min} apart. Then the time delay of the ith vehicle, Δt_i, is found by replacing D_{min} by $(i - 1)D_{min}$ in equation (b). Thus

$$\Delta t_i = \frac{D^*}{V_L}\left[\frac{V_L}{V^*} - 1 - (i-1)(\nu - 1)\frac{D_{\min}}{D^*} \right] \tag{c}$$

$\Rightarrow \Delta t_1 - (i-1)(\nu-1)\frac{D_{\min}}{V_L}$

The number of vehicles delayed n is found by assuming $\Delta t_{n+1} = 0$. Thus

$$n = \frac{1}{(\nu - 1)}\frac{D^*}{D_{\min}}\left(\frac{V_L}{V^*} - 1 \right) \tag{d}$$

If the average number of people per vehicle is p_v, the total number of person-hours of delay is

$$n_{12}\tau_{12} = p_v\left(\sum_{i=1}^{n} \Delta t_i + \frac{2V_L}{a} + t_{sd} \right) \tag{e}$$

Substituting equation (c), and performing the summation,

$$n_{12}\tau_{12} = \frac{P_v D^*}{V_L}\left[\left(\frac{V_L}{V^*} - 1 \right) n - (\nu - 1)\frac{D_{\min}}{D^*}\frac{n(n-1)}{2} \right] + p_v\left(\frac{2V_L}{a} + t_{sd} \right) \tag{f}$$

Substituting equation (d)

$$n_{12}\tau_{12} = \frac{D^{*2}P_v}{2(\nu - 1)V_L D_{\min}}\left(\frac{V_L}{V^*} - 1 \right)\left[\frac{V_L}{V^*} - 1 + (\nu - 1)\frac{D_{\min}}{D^*} \right] + p_v\left(\frac{2V_L}{a} + t_{sd} \right) \tag{g}$$

In most cases, the ratio $D_{\min}/D^*$ is much less than 1. Also note that the average flow f_{av} is

$$f_{av} = \frac{V_L p_v}{\nu D_{\min}} \tag{9.4.2}$$

With these substitutions, equation (g) becomes

$$n_{12}\tau_{12} = \frac{\nu}{2(\nu - 1)}\left(\frac{D^*}{V_L}\right)^2\left(\frac{V_L}{V^*} - 1\right)^2 f_{av} + p_v\left(\frac{2V_L}{a} + t_{sd}\right) \tag{9.4.3}$$

Only the first term is in the form of a flow multiplied by a time delay squared (see equation (8.7.3)), but this is usually the dominant term.

It has been mentioned that the above analysis neglected the finite time required to change speed from V_L to V^*. Examination of the above analysis shows that if the position-time curve of vehicle 1 in figure 9-1 resumes speed V_L at t^*, the only change is that in equation (9.4.3) V_L/V^* is replaced by

$$\frac{V_L}{V^*} \rightarrow \frac{V_L}{V^*_{act}}\left[1 - \frac{(V_L - V^*_{act})^2}{aD^*}\right]$$

in which V^*_{act} is the actual reduced line speed. It is seen that the correction is small if D^* is large compared with twice the stopping distance from a speed $V_L - V^*_{act}$.

Class 3 Failures

In Class 3 failures, the failed vehicle, denoted vehicle 1, is assumed to stop on the guideway. Vehicle 2, behind it, stops and then pushes it up to line speed. Vehicles 3, 4, and so on slow down, may stop, and then resume line speed. The position-time diagrams are idealized in figure 9-2. Assume that before failure, a cascade of vehicles travelling at velocity V_L is spaced at an average nose-to-nose distance of νD_{min} where, as before, D_{min} is the minimum nose-to-nose spacing. Vehicle 1 stops at $t = 0$. It waits until vehicle 2 can stop behind it and push it back to line speed. Vehicle 2 stops $\nu D_{min}/V_L$ units of time later. The stopping time is approximately V_L/a, where a is the deceleration rate. Therefore, counting the time required to stop and to resume speed, vehicle 2 is delayed $2V_L/a$ plus the delay time τ_p required for operation of the pushing mode. With these considerations,

$$\Delta t_1 = \frac{\nu D_{min}}{V_L} + \frac{2V_L}{a} + \tau_p + \tau_{11} \tag{a}$$

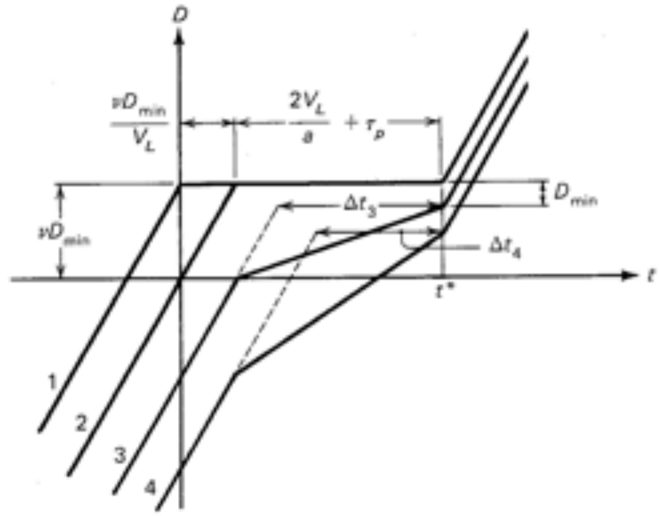

Figure 9-2. Position-Time Diagrams for Pushable Failure

in which τ_{11} (equation (9.4.1)) is added to account for the additional delay of passengers in vehicle 1 in transferring vehicles in the station nearest the failure. Similarly,

$$\Delta t_2 = \frac{2V_L}{a} + \tau_p + \tau_{11}$$

In analogy with the analysis of Class 2 failures,

$$\Delta t_3 = \frac{2V_L}{a} + \tau_p - (\nu - 1)\frac{D_{min}}{V_L} \tag{c}$$

$$\Delta t_i = \frac{2V_L}{a} + \tau_p - (i-2)(\nu - 1)\frac{D_{min}}{V_L}, \quad i = 3, 4, \ldots \tag{d}$$

If n is the total number of vehicles delayed, the $(n + 1)$th vehicle is not delayed. Therefore,

$$\Delta t_{n+1} = 0 = \frac{2V_L}{a} + \tau_p - (n-1)(\nu - 1)\frac{D_{min}}{V_L}$$

and

$$n - 1 = \left(\frac{2V_L}{a} + \tau_p \right) \frac{V_L}{(\nu - 1)D_{\min}} \tag{e}$$

If, as above, the average number of people per vehicle is p_v, and we take note of equation (9.4.1),

$$n_{13}\tau_{13} = p_v \left(\sum_{i=3}^{n} \left[\frac{2V_L}{a} + \tau_p - (i - 2)(\nu - 1) \frac{D_{\min}}{V_L} \right] \right. \tag{f}$$
$$\left. + 6V_L/a + 2t_{sd} + \tau_p + \nu D_{\min}/V_L \right)$$

If the sums of equation (f) are placed in closed form,

$$n_{13}\tau_{13} = p_v \left\{ (n - 1) \left[\frac{2V_L}{a} + \tau_p - \frac{(\nu - 1)D_{\min}}{2V_L} (n - 2) \right] \right.$$
$$\left. + \frac{6V_L}{a} + 2t_{sd} + \tau_p + \frac{\nu D_{\min}}{V_L} \right\} \tag{g}$$

Substituting equation (e) and simplifying the algebra

$$n_{13}\tau_{13} = p_v \left[\frac{V_L}{2(\nu - 1)D_{\min}} \left(\frac{2V_L}{a} + \tau_p \right)^2 \right.$$
$$\left. + \frac{7V_L}{a} + 3/2\, \tau_p + 2t_{sd} + \frac{\nu D_{\min}}{V_L} \right]$$

Finally, substitute equation (9.4.2). Then

$$n_{13}\tau_{13} = \frac{\nu}{2(\nu - 1)} \left(\frac{2V_L}{a} + \tau_p \right)^2 f_{av}$$
$$+ p_v \left(\frac{7V_L}{a} + 1.5\tau_p + 2t_{sd} \right) + \frac{p_v^2}{f_{av}} \tag{9.4.4}$$

If the vehicles are trained, p_v is the number of people per train. In almost all cases, the third term can be neglected, and often the second.

Equation (9.4.4) is valid unless the string of delayed vehicles is so long that some of them can be shunted around the delay by an alternate path or unless $(n - 1)\nu D_{\min}$ exceeds the total length of track occupied by vehicles upstream of the point of failure. Thus, if D^* is the length of track occupied by vehicles upstream of the failure (analogous to the same symbol used in analysis of Class 2 failures), equation (e) applies if

$$D^* > (n - 1)\nu D_{\min}$$

If this inequality is not satisfied, substitute

$$n - 1 = \frac{D^*}{\nu D_{\min}} \tag{9.4.5}$$

and then equation (9.4.2) in equation (g) to obtain

$$n_{13}\tau_{13} = \frac{D^*}{V_L}\left[\frac{2V_L}{a} + \tau_p - \frac{(\nu - 1)}{2\nu}\frac{D^*}{V_L}\left(1 - \frac{\nu D_{\min}}{D^*}\right)\right]f_{av} + p_v\left(\frac{6V_L}{a} + 2t_{sd} + \tau_p\right) + \frac{p_v^2}{f_{av}} \tag{h}$$

When equation (h) applies, $\nu D_{\min}$ is much less than D^*. Therefore,

$$n_{13}\tau_{13} = \frac{D^*}{V_L}\left[\frac{2V_L}{a} + \tau_p - \frac{(\nu - 1)}{2\nu}\frac{D^*}{V_L}\right]f_{av} + p_v\left(\frac{6V_L}{a} + 2t_{sd} + \tau_p\right) + \frac{p_v^2}{f_{av}} \tag{9.4.6}$$

This equation applies when

$$\frac{2V_L}{a} + \tau_p > \frac{(\nu - 1)}{2\nu}\frac{D^*}{V_L}$$

an inequality which may be satisfied either if the flow is near saturation ($\nu = 1$), or if the delay time τ_p is unusually long. The first condition ($\nu = 1$) is not likely to happen in practical cases because merging becomes increasingly difficult as ν approaches 1. On the other hand, a long pushing delay, if an automated pushing strategy is incorporated in the system, implies either a failure in the pushing mode or a Class 4 failure, that is, one in which the failed vehicle cannot be pushed.

Class 4 Failures

Based on the above discussion, $n_{14}\tau_{14}$ is given by equation (9.4.6), in which $\tau_p \rightarrow \tau_4$ becomes the time required to restore service—long compared to the other time intervals in equation (9.4.6). Thus

$$n_{14}\tau_{14} \approx \tau_4 \left(\frac{D^*}{V_L} f_{\mathrm{av}} + p_v \right) + \frac{p_v^2}{f_{\mathrm{av}}}$$

But $(D^*/V_L)f_{\mathrm{av}}$ is the number of people in vehicles in the distance D^* between bypass tracks. This is generally large compared to p_v. Moreover,

$$\sqrt{\frac{\tau_4}{D^*/V_L}} \left(\frac{D^*}{V_L} f_{\mathrm{av}} \right) >> p_v$$

since, if the vehicle cannot be pushed, $\tau_4 >> D^*/V_L$. Therefore $n_{14}\tau_{14}$ simplifies to

$$n_{14}\tau_{14} = \tau_4 (D^*/V_L) f_{\mathrm{av}} \tag{9.4.7}$$

in which D^* is either the mean distance from the failure to the nearest upstream alternative path or the length of the vehicle stream, whichever is shorter.

9.5 Station Entry Monitoring Equipment

Perhaps the most critical manuever in operation of a transit system is the one in which a vehicle or train approaches and stops behind another unloading and loading passengers. For on-line station train systems, this problem is discussed in section 4.2; and for off-line station systems with vehicles stopping behind one another, it is discussed in section 7.2. In this section, we consider the consequences of a combination of failures that causes a vehicle to fail to slow down on entry into a station. Such a failure implies a failure of all braking systems. With redundant systems, such a failure will be rare, but the station entry maneuver occurs with every vehicle-trip and is therefore of primary concern. One approach is to try to make the vehicle systems sufficiently reliable that the probability of station entry failure can be tolerated. Another approach, discussed here, is to add a station entry monitor to the equipment in each station. The monitor is designed to check the speed of each vehicle at one or more points while it is entering the station and to actuate an independent braking system if the speed is excessive.

The station entry monitors will of course add to the cost of the system, and themselves may fail, thus requiring the station to be bypassed until the repair is made. Thus the trade-off between increased reliability of vehicle-borne equipment to meet station entry requirements and the provision of station entry monitors need to be considered.

MTBF *between Collisions in Stations with No Monitor*

Let $MTBF_{vb}$ be the mean time between failures of the entire vehicle braking system. Assume that a vehicle-borne failure monitor detects the failure and, if the vehicle is not already committed to switch into a station, causes the switch to be locked in the position for station bypass, until the vehicle can be stopped safely. Thus failure of the braking system may cause a station collision only if it occurs after the vehicle is committed to enter the station.

The critical time t_{cr} during which the vehicle is committed to enter a station is the time interval from switch command to station stop. The switch command must occur far enough ahead of the station diverge point to permit the switch to be thrown, verification that it is thrown, and the vehicle stopped before the diverge point in case verification does not occur. At line speed V_L, the time to traverse the stopping distance $V_L^2/2a$ is $V_L/2a$. From equation (3.4.3), the time required to traverse the spiral section of the off-line track is $(32H/J)^{1/3}$. Finally, the time required to decelerate at the service rate to a stop is $V_L/a + a/J$. Thus,

$$t_{cr} = \text{time to switch and verify} + V_L/2a + (32H/J)^{1/3} + V_L/a + a/J \qquad (9.5.1)$$

For example, if $V_L = 15$ m/s, $a = 2.5$ m/s^2, $J = 2.5$ m/s^3, $H = 3$ m, and the switch/verify time is say 5 s, $t_{cr} = 18.4$ s.

If the average trip time is T_{trip}, then the fraction of braking failures in a specific vehicle that could result in in-station collisions is t_{cr}/T_{trip}. If there are N_v operational vehicles (or trains) in the system, the mean time between station collisions with no monitor in the whole system is

$$MTBF_{sc_{\text{w/o monitor}}} \geqslant \frac{MTBF_{vb}(T_{\text{trip}}/t_{cr})}{N_v} \tag{9.5.2}$$

The sign "$\geqslant$" indicates that a vehicle braking failure in the critical period sets up the conditions for a collision, but a collision does not occur in all circumstances, for example, when there are no parked vehicles in the station.

MTBF *between Collisions in Stations with Monitors*

Let the mean time between failures of the station monitor be $MTBF_{sm}$. If the monitor is inoperative, a failure detection system, operating with time delay t_{fd}, commands all approaching vehicles to bypass the station. Then only vehicles already committed to enter the station will do so. Thus it can be said that the station entry maneuver is unmonitored for vehicles within $t_{fd} + t_{cr}$ of the station, in which t_{cr} is given by equation (9.5.1). The number of vehicles in this critical period is simply $N_{cr} = (t_{fd} + t_{cr})/T_{sh}$, in which T_{sh} is the headway between vehicles entering the station. If the vehicles are equally spaced, the probability that one of the N_{cr} vehicles fails during the critical period is

$$P_{\text{veh. failure}} = \frac{(t_{fd} + t_{cr})}{MTBF_{vb}} \left(\frac{1 + 2 + \ldots + N_{cr}}{N_{cr}} \right)$$

$$= \frac{(t_{fd} + t_{cr})(t_{fd} + t_{cr} + T_{sh})}{2MTBF_{vb}T_{sh}}$$

The reciprocal of this expression can be interpreted as the number of times the station monitor can fail for every time its failure is accompanied by a vehicle failure in the critical period. Thus, the mean time between potential collisions in a specific station is $MTBF_{sm}/P_{\text{veh. failure}}$. If there are n_s stations in the system, the mean time between potential collisions in the whole system is

$$MTBF_{sc_{\text{w/monitor}}} = \frac{2MTBF_{sm}MTBF_{vb}T_{sh}}{n_s(t_{fd} + t_{cr})(t_{fd} + t_{cr} + T_{sh})} \tag{9.5.3}$$

Dividing by equation (9.5.2), the improvement in $MTBF_{sc}$ due to the station monitor is

$$\frac{MTBF_{sc\ \text{w/monitor}}}{MTBF_{sc\ \text{w/o monitor}}} = \frac{2N_v}{n_s} \frac{T_{sh}t_{cr}MTBF_{sm}}{(t_{fd} + t_{cr})(t_{fd} + t_{cr} + T_{sh})T_{tr}} \qquad (9.5.4)$$

in which

T_{sh} = station entry headway
t_{fd} = time constant of in-station failure detection system
t_{cr} = value given by equation (9.5.1)
T_{tr} = average trip time
N_v = number of vehicles
n_s = number of stations

Typical values might be $t_{cr} = 20$ s, $t_{fd} = 10$ s, $T_{sh} = 10$ s, $T_{tr} = 10$ min, $N_v/n_s = 10$. Then the right side of equation (9.5.4) becomes $20MTBF_{sm}$, in which $MTBF_{sm}$ is in hours. Thus, with redundancy in the station monitor, the *MTBF* for station collisions can be improved by use of monitors by a very large factor, for example, for $MTBF_{sm} = 1000$ hours, by a factor of 20,000. Without the monitors, $MTBF_{vb}$ must be improved by the same factor to give the system performance possible with station monitoring.

Required MTBF *of Station Monitors*

In the previous paragraph, the mean time between in-station collisions in an entire system is related to the MTBF of the station monitors. The required *MTBF* of the station monitor is determined by equations (8.8.3, 8.8.4) in which the $n\tau$ and the *LCC'* corresponding to the monitor must be included. If the station monitor is inoperative, there are two choices: (1) all vehicles bypass the station until the monitor is restored to service; and (2) all vehicles passing the station slow down to a predetermined safe speed V^* until the monitor is restored to service. In the first case, persons destined for the failed station are rerouted to a different station and then must make their way to their final destination by alternative means; and persons initiating their trips at the failed station must either wait until the monitor is restored to service or go to another station. The number of people thus delayed is the sum of the flows originating and terminating their trips at the failed station, multiplied by the mean time to restore service. The time delay of each person is the additional time required to reach the destination via an alternate route. Thus

$$(n\tau)_{\text{station monitor}_1} = (f_{s_{\text{in}}} + f_{s_{\text{out}}})(MTRS_{sm})(\Delta \text{ trip time}) \qquad (9.5.5)$$

In the second case, the entire line flow f_{av} slows down for a period $MTRS_{sm}$, but there is no further delay of passengers passing the station in vehicles, or initiating or terminating their trips at the failed station. The corresponding $n\tau$ is given by equation (9.4.3) without the second term, and with $D^* = V^*t^*$ where, from figure 9-1, $t^* = MTRS$. The flow of passengers initiating trips at the failed station is delayed if the flow of vehicles into the station is inadequate to accommodate the initiating passengers. This flow includes both the occupied and empty vehicle flows into the failed station. The delay time is the same as the delay time of persons terminating at the failed station. With these factors in mind, the corresponding $n\tau$ for Case 2 is

$$(n\tau)_{\text{station monitor}_2} = \frac{\nu}{2(\nu - 1)} MTRS^2_{sm}\left(1 - \frac{V^*}{V_L}\right)^2 (f_{av} + f_{s_{\text{in}}}) \qquad (9.5.6)$$

in which $f_{s_{\text{in}}}$ is the flow of passengers initiating trips at the failed station. Comparing with equation (9.5.5), the appropriate strategy can be determined. In terms of passenger discomfort and distress the (Δ trip time) associated with going to an alternative station should be weighted more heavily than the additional delay associated with slower movement through the station. Thus unless the line flow is much larger than the station flow and $MTRS$ is of the order of (Δ trip time), the best strategy is the second one.

9.6 Failures of Passenger-Processing Equipment in Stations

Patrons beginning their trips may be delayed at a station due to the following types of equipment malfunction:

1. Malfunction of automatic equipment such as destination selectors, fare collectors, and ticket dispensers
2. Malfunction of automatic equipment for assigning passengers to vehicles
3. Malfunction of automatic station doors leading from the station platform to the vehicle
4. Malfunction of automatic doors on the vehicle
5. Malfunction of starting equipment on vehicle

Patrons planning to end their trips at a certain station may be caused to bypass the station due to failure of station entry monitoring equipment, as described in section 9.5. They may also be caused to bypass the station due to malfunction of equipment described above which prevents the free flow of vehicles through stations. For example, failure of a vehicle to start moving after loading its passengers blocks the station. Once all station platforms behind the failed vehicle and all entering queue positions are filled, additional vehicles programmed to enter the station must be diverted to an alternate station. Thus, it is necessary in considering the required *MTBF* of station equipment to take into account as appropriate both the people initiating and terminating their trips at the malfunctioning station.

In group-riding transit systems, it is generally felt that automatic vehicle doors are necessary because no one individual can be expected to take responsibility for opening or closing the doors. In single-party, demand systems, on the other hand, manual doors may more likely be satisfactory. In either case, attainment of reasonable *MTBF*s requires that the doors be provided with a manual override both inside and outside to minimize both the number of people inconvenienced and the *MRTS*. If the vehicle doors are designed so they cannot lock and trap people inside, and that at worst a door malfunction is cause for dispatching the vehicle to a maintenance shop, they need not be considered further in this analysis.

To prevent people from accidentally or purposefully entering the path of vehicles moving through stations, and to improve the station climate, it has been thought that automatic station doors that slide open directly opposite the vehicle doors are a necessity. This is, of course, a degree of refinement not accorded many conventional transit systems. In new off-line station automated transit systems the vehicles move more slowly through the stations, and the wait time is minimum. Thus, the need for automatic station doors may in many cases be marginal. They can, however, be considered as one of the components in the following analysis. These doors should also be equipped with manual override devices which can be operated from either side.

For purposes of systems anlaysis, the failures that impede the flow of passengers as a result of malfunctions in stations can be divided into three classes:

1. Malfunctions that affect only the passengers initiating trips at the station in question
2. Malfunctions that affect incoming and outgoing passengers but do not divert passengers to other stations
3. Malfunctions that are serious enough to cause passengers to be diverted to other stations

Equipment on board a vehicle that affects its ability to start on command may be the same as that which could cause a malfunction while on line; but should still be included in the computation of required *MTBF* of the station equipment. The reason is that in the systems analysis, we compute the required *MTBF*s of the various classes of failures, not of specific components. The required *MTBF* of the components or subsystems is determined as indicated in section 8.9.

For Class 1 failures, the number of person-hours of delay can be found by considering figure 9-3, which shows the position-time lines of groups of passengers entering a station. Let $p_g$be the average number of people per group.

The first group entering the station following a malfunction is delayed τ_1 units of time. The second group, walking in at an average speed V_w, moves up to a minimum separation h_{min} behind the first group and waits until the malfunction is cleared. If T_h is the normal time headway between groups entering the station, the second group begins waiting $T_h - h_{min}/V_w$ units of time later than the first group. If T_{min} is the minimum time headway through stations, corresponding to the maximum flow rate of p_g/T_{min} people per unit time, the second group begins moving $T_{min} - h_{min}/V_w$ later than the first group. Thus the second group is delayed $\tau_1 - (T_h - T_{min})$. Similarly, the third group is delayed $\tau_1 - 2(T_h - T_{min})$. If q is the number of groups delayed, it may be seen from figure 9-3 that

$$q = \frac{\tau_1}{T_h - T_{min}} \tag{a}$$

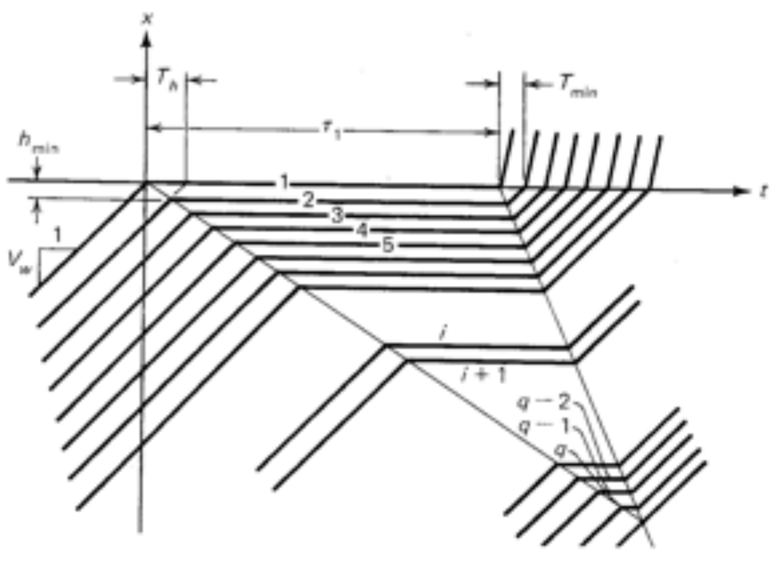

Figure 9-3. Position-Time Diagrams for Passengers Waiting for Service as a Result of a Delay of Duration τ_1

Then, the total number of person-hours of delay for Class 1 failures of station equipment is

$$(n\tau)_1 = p_g \sum_{i=1}^{q} [\tau_1 - (i - 1)(T_h - T_{\min})] \tag{b}$$

$$= p_g[q\tau_1 - (T_h - T_{\min})(q - 1)q/2]$$

$$= \frac{p_g \tau_1 q + 1)}{2} \tag{c}$$

In cases of consequence, q is much greater than 1. Then, after substituting equation (a) into equation (c),

$$(n\tau)_1 = fs_{\text{eq}}\tau_1^2 \tag{9.6.1}$$

where

$$fs_{\text{eq}} = \frac{p_g}{2(T_h - T_{\min})} \tag{9.6.2}$$

is an equivalent station flow. If the station is operating at maximum capacity when the failure occurs ($T_h = T_{\min}$), $(n\tau)_1$ approaches infinity in theory, but in practice maximum flow will occur only for a short period so that the smallest average value of T_h is greater than $T_{\min}$. If T_h varies with time, $(n\tau)_1$ can be found by direct summation of equation (b) for all values of q for which the summand is positive.

For Class 2 failures, the number of person-hours of delay is $(n\tau)_1$, given by equation (9.6.1), plus a corresponding term for the people terminating their trips at the failed station. The latter term is approximately of the form of equations (9.6.1) and (9.6.2) even if each vehicle carries more than one group. Thus

$$(n\tau)_2 = \frac{p_g}{2}\left(\frac{1}{T_{h_{\text{in}}} - T_{\min}} + \frac{1}{T_{h_{\text{out}}} - T_{\min}}\right)\tau_2^2 \tag{9.6.3}$$

in which $T_{\min}$ is the same value in both cases because of continuity of flow, and τ_2 is the mean time to restore service for Class 2 failures.

For Class 3 failures, substantially all of the vehicles terminating at the failed station are diverted to another station. The number of people thus involved is τ_3 times the flow into the station from the line, $fs_{in} = p_g/T_{h_{in}}$ in which $T_{h_{in}}$ is the equivalent minimum headway if there were only one group per vehicle. The delay time is the time added to the trip as a result of diversion to an alternate station. Thus

$$(n\tau)_3 = (n\tau_3)_1 + \frac{p_g \tau_3 \Delta T_{\text{trip}}}{T_{h_{in}}} \qquad (9.6.4)$$

in which $(n\tau_3)_1$ is as in equation (9.6.1) with τ_3 substituted for τ_1.

9.7 Merge Equipment Failures

Wayside merge equipment is needed to avoid collisions in car-follower systems by transferring the image of each car to the opposite branch of the merge, and in point-follower systems by sensing vehicle positions and commanding vehicles to slip slots. In either case, a failure of wayside equipment could in the worst case cause two vehicles to wedge together in the merge point. This is one of the worst types of system-caused failures in automated guideway transit (AGT) systems.

Failure monitoring is needed to minimize the consequences of merge equipment failures. If a failure occurs, the action can be either to stop the two streams of traffic entirely, or to slow them to a safe speed. In the latter case, the number of person-hours of delay is greatly diminished. Equations (9.4.3, 9.4.4, 9.4.6 and 9.4.7) apply directly to this case if account is taken of the involvement of two streams of traffic instead of one.

9.8 Diverge Equipment Failures

The purpose of wayside diverge point equipment is to read the destination of each car, determine the direction it should be switched, and cause the switch to be actuated. If the switch is in the track, the diverge point equipment includes the switch; if the switch is in the vehicle, it is included in vehicle-borne equipment.

Failures of diverge point equipment may be divided into two classes:

1. Some of the vehicles are misdirected and must either be rerouted or passengers must make their ways to their destinations by alternate routes.
2. The switch is locked in the middle thus requiring all vehicles to stop until it is restored to service.

In Class 1 failures, the number of person-hours of delay is

$$(n\tau)_1 = (\text{Misdirected flow})(\tau)(\Delta\text{trip time}) \qquad (9.8.1)$$

in which τ is the mean time to restore service, and (Δtrip time) is the extra time needed to arrive at the destination by an alternate route.

In Class 2 failures, $(n\tau)_2$ is the same as a Class 4 vehicle failure and is given by equation (9.4.7).

9.9 Failures in Wayside Communications Equipment

In some types of automated transit systems all essential control equipment, except for wayside merge and diverge equipment, is aboard the vehicles. In this case the failure of wayside communications equipment, if there is any, may cause person-hours delay when some other failure has occurred or may decrease system capacity, thus causing delay in the peak periods. In other types of systems, the wayside communication link is essential to all control functions and its failure is of major consequence. To be meaningful, computation of $n\tau$ for these failures must be left to specific cases.

9.10 Failures in Central Control Equipment

Use of central control equipment in AGT systems may vary from complete control of the movement of every vehicle from a central facility, to supervisory functions in a central facility, to no central control.

Complete Central Control

If all control functions pass through a central control facility, a breakdown in this facility requires that all vehicles be stopped. Because of the excessive level of inconvenience this will cause, the system should be designed so that the vehicles can then move at slow speed under battery power into the nearest stations. Because of the possibility of a general power failure, such a back-up system is mandatory.

The corresponding value of $n\tau$ is composed of two groups of people: (1) those on the system at the time of failure; and (2) those seeking service. For the second group, the number of persons delayed is the total flow rate into the system t_h multiplied by the mean time to restore service, *MTRS*. Thus the number of person-hours of delay is

$$(n\tau)_2 = t_h(MTRS)^2$$

For the first group, the number of persons delayed is the number of persons riding the system at any one time. From ~~equation (4.5.17)~~, this number is t_h

page 68

times the average trip time, T_{trip}. The delay time depends on whether or not batteries are provided on each vehicle. If they are not provided, the delay time is *MTRS*. If batteries are provided, the delay time is the increase in trip time due to the decrease in speed from V_L to V^*. From equation (2.5.3) this time interval is approximately $(D_s/V_L)(V_L/V^* - 1)$ since the term V_L/a_m is generally small.

Summarizing, the total number of person-hours of delay due to a central control or power failure is

$$\left.\begin{aligned}(n\tau)_{central} &= t_h(MTRS + T_{trip})MTRS && \text{no batteries}\\ &= t_h[MTRS^2 + T_{trip}(D_s/V_L)(V_L/V^* - 1)] && \text{with batteries}\end{aligned}\right\} \quad (9.10.1)$$

Central Supervisory Control

The consequences of failure can be reduced by decentralizing as much of the control as possible into the vehicles, stations, and switch points. It is still, however, desirable to exercise supervisory control at a central location for two reasons:

1. Prevention of overloads on specific lines and in specific stations by delaying the dispatching of vehicles to potentially overloaded stations
2. Optimum routing of empty vehicles

Central Register/Dispatcher

In the first function, rerouting along different paths to prevent line overloading can be accomplished by use of diverge point routing computers which communicate with downstream merge point computers. However, to avoid denying access to a station by vehicles programmed to that station because too many vehicles have been routed to it, central supervisory monitoring and control is necessary. The equipment is simple. All that is necessary is to communicate to a central register the estimated arrival times at the desired destinations of all trips ordered. If an arrival time comes into the station-*i* register too soon after the previous arrival time to station *i*, a communication is sent back to the origin station to order a specific time delay in dispatching of the vehicle so that the arrival rate does not exceed a specified value. Thus, before permitting a vehicle to leave a station, the station dispatcher asks permission of the central register. The central register then causes vehicles to be dispatched on a first-come, first-serve basis with time delays if needed. These delays will normally be too short to be recognized as delays.

The above-described central reigster function is simple enough to be inexpensively duplicated to reduce its required *MTBF*. If it doesn't work, the consequence is that a vehicle may arrive at its destination only to be aborted, that is, caused either to stop at an alternate station or to circle back for a second try. Causing vehicles thus to circle adds to the flow along lines already near their maximum flows, and thus may induce instability in a network AGT system. The problem is eased, however, by the existence of diverge point computers operating as described above. The number of person-hours of delay due to failure of the central register/dispatcher is best determined in a computer simulations of specific systems.

Empty Vehicle Dispatcher

The possibility of failure of a central computer/dispatcher which routes empty vehicles in an optimum way introduces a requirement for a suboptional but simpler empty vehicle dispatching scheme in which computer/controllers at each station are able to rid the station of excess empty vehicles by dispatching them to the next station, and to call for empty vehicles from one or more stations up stream.

Failure of the optimal dispatcher may cause excess time delays because of a temporary local shortage of vehicles, particularly if it occurs during the rush period. Computer simulation of specific networks are again required to determine the number of person-hours of delay due to failures.

9.11 Escape Mechanisms

A means for escape from an AGT vehicle must be provided in two circumstances:

1. The vehicle is stuck on the guideway and cannot be removed in a reasonable time.
2. There is a fire on board.

The kind of escape mechanism that should be provided depends on the probability of each type of emergency and the cost and safety level of the mechanism. The control system enters the consideration of escape mechanisms insofar as it may reduce the probability of emergencies. As indicated in section 9.4, inclusion of a pushing mode in the longitudinal control system will greatly reduce the mean time between instances in which passengers must be removed from the vehicle. Addition of redundancy and monitoring equipment at merge and diverge points will greatly reduce the need for emergency escape at those points.

The most commonly mentioned escape mechanism is an emergency walkway along the entire length of the guideway. Such a walkway should be designed to be serviceable in inclement weather by the less agile members of society and permit people to walk safely a distance of up to half the station spacing. The advantages of emergency walkways lie in their simplicity and continual presence. Their disadvantages are cost and visual impact, both of which may significantly reduce the viability of the system. If escape mechanisms are not required very frequently, a small fleet of trucks equipped with hydraulic lifts may be satisfactory. A third mechanism, which also may simplify guideway maintenance, is a vehicle designed to run on the side of the guideway such as has been designed by DEMAG-MBB for their systems. See figure 9-4. One such vehicle in each loop of the system on standby at a station would be required.

In the case of fire, it may be equally satisfactory to cause the vehicle to proceed to the next station, usually no more than a minute away, as to let the patrons egress onto a walkway in highly unfavorable weather conditions. The extent to which the vehicles can be made fireproof and to which fire extinguishers can be provided will of course influence this tradeoff.

A long delay due to a vehicle stuck on the guideway is a Class 4 vehicle failure, and the number of person-hours of delay due to such a failure is given by equation (9.4.7). It can be anticipated that if the required *MTBF*s are computed to satisfy system requirements, the frequency of use of escape mechanisms will be very low. In this circumstance, the use of systems other than walkways appears warranted even though they involve a delay before egress is possible.

9.12 Reliability Allocation

The required reliabilities of the various subsystems and components can now be allocated by substituting appropriate $n\tau$ values such as estimated in sections 9.4-9.10 for all failure classes of all subsystems into equations (8.8.3, 8.8.4). The calculations require knowledge of the slopes of the life cycle cost curves LCC'_{ij}; however, to gain some insight and to illustrate application of the theory some simplifying assumptions about the LCC'_{ij} can be made. For some equipment it is not particularly expensive to increase reliability, that is, LCC'_{ij} is small and the corresponding equipment does not enter strongly into equation (8.8.4). In other cases, it may initially be sufficient to assume the LCC'_{ij} are all the same.

To develop a specific illustration, assume the only subsystems that need to be considered are the vehicles, the station monitors, the station passenger-processing equipment, and central control. For the first three subsystems, assume four, one, and three classes of failure, respectively, as

Figure 9-4. Service Vehicle in Operation on the Side of the Guideway of The Cabinlift System—at the Ziegenhain Hospital near Kassel, West Germany. (Courtesy of DEMAG + MBB)

computed in sections 9.4, 9.5, and 9.6. For central control, assume one class of failure—a power failure. Let the subscripts in equations (8.8.3, 8.8.4) correspond to these subsystems and failure classes in the same order. Then in the application of equations (8.8.3, 8.8.4) it is more convenient to write them in the form

$$\left.\begin{aligned} MTBF_{mn} &= \frac{(n_{mn}\tau_{mn})^{1/2}(T_w/T_v)^{1/2}}{\epsilon_{\text{spec}} t_h T_{\text{trip}}} \sum \\ \sum &= N_v \sum_{j=1}^{4} (n_{1j}\tau_{1j})^{1/2} \\ &+ \left(\frac{T_w}{T_v}\right)^{1/2} \left\{ n_s \left[(n_{21}\tau_{21})^{1/2} + \sum_{j=1}^{3} (n_{3j}\tau_{3j})^{1/2} \right] + (n_{41}\tau_{41})^{1/2} \right\} \end{aligned}\right\} \qquad (9.12.1)$$

in which it is assumed that all LCC' in equations (8.8.3, 8.8.4) are approximately equal, n_s is the number of stations, and PH_{yr}/T_v has been made specific by substituting equation (9.2.12). From section 8.5, it will be assumed in the following analysis that $(T_w/T_v)^{1/2} = 1.7$. To be specific, also assume that $\epsilon_{\text{spec}} = 10^{-4}$, that is, that each regular traveler on the average will experience one hour of accumulated delay every 10,000 hours. Assuming 200 hours of travel per year, this corresponds to one hour of delay every 50 years, or in other words, every fiftieth regular passenger will experience one hour of delay per year.

For the vehicle failure classes, the corresponding $n\tau$ are given respectively by equations (9.4.1, 9.4.3, 9.4.4, 9.4.7). In these equations, it is reasonable to assume for a first-order estimate that only the terms proportional to f_{av} are important. Then

$$\sum_{j=1}^{4} (n_{1j}\tau_{1j})^{1/2} \approx f_{av}^{1/2} \left\{ \left[\frac{\nu}{2(\nu-1)} \right]^{1/2} \left[\frac{D^*}{V_L}\left(\frac{V_L}{V^*} - 1 \right) + \frac{2V_L}{a} + \tau_{p_3} \right] + \left(\tau_4 \frac{D^*}{V_L} \right)^{1/2} \right\} \qquad \text{(a)}$$

in which τ_{p_3} is the pushing delay time, and τ_4 is the time required to remove a nonpushable vehicle. From equation (9.5.6), for the monitor,

$$(n_{21}\tau_{21})^{1/2} = \left[\frac{\nu}{2(\nu - 1)}\right]^{1/2} MTRS_{sm}\left(1 - \frac{V^*}{V_L}\right) f_{av}^{1/2}(1 + fs_{in}/f_{av})^{1/2} \qquad \text{(b)}$$

From equations (9.6.1) through (9.6.4)

$$\sum_{j=1}^{3} (n_{3j}\tau_{3j})^{1/2} = (p_g/2)^{1/2}\left[\frac{\tau_1}{(T_{h_{in}} - T_{min})^{1/2}}\right.$$

$$+ \tau_2\left(\frac{1}{T_{h_{in}} - T_{min}} + \frac{1}{T_{h_{out}} - T_{min}}\right)^{1/2}$$

$$\left. + \tau_3\left(\frac{1}{T_{h_{in}} - T_{min}} + \frac{2\Delta T_{trip}}{\tau_3 T_{h_{in}}}\right)^{1/2}\right] \qquad \text{(c)}$$

From equation (9.10.1),

$$(n_{41}\tau_{41})^{1/2} = MTRS_{power} t_h^{1/2} \qquad \text{(d)}$$

one-way

in which it is assumed that batteries are used and, in the second form of equation (9.10.1), the second term is negligible.

As an illustration, let us compute the required *MTBF* for pushable vehicle failures in a loop system. Then $(n_{mn}\tau_{mn})^{1/2}$ is the sum of the second and third terms in equation (a) and $f_{av}/t_h = 1/2$. Assume the trip time is $T_{trip} = 0.1$ hour. For $(T_w/T_r)^{1/2} = 1.7$ and $\epsilon_{spec} = 10^{-4}$, equation (9.12.1), for $m = 1$, $n = 3$, becomes

$$MTBF_{13} = \overset{9.5}{\cancel{5}}(10)^4\left(\frac{2V_L}{a} + \tau_{p_3}\right)\frac{1}{f_{av}^{1/2}}\sum \qquad \text{(e)}$$

in which it is assumed that the average flow is at the rather high value of one half the maximum possible, that is, $\nu = 2$. To estimate the summation in equation (e), it can be assumed in equation (a) that τ_4 is by far the largest time parameter. Thus, only the right-hand term will be included. In equation (b) assume $V^*/V_L = 0.5$ and note that on the average $f_{av}/fs_{in} = n_s$, the number of stations. In equation (c) assume $\cancel{p_g = 1.3}$, $\tau_1 = \tau_2 << \tau_3$, and $T_{h_{in}} = 2T_{min}$. But $p_g/T_{h_{min}} = fs_{in}$. With these assumptions,

$$\frac{1}{f_{av}^{1/2}} \sum = N_v\left(\tau_4 \frac{D^*}{V_L}\right)^{1/2} + 1.7\left\{n_s\left[\frac{MTRS_{sm}}{2}\left(1 + \frac{1}{n_s}\right)^{1/2} + \frac{\tau_3}{n_s^{1/2}}\left(\frac{1}{\underset{1}{\cancel{2}}} + \frac{\Delta T_{trip}}{\tau_3}\right)^{1/2}\right] + \sqrt{2}\, MTRS_{power}\right\} \tag{f}$$

In equations (e) and (f), assume D^*, the distance between stations, is 500 m, $V_L = 10$ m/s, $a = 2.5$ m/s. Then equation (e) with equation (f) substituted becomes

$$MTBF_{13} = 5(10)^4 \frac{(8 + \tau_{p_3})}{3600}\left\{\left(\frac{50\tau_4}{3600}\right)^{1/2} N_v + 1.7\left[\frac{MTRS_{sm}}{2}\left(n_s^2 + n_s\right)^{1/2} + n_s^{1/2}\tau_3\left(\frac{1}{\underset{1}{\cancel{2}}} + \frac{\Delta T_{trip}}{\tau_3}\right)^{1/2} + \sqrt{2}\, MTRS_{power}\right]\right\} \tag{9.12.2}$$

Assume $N_v = 300$, $n_s = 7$. Then let the delay time for nonpushable failures be $\tau_4 = 1$ hour, the time to restore a station monitor to service be $MTRS_{sm} =$ 0.5 hour, the *MTRS* for a serious station failure be $\tau_3 = 0.5$ hour, and the *MTRS* for a power failure chargeable to the system be $MTRS_{power} = 1$ hour. Further, assume $\Delta T_{trip}/\tau_3 = 1$. Finally, let the time to push be $\tau_{p_3} = 15$ seconds. Then, if the terms are listed in the same order as in equation (9.12.2),

$$\begin{aligned} MTBF_{13} = 319 \{ \; & 35.4 && \text{vehicles} \\ + \; & 3.2 && \text{station monitors} \\ + \; & \overset{3.2}{\cancel{2.8}} && \text{passenger processing} \\ + \; & 2.4 \} && \text{control station} \\ = \; & 14{,}000 \text{ hours} \end{aligned}$$

This is too high an *MTBF* to be practical with single-chain components. With redundancy, equation (9.2.1) shows that the required *MTBF* of each redundant unit is

$$MTBF_{\text{unit}} = [2\tau(14{,}000)]^{1/2}$$

in which τ is the time required to get the vehicle off line after the failure has occurred. Let τ be the trip time of 0.1 hour, thus implying on-board failure monitoring. Then

$$MTBF_{\text{unit}} = 53 \text{ hours}$$

The above is an example calculation to illustrate the method. The numbers are guesses but are felt to be representative, and all elements in the system have not been taken into account.

9.13 Summary

In chapter 8, a theoretical method is developed to allocate the reliabilities of the subsystem of a general system in such a way that the life cycle cost is minimized while a given constraint on service availability is met. While it was not treated explicitly, the case in which some of the subsystem reliabilities are already known can be treated in a straightforward manner by replacing the unavailability factor ϵ by the net unavailability requirement of the subsystems with underdetermined reliabilities. By considering the subsystems as conglomerates of series-connected components, it was shown how the reliabilities of subsystems and components at all levels can be allocated in an optimum way.

The purpose of chapter 9 is to expand on and to illustrate the use of the theoretical method of chapter 8. It begins with the consideration of parallel connections between components, that is, redundancy. It is shown how to compute the reliability of systems of redundant members and that, with failure monitoring, redundancy greatly increases the service dependability of transit systems. Assuming only vehicle failures, the theory of redundancy is used to develop equations for the reliability of loop and network transit systems.

Next, the full application of the reliability allocation theory is initiated by developing formulas for the average number of person-hours of delay ($n\tau$) in a variety of classes of failure of vehicle and wayside subsystems. In specific systems, it may be possible to develop corresponding formulas for all significant failure classes; however, such a comprehensive treatment is not attempted. The purpose, rather, is to develop enough of the $n\tau$ formulas to illustrate application of the reliability allocation theory. In the final section of chapter 9, the reliability allocation theory is assembled and applied to a particular case.

Application of the reliability allocation theory is of fundamental importance both in the development and design of new transit systems and in the improvement of existing systems, and gives a great deal of quantitative insight into the most efficient and appropriate means of meeting system reliability goals at minimum cost. In particular, it shows the dramatic improvements in system reliability that can be made possible by introducing redundancy, failure monitoring, and rapid automated pushing of failed vehicles.

References

1. C.L. Olson, G.H. Fuller, and R.B. Fling, "Some Reliability, Dependability, and Safety Considerations for High-Capacity PRT Systems," *Personal Rapid Transit III*, Audio Visual Library Services, University of Minnesota, Minneapolis, Minn., 1976.

2. Harry Bernstein and Arthur Schmitt, "Emergency Strategies for Safe Close-Headway Operation of PRT Vehicles," *Personal Rapid Transit*, Audio Visual Library Services, University of Minnesota, Minneapolis, Minn., 1972.