Technical Meeting of the Institution

held at

The Institution of Electrical Engineers

Thursday, February 9th, 1967

The President (Mr. R. DELL) in the chair.

The Minutes of the Technical Meeting held on 11th January, 1967, were read and approved.

The President then requested Mr. H. W. Hadaway (London Transport) to read his paper entitled " Fail Safe."

Fail Safe

By H. W. HADAWAY*

1. INTRODUCTION

A popular novel has the title " Fail Safe " and posters advertising a similarly entitled film are on display. The term is in public use in a way that its originators could never have imagined would happen.

" Fail Safe " is known to all Signal Engineers at a very early stage in their careers. So far as I am aware no generally accepted definition exists of the term and for a subject so vital it is of surprise to me that no paper has as yet been given to this Institution with such a title.

The need to design systems and equipment to fail safe requirements has existed since signalling equipment was first used to share responsibility with staff for the safety of train operation. When the responsibility had depended solely on the human element then such equipment as was provided needed to be no more than reliable.

The change in conditions that has occurred with the abolition of so many of the manual and mechanical features and their substitution by automatic electrical or electronic systems is now rapidly approaching the point where little responsibility can be counted upon from the human element and the machine must be capable of accepting full responsibility for safety.

These changes involve not only the members of this Institution, but all railway staff responsible for the operation of train services, together with specialist electrical engineers who see possibilities of the application of their particular systems and methods for the benefit of railway operation.

*London Transport

1964 PASSENGER FATALITIES

Category	*Passenger Fatalities*	*Estimated Passenger Miles* $10^3 \times 10^6$	*Passenger Fatalities per* $10^3 \times 10^6$ *Passenger Miles*
1. ROAD Public Service Vehicle	88	40.3	2.18
2. ROAD Private Car and Taxi	1588	125.5	12.6
3. AIR Domestic Air Services U.K.	75	6.45	11.6
4. RAIL	5	23.0	0.22

In my opinion it is therefore timely to review the subject of safety from the Signal Engineer's viewpoint with its particular reference to " Fail Safe." The record of discussion that I hope will arise will be of benefit to all concerned in these matters, and assist the younger members of our profession who, I feel, may be no little confused by the present use of descriptive literature generously assigning as " Fail Safe " forms of equipment that in the eyes of the Signal Engineer and his standards does not truly measure up to such requirements.

Consideration of the term " Fail Safe " cannot be made without involving other and related terms, wrong and right side failures, redundancy, reliability, and so on, and reference will be made to these matters during the course of this paper.

Above all else I wish to make clear that regarding " Fail Safe," being an intangible and largely dependent upon quality of design, there can be no absolute measure of quantity; the recognition of the degree of safety requirement and achievement will depend upon the individual view of the engineer concerned, the experience he has enjoyed or suffered, as the case may be, and the conditions and circumstances of the railway concerned. This being so, the thoughts I have to offer on this subject arise mainly from my experience with the Underground Railways of London Transport and its predominantly close-headway service in tube tunnels, although some measure of main line conditions are involved in high speed and mixed traffic.

2. PUBLIC SAFETY

Public safety in matters of railway travel is governed by a code of practice established by the Ministry of Transport.

The requirements of the Ministry as published define many signalling features for system safety but do not refer to " Fail Safe " as such. However, it is a matter very much to the fore in an Inspecting Officer's consideration of systems and installations, and the Ministry expects a " Fail Safe " standard to be observed in conformity with past practice or to be set to a new and satisfactory level when changes are made.

As assessment of relative safety in public transport can be made by considering the statistics given by R.O.S.P.A. for accidental deaths in Great Britain is given in the above table.

These figures can be analysed in many ways and I suppose profound reasons advanced for them. It is not my intent to do more in this paper than to point out the very favourable figures of the rail system.

The comparison of safety shown by the figures in the fourth column may well be significant when judging the suitability of equipment forms of control proposed since a type of equipment that will increase the overall safety in air control may, if applied to rail, produce a lower standard of safety.

3. DEFINITION

A definition of the term " Fail Safe " that I offer is:— A design quality of mechanical and electrical signalling equipment and of the system within which it is used, that under failure conditions will provide safety for traffic.

4. EXAMPLES OF MECHANICAL FORMS

4.1. Points.

Power for point movement is usually provided by motors operated electrically

or pneumatically and it must therefore always be assumed that power may be lost at any time and the point switch must continue to be held closely to the stock rail.

The chairlock point movement keeps switch and stock rails firmly together despite widening of the permanent way track gauge, and in this respect provides a higher degree of safety than the more conventional point lock form.

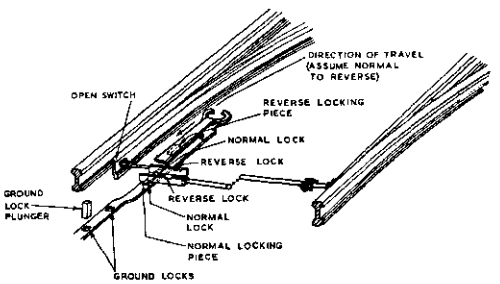

Fig. 1. Points—Facing Point Lock with Ground Lock.

The conventional facing point lock makes engagement in ports of locking blades attached to the point switches and holds the switches in position when power is removed from the point motor, Fig. 1. Power is required to move the lock plunger to disengage the locks to allow the points to be moved to a new position. It is also arranged that a ground track lock plunger does by gravity or by the action of a spring hold the facing point lock in position. This is considered necessary since a loss of power may with vibration cause a movement of the facing point lock.

The natural phenomena of gravity is the most commonly used form for mechanical movement and provides a sound basis of " fail safe " achievement.

4.2. Signals.

The semaphore signal arm operating in the upper quadrant made ideal use of gravity for its return to the danger position, whereas the arm operating in the lower position was made to return to danger by gravity only by the use of a counterweight coupled to the arm by a rod connection, Fig. 2. These two

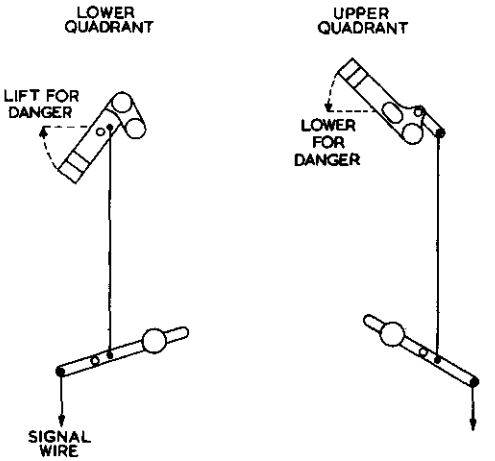

Fig. 2. Signal Arm—Semaphore.

illustrations serve to demonstrate the difference between the ideal and a compromise, in that both forms can be said to return to danger by gravity.

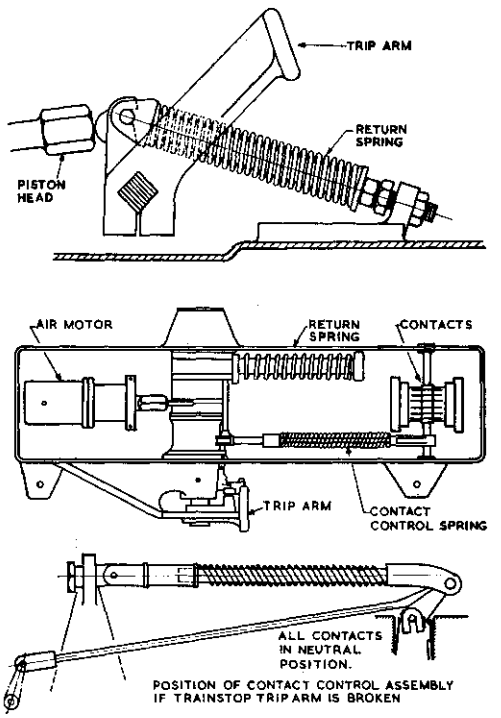

Fig. 3. Trainstop.

The lower quadrant arm is obviously more liabile to failure in the event of a broken rod or a displaced pin than would the arm used in the upper quadrant. Both cases depend upon the bearings being free and well maintained—a requirement both of design and maintenance.

4.3. Trainstops.

The trainstop is not returned to danger by gravity. In this case a double coiled spring is used to return the trainstop to the danger position, see Fig. 3. The spring, provided care is exercised in design and also in its form of application, is very dependable and is commonly used for " fail safe " purposes.

4.4. Proving of Mechanical Movements.

Despite good design and manufacture of mechanical movements, to obtain the required degree of safety it is generally necessary to detect and prove by electrical circuits the proper positioning of the mechanical features.

4.5. Relays.

The relay form as shown in Fig. 4 has played a key part in all signalling systems of the last forty years. It still continues to play a major role at the present time, although the competition of electronics is now threatening to relegate relays to a minor role, if not ultimately to total extinction. It is interesting to see that this threat has engendered a resurgence of life on the part of the relay. The development of the " Reed " type contact, and its application, may well prolong the contest for use in circuits where fusible contacts are acceptable. Where safety is involved carbon contacts have been considered essential in order to prevent fault current fusing the metal parts so as to hold the contacts closed when they should be open. The standard British practice has been to make one contact of carbon and the other generally of silver. The relay at present used for safety signalling circuits was first developed as a track relay, and the design then established has set the standard since that time.

Avoidance of mechanical failure is achieved by a design of robust and ample proportions, with large bearing surfaces for the pivoting of the armature to withstand conditions of railway operation

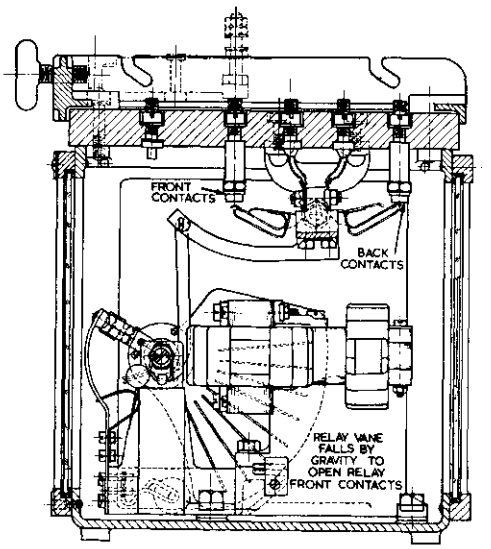

Fig. 4. Track Relay.

generally associated with heavy vibration and a requirement of a 30-year life. Loss of supply to the relay causes the coils to be de-energised and the relay vane to fall by gravity, so as to open the front contacts and close the back contacts.

It is of interest to note that Continental practice, whilst coinciding with British practice as to the requirements of the track relay, permits a smaller form of relay with metal to metal contacts to be used on other circuits, where it is then claimed possible to use proving that the relay is functioning properly.

5. EXAMPLES OF ELECTRICAL FORMS

5.1. The Track Circuit.

The track circuit provides the foundation upon which all present signalling systems of power form depends. Until recently its supremacy for the detection of trains was unchallenged. A number of substitutes not using the wheels, axles and rails for a circuit path are now being actively considered in many parts of the world. These include the " wiggly wire " system, and radar wave guides for transmission of radar signals between trains on adjoining sections of line. A Paper by Professor F. T. Barwell and Mr. H. H. Ogilvy presented to this Institution on December the 5th, 1966 included reference to these developments.

It is natural that such new systems should be received with reserve by the conventional Signal Engineer who, in taking the responsiblity of traffic safety, is less inclined to be receptive to fresh ideas that have not been severely tested by working conditions for a long period of time, than for a designer who, in his enthusiasm, may be over optimistic as to the potential of his proposals and perhaps a little short sighted as to its defects. Whilst it is natural for the Signal Engineer to require full assurance of new systems, past history recorded in the archives of the Institution reveals that with the introduction of the track circuit there was a body of opinion within the Signal Engineers of that time who were firmly convinced that the track circuit would not be able to replace the block instrument, and who had no hesitation in voicing this view. Events have subsequently proved how wrong the " diehards " were, and the track circuit in all its varied forms continues to play its part, whilst new methods have yet to prove their worth by experiment and service tests, to allow the authority of the track circuit to be replaced step by step, perhaps to its ultimate demise.

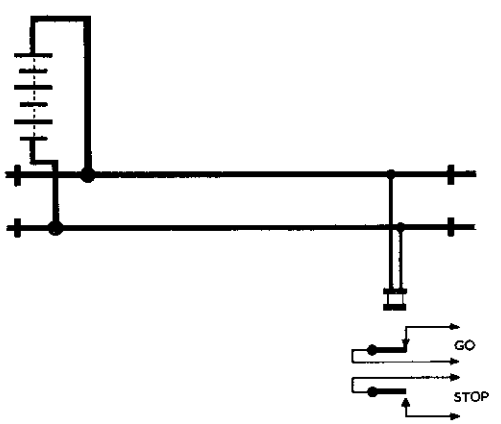

Fig. 5. The Track Circuit.

The form of circuit as shown on Fig. 5 employs the " Fail Safe " principle, since an open circuit at any part of the circuit will cause the relay to be de-energised to the train " Stop " position. Good as the track circuit is, it is not without its limitations. The means of detection of the train by contact between the wheels and axles of the train with the rail surfaces to shunt the relay is open to mal-operation should the rail surfaces be other than clean and bright. The great majority of the railway system is trouble-free in this respect and it is part of the Signal Engineer's experience and knowledge to recognise where such difficulties may arise and make appropriate arrangements to meet the requirements. Protection against bobbing of track circuits at interlockings is made by use of normally de-energised track circuits and time controlled circuits to reinforce the authority of the normal track circuit. This may also include the application of a stainless steel deposit on the rail surface, using a type of track circuit with a pulse feed and relatively high rail voltage, or arranging with the Permanent Way Department for rails to be cleaned regularly, and to see that the Operating Department schedule regular movements through the various connections. It may be argued in these days of economy and efficient use of services that if the rails are so little used as to become rusty then there is a clear indication that there may be a case for the removal of the particular connection concerned. Reference to this was also made in a Paper by the present author: " L.T.E. Methods for the Control and Locking of Junctions " read before this Institution in March 1961.

5.2. Signal Circuits—Fig. 6A.

The diagram shows a conventional circuit arrangement for a semi-automatic signal control, and contains provision for " Fail Safe " in a number of respects. A failure of the track circuits or point detection relay to be energised will cause No. 1 signal to display red. An open circuit in No. 1 signal selection at any of the fuses, at No. 1 lever reversed contact, or at any one of the three relay contacts will produce the same result. An open circuit of the No. 1 GR relay coil will cause the signal to display red. The circuits for the green light and for lowering the trainstop require the GR to be energised and contacts to be closed. The red light circuit is completed over a back contact of the GR. An alternative circuit is also provided for the red light when the trainstop is in the " Up " position to engage the tripcock arm of the train and put the brakes on. In view of

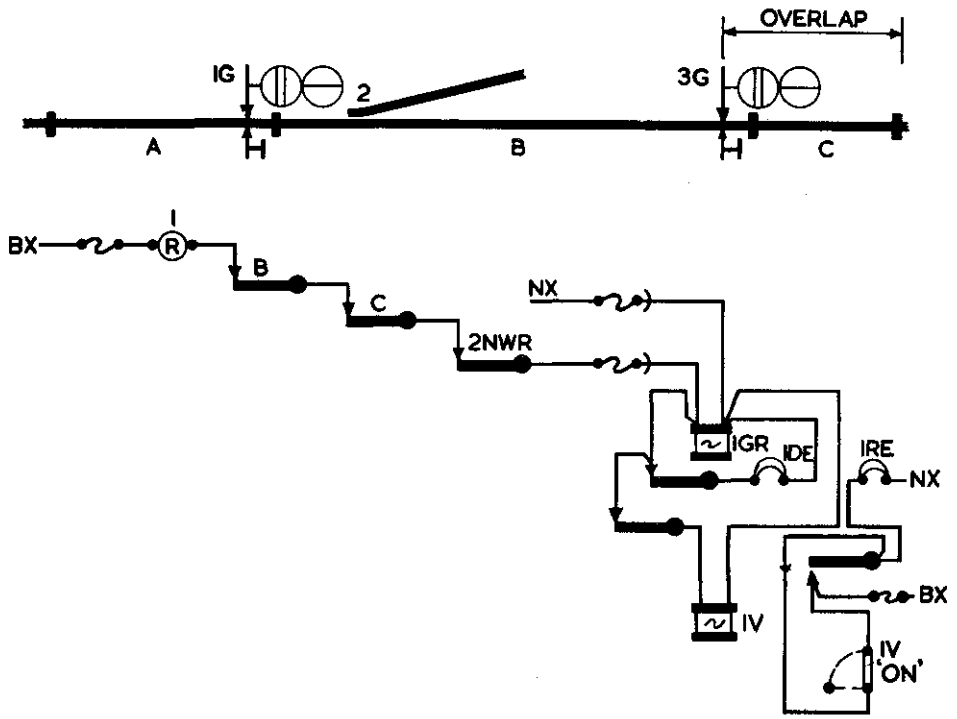

Fig. 6A. The Signal Circuit with " Fail Safe " Design.

the present development of solid state circuits for safety signalling it is nevertheless interesting to recall that many years ago the ' green ' and ' red ' circuits were operated without the signal relay by the flux-neutraliser type of signal circuits. It may well be that type of circuit will be used again, assisted as it could be by the adoption of 125 C/S as the standard frequency of supply, instead of $33\frac{1}{3}$ C/S. On sections of line where the locomotives are not fitted with tripcocks and the display of a red light is vital to bring a train to a stand, the absence of the trainstop demands substitute arrangements. A lamp filament is, of course, a very vulnerable part of an electrical circuit and standby facilities need to be provided. These usually take the form of additional lamps to be switched in by lamp filament detection circuits or lamps with double filaments, one of the filaments being under-run. Standby power supplies are also necessary from trickle charged batteries.

Proving of these circuits must also be used to meet " Fail Safe " requirements so that in the event of total lamp failure, a signal at rear can be held at danger. The complications required to substitute for the trainstop to give system-safety demonstrate the difficulties that arise when the system as a whole possesses an inherent shortcoming. In this context it is also a fact that the red lamp, whatever is done to maintain its illumination under failure conditions, necessitates observation and proper action on the part of the driver of the train. In this respect only the trainstop, or an equivalent, provides a fully " Fail Safe " system.

As an exercise Fig. 6B has been drawn on the assumption that the circuit designer knew nothing of " Fail Safe " requirements and his main concern was to conserve power. The track circuits would then be of the normally de-energised type picking up only when the track circuit is occupied. It is assumed that the signal displays green for the greater part of its life and therefore the feed to the GR is applied when it is necessary for the signal to be at red. The circuit will cause the signal to respond properly and display red and

green with the trainstop lowered when required to do so. The possibility of failure causing a false clear of the green aspect is so great that the circuit is quite impracticable. An open circuit in the GR circuit will cause the signal to show a false green. The green lamp circuit will be falsely fed if the relay failed to pick up. In the conventional circuits should the relay be mechanically held up the green lamp would not be falsely displayed, as it is fed from the selection circuit.

The circuit, bad as it is, has one very great merit which the conventional circuit form does not possess. In the event of a false feed being present in the selection circuit the signal is made to show red, a quality of " Fail Safe " that conventional circuits do not contain under these conditions. Proper design, installation and maintenance is made to guard against such a failure.

The latter circuit, although over simplified has demonstrated some factors in assessing the equipment and circuit form to meet " Fail Safe " requirements.

5.3. Circuit Form.

5.3.1. General.

Mention has been made as to the possibility of a false feed in the circuit causing a false " Clear."

The need to use a circuit form to protect against open circuited contacts, broken wires or connections and failure of supply, all of which may be regarded as the most common form of failure possibility, makes the circuit used vulnerable to the less likely form of failure caused by a fault connection between independent circuits. The false feed arising from this condition may then create an unsafe condition.

It is necessary to give every consideration to prevent the possibility of this happening. A most likely position for such circuit inter-connection to take place is in the cabling between the circuits in the relay room and the trackside equipment for the operation of the points, signals and track circuits. For this reason great care is needed in the design, manufacture, installation and maintenance of the cable system.

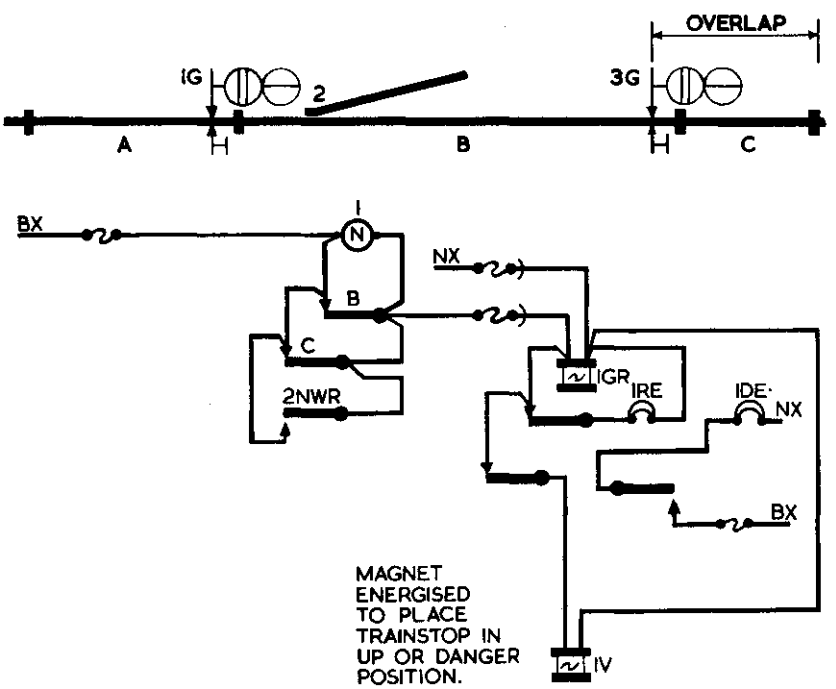

Fig. 6B. The Signal Circuit Designed for Power Economy Alone and with Normally De-energised Track Circuits.

5.3.2. Cable Form Influence.

For many years a cable has been used consisting of two insulated conductors surrounded by an outer lead sheath to allow the feed and return of a circuit to be enclosed within a protective earth screen. This ensures a high degree of immunity for circuits under cable fault conditions, provided the lead sheath of the cable is properly included in the earth connected circuit, see Fig. 7.

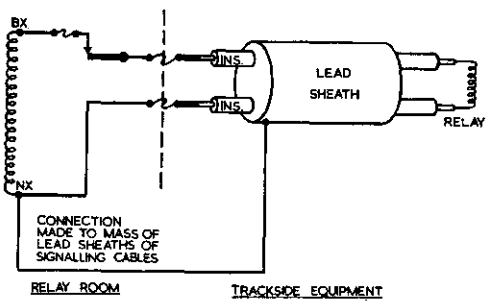

Fig. 7. Cable Form.

This circuit, described as a single cut circuit, since the selection contacts are contained only in the BX pole, will cause a fuse to blow should a fault occur within the cable to bring the BX conductor in contact with either the NX conductor or the lead sheath of the cable. The circuitry within the relay room is wired with a single-conductor heavily insulated wire. It is run in hooks so as to be completely visible in a tree form, usually not containing more than 150 wires. The possibility of wires coming into contact with each other is thus avoided in the sheltered conditions of the relay room. The wire-run hooks are mounted on metal strapping which is connected to the earth system of the lead cabling. Within the relay itself, and its contacts used for the circuit selection, a design of assembly is used to obviate the possibility of the improper bridging of the contact or the connecting together of adjacent contacts, again to cause circuits to be falsely fed.

This metal casing of the relay is connected to the metal of the rack on which it stands, and the rack is in turn connected to the lead of the cabling system. An earthed wire or an earthed circuit of a relay will therefore again blow a fuse and provide safety.

An earthed wire of the NX circuit will not blow a fuse but this is not unsafe, since there are no selection contacts in the NX circuit. Periodic tests are necessary to determine the continuity insulation of the NX wiring.

The provision of an individual return wire for each separate equipment or apparatus function gives protection against a fault condition in the return wiring, see Fig. 8.

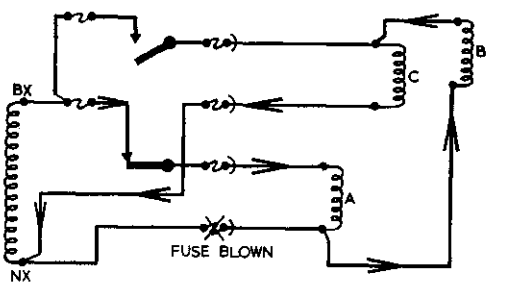

Fig. 8. Common Return Failure.

This fault, as shown in the diagram, arises when the returns of circuits are commoned, but the feed circuits are separate. The return current of relay A is made to flow through relays B and C in series, with the possibility of falsely energising these relays. With common returns there is a variety of ways for this fault to occur. To avoid this form of fault the return circuits for each supply should be separately connected to a point as close to the supply transformer as can reasonably be made.

An alternative to earthing one pole has been made to provide earth detection equipment to indicate the state of insulation of both poles of the system. Some difficulty has been found in using this method, as the leakage capacity of the line cables varies considerably between the BX and NX poles, depending upon the selection circuits made up on the BX pole. In addition, and perhaps of greater importance, a line earth fault appears and disappears upon the circuit conditions. This creates difficulty in tracing such a fault and tends to promote an outlook on the part of the maintenance staff that the fault is not worth pursuing as it has in all probability cleared itself. In this respect the fault that blows a fuse

and makes itself evident, even if delay may be caused, has the merit in demanding instant attention and by so doing possibly averts a more serious fault condition arising from the existence of more than one line fault.

It is worthy of mention, although only indirectly concerned with safety, that the use of lead covered cables on a railway system with an electric traction system makes necessary the observance of a strict code of practice in order to prevent traction fault currents passing through earth from damaging the lead cables.

With the proved use of plastics and the improved cables obtained, coupled with other changes in equipment and system requirements, it is proposed to make considerable changes in circuit arrangements for future signalling installations.

6. VICTORIA LINE CIRCUITS

6.1. Relay Design.

The standard relay used on the London Transport Board for many years has been the A.C. vane type of size approximately one cubic foot. A smaller D.C. relay is now available to a B.R. specification in size approximately one tenth of a cubic foot, that obviously offers great advantage in reducing the size of relay rooms. The relay also offers a great number of contacts. The relay is converted to A.C. operation by the use of diodes, now of a size and reliability to make this conversion method worthwhile.

The present form of A.C. relay is fitted with a detachable top to enable relay changing to be made without the disconnection of wires. This feature has been reproduced in the new relay, but

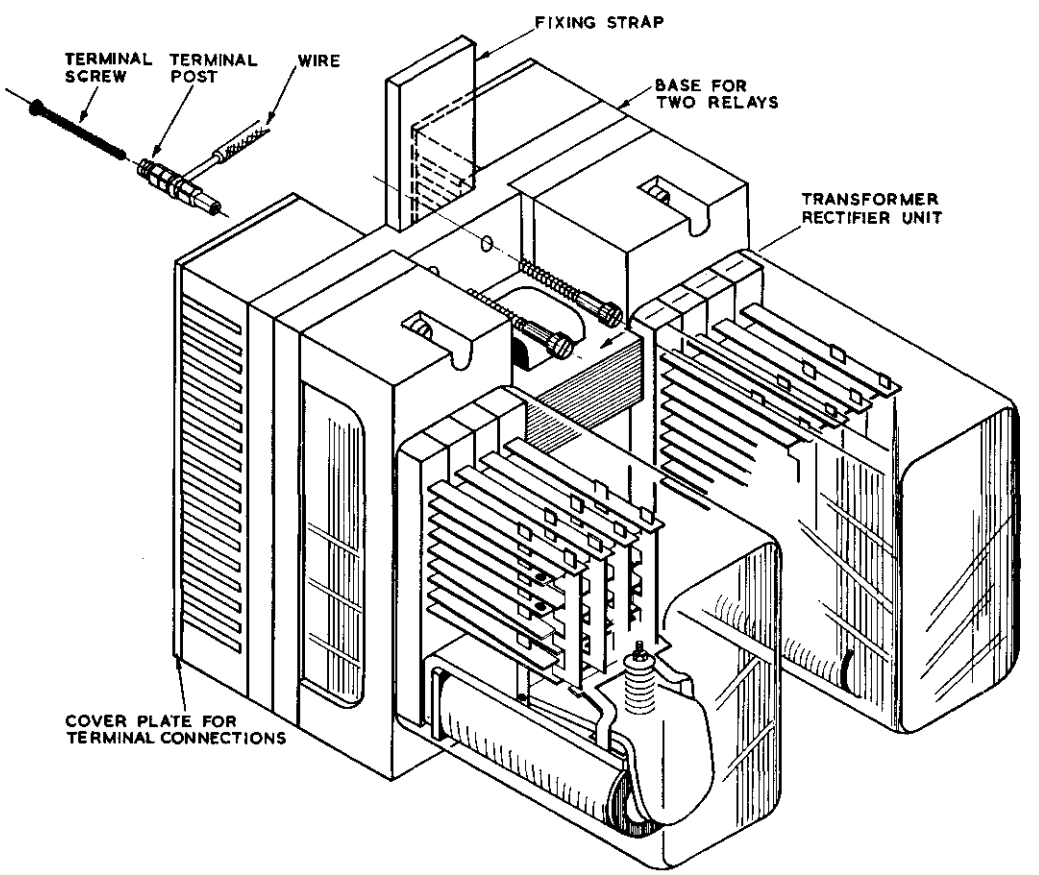

Fig. 9. Standard Line Relay Unit.

as a small number of failures have been recorded with the present form of detachable top due to the spring loaded contact arrangement, opportunity has been taken to redesign this part of the new relay to make each terminal connection by a screw. The screw of each terminal, when removed to detach the relay, will keep the wires connected to their respective terminals on the relay base, see Fig. 9.

At the same time as adopting the new design of relay, consideration was given to the conditions that apply when train movement is entirely automatic, both for driving of the train and also for route setting.

When the system no longer includes the supervision exercised by the driver and signalman, and which cannot be regarded as being adequately replaced by the train operator or regulator, a greater responsibility is placed on the safe functioning of the signalling equipment.

6.2. Circuit Design.

To meet this additional requirement it has been decided to duplicate the relay, so that in the event of a relay failing to open its front contacts when it should, a second relay can be depended upon to perform this function. As shown in Fig. 10, in terms of size the two relays mounted upon a single base are still smaller than the original A.C. relay and the cost of the complete double relay unit compares favourably with the A.C. relay with its detachable top.

The contacts of the two relays will be used in a " double cut " form of circuit with the contacts of one relay always used in the BX pole and the contacts of the other relay used only in the NX pole.

For convenience of testing each contact of each relay in a circuit, three terminals are provided on the front of the relay unit base below the transformer and diode bridge to allow each relay winding to be bridged in turn and so test the circuit by opening one selection contact at a time. The three terminals are connected to the D.C. coils of the two relays wired in series, and a three position switch connected by temporary test wiring bridges one or other of the relays when the switch is operated away from the mid-position. A coincidence circuit is used on each relay so that should a relay remain falsely

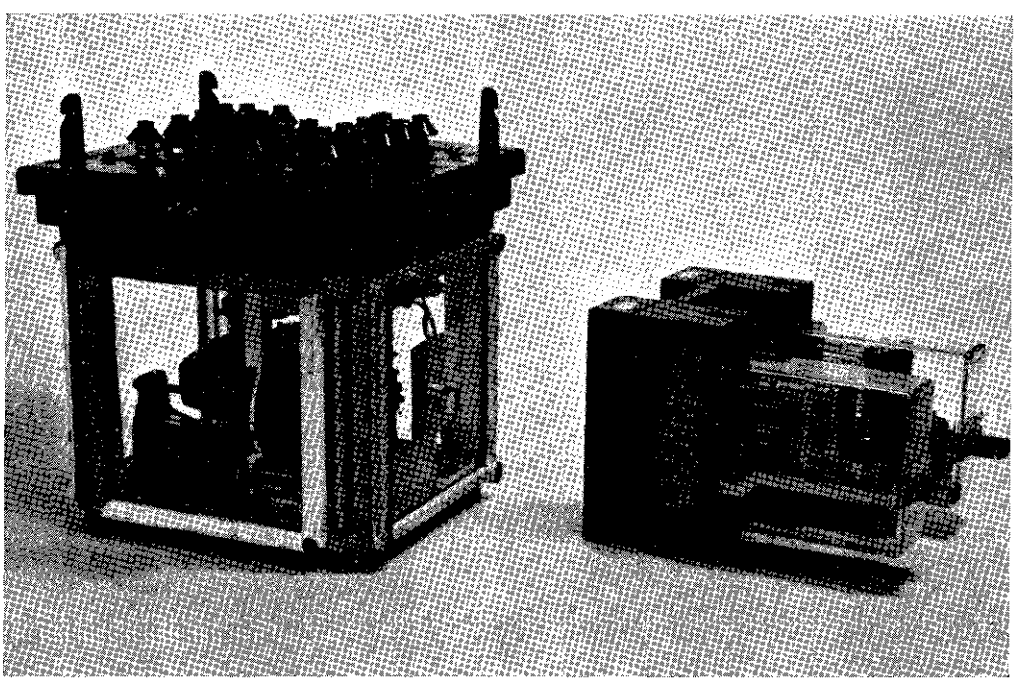

Fig. 10. Old and New Relays.

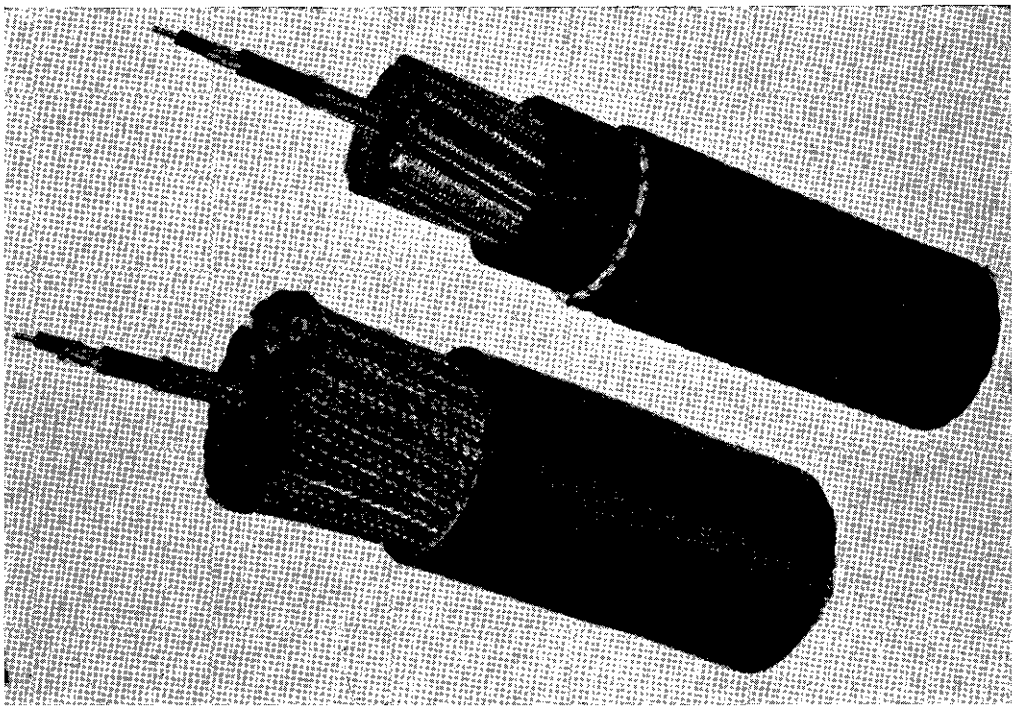

Fig. 11A. New Multicore Cable.

"Up" a warning is sounded in the regulating room of the fault condition.

Using the NX pole for selection purposes then makes it necessary to insulate this pole from earth and the circuit form as previously used is no longer suitable.

6.3. Cable Design.

The opportunity has also been taken to redesign the standard cable from a lead covered 2-cored cable to a multicored cable with plastic covering which, when used in tube tunnels, will also have a finished covering of asbestos treated with a fireproof Neoprene paint. Each of the two conductors within the cable used for the BX and NX supply of a circuit will be protected by a covering screen of copper to prevent faults within the cable causing isolated circuits to be brought into contact with each other. Fig. 11A shows photographs of specimens of this type of cable, and Fig. 11B shows a pictorial view of the cable.

Fig. 12 shows the circuit form employed. As the cable has no lead sheath there is no danger of the cable carrying 600V. D.C. traction earth fault current. Also both poles and the supply transformer centre tap of the secondary winding are free from earth. The circuit will cause a fuse to blow should a fault appear between the BX centre core and the NX stranded concentric conductor, as well as for a fault between the NX concentric conductor and the concentric braided fault screen.

The fault between BX and NX legs of the cable is likely to cause both the BX and NX fuses to be blown. The fault between NX and fault screen will

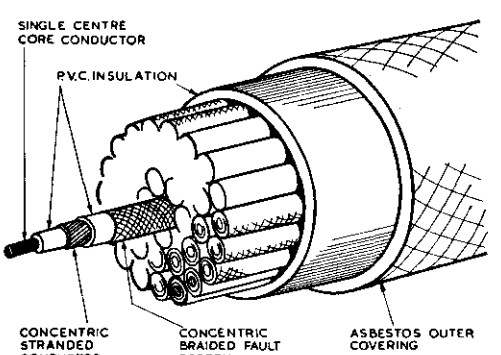

Fig. 11B. Multicore Cable.

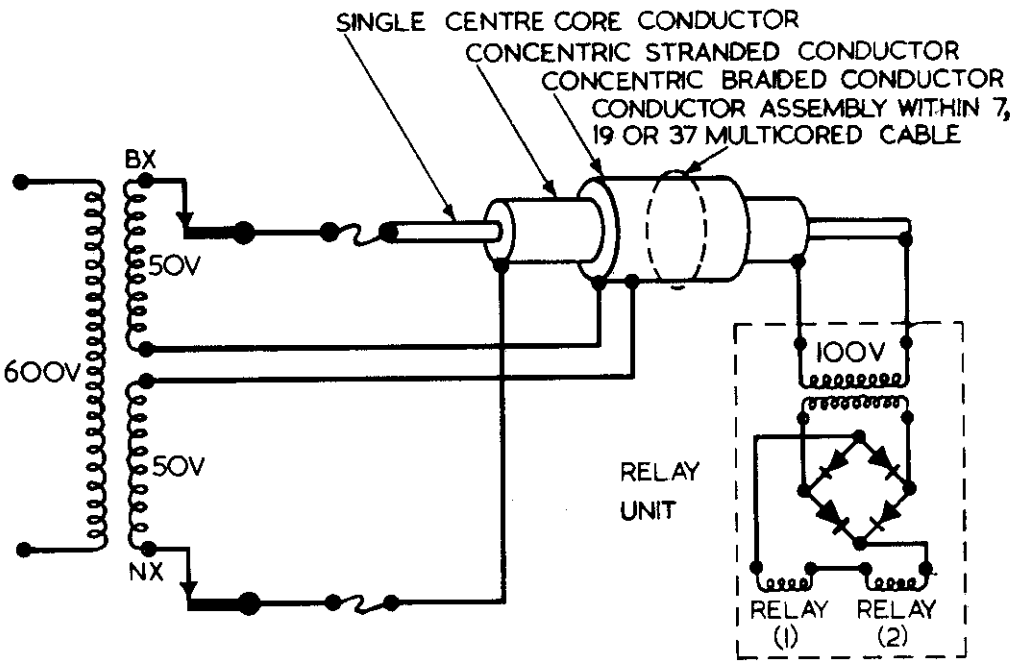

Fig. 12. Victoria Line Circuit Form.

place a short circuit on only the NX half of the secondary winding and hence only that fuse will be blown. The normal characteristics of the D.C. relay gives a ratio of approximately one to two for the hold up to normal relay voltage.

The 50 volts then available on the BX pole to screen when the NX fuse is blown may be sufficient to hold up the relay under this fault condition. The relay unit has been so designed by making use of the diode characteristic that a voltage level of 0.75 V. is required before current is passed to the relay. Fig. 13 illustrates the relay operating values compared with the A.C. input voltages. The relay unit will pick up at 80 V. and drop away at 60 V. There is then an adequate margin to be sure that the 50 volts present in the circuit when an NX fuse is blown will not be able to close the front contacts of the relay. This form of multi-cored cable gives similar protection against line faults as did the lead covered cable.

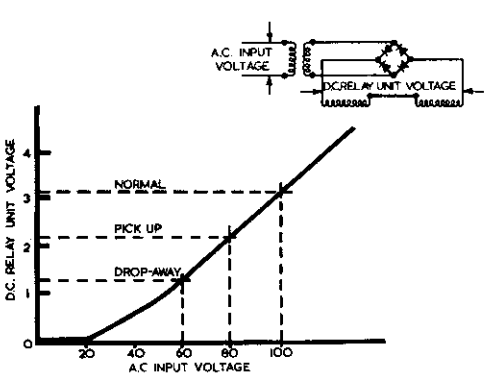

Fig. 13. Characteristic Curve for A.C. Line Relay.

6.4. Effect of Circuit Faults.

Fig. 14A illustrates a condition set up on the assumption that one of the relays maintains its front contacts in the closed position although the relay is de-energised. In the diagram the contact in the BX pole is falsely closed and the contact in the NX pole is opened. The BX supply is taken to the relay coil by the centre conductor and returned from the coil to the concentric conductor where the circuit is then broken to NX by the open circuited relay contact. The connection to the secondary winding centre taps from the fault screen is then coupled to the NX concentric conductor by the cable leakage capacity existing between the NX conductor and the fault screen (C2). Since

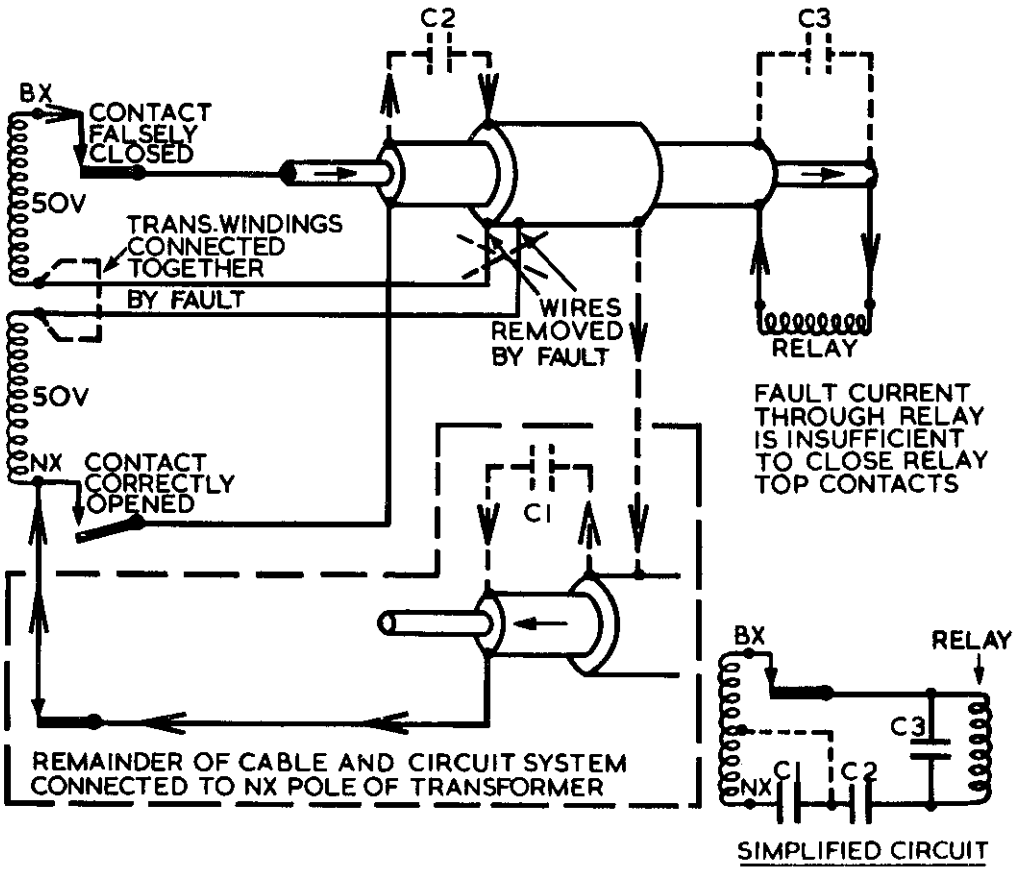

Fig. 14A. Circuit for Fault Condition on BX Pole.

the voltage of the supply across one half of the supply winding is 50 volts the relay will not be energised to close the contacts. If it is assumed that the connections to the supply winding centre tap are disconnected from the cable fault screen in such a way as to keep the two windings continuous and complete the transformer circuit, a path will then be offered to the current in the cable fault screen via other fault screens and their capacity (C1) to the NX pole circuits completed to the transformer NX terminal.

For purposes of assessing the effect of these leakage capacities, C1 is assumed to be of infinite capacity giving zero impedance. The circuit is shown in simplified form and the 100 volt supply is fed in series with C2 through the relay coil. Condenser C3 acts as a shunt across the relay coil. Making the worst possible assumption, that this screen is disconnected the voltage on the relay is insufficient to give false operation.

Fig. 14B is drawn to illustrate the effect of a relay contact in the NX pole being falsely closed and the contact in the BX pole being opened. Here no connection to the BX pole is offered in any way and no voltage is developed across the relay winding.

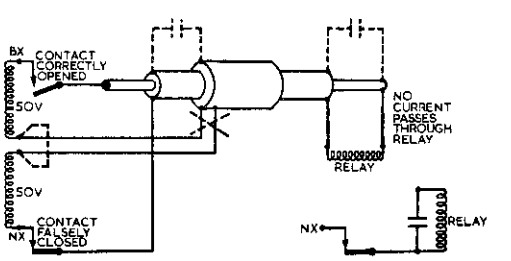

Fig. 14B. Circuit for Fault Condition on NX Pole.

Fig. 15 shows the effect of increase in cable length on voltage developed across the relay winding due to effect of cable capacity on a circuit fault condition. The natural capacities between the conductors of the cable are in the ratio of two to one and the diagram shows that the cable length needs to be in excess of 1,000 yards to energise the relay under the fault conditions previously described. Should a longer length of cable be needed, a four terminal condenser will be used at the fuses in the relay room, to increase the effect of condenser C3 and reduce the relay voltage. The effect of this capacity increase is also shown on the diagram. A four terminal condenser is specified for this purpose to ensure an open circuit in the lines should this condenser become disconnected at its terminals.

6.5. Effect of Circuit Isolation by Transformers and Code Feed units.

With the use of equipment that creates an isolation from the main supply circuits, additional connections to the cable fault screens are necessary. Fig. 16 shows an arrangement to provide for this contingency. A busbar form of connection is made to the screens of each multi-cored cable and the cables to the main supply transformer are sweated to the busbars to prevent casual disconnections being made. The making of the transformer centre tap connections and the connections of the isolating transformers, etc., to the screen system in a form as illustrated obviates the effects caused by broken return circuits.

6.6. Coded Track Circuits.

With the introduction of automatic train operation and the consequent use of coded track circuits, it is necessary to use double rail track circuits. The leakage effect from a common rail is shown on Fig. 17. For convenience it is assumed that the length of each track

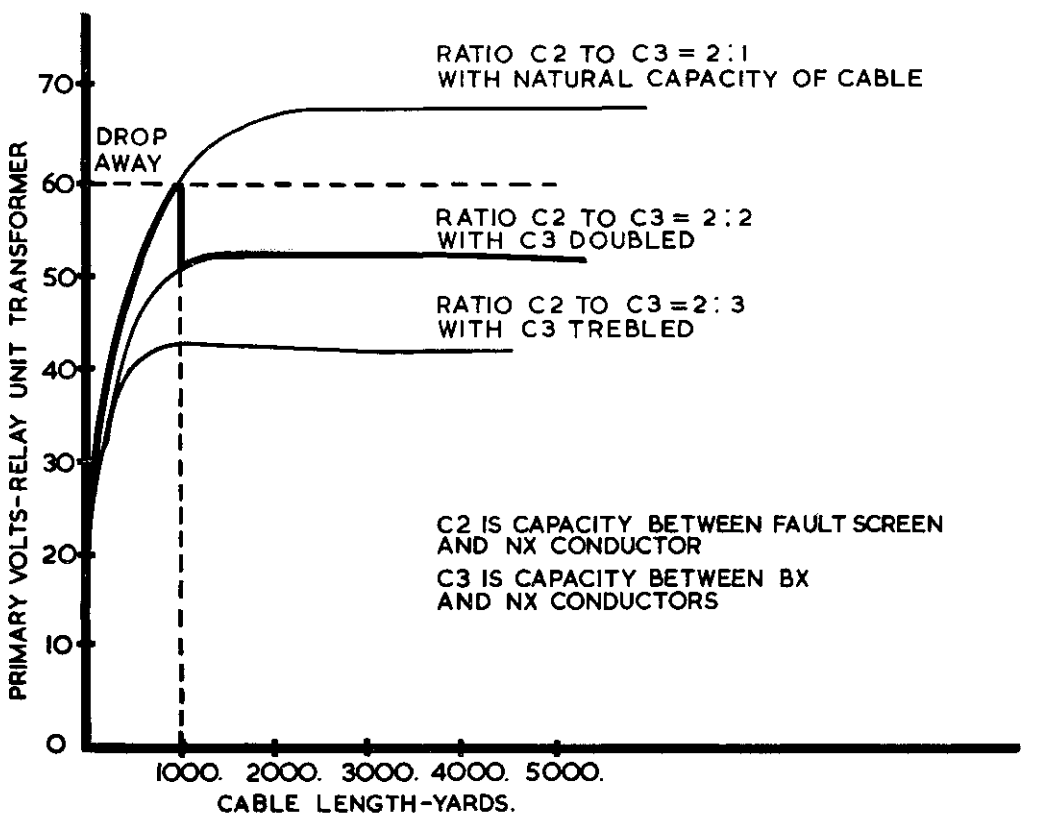

Fig. 15. Cable Capacity Leakage Effect.

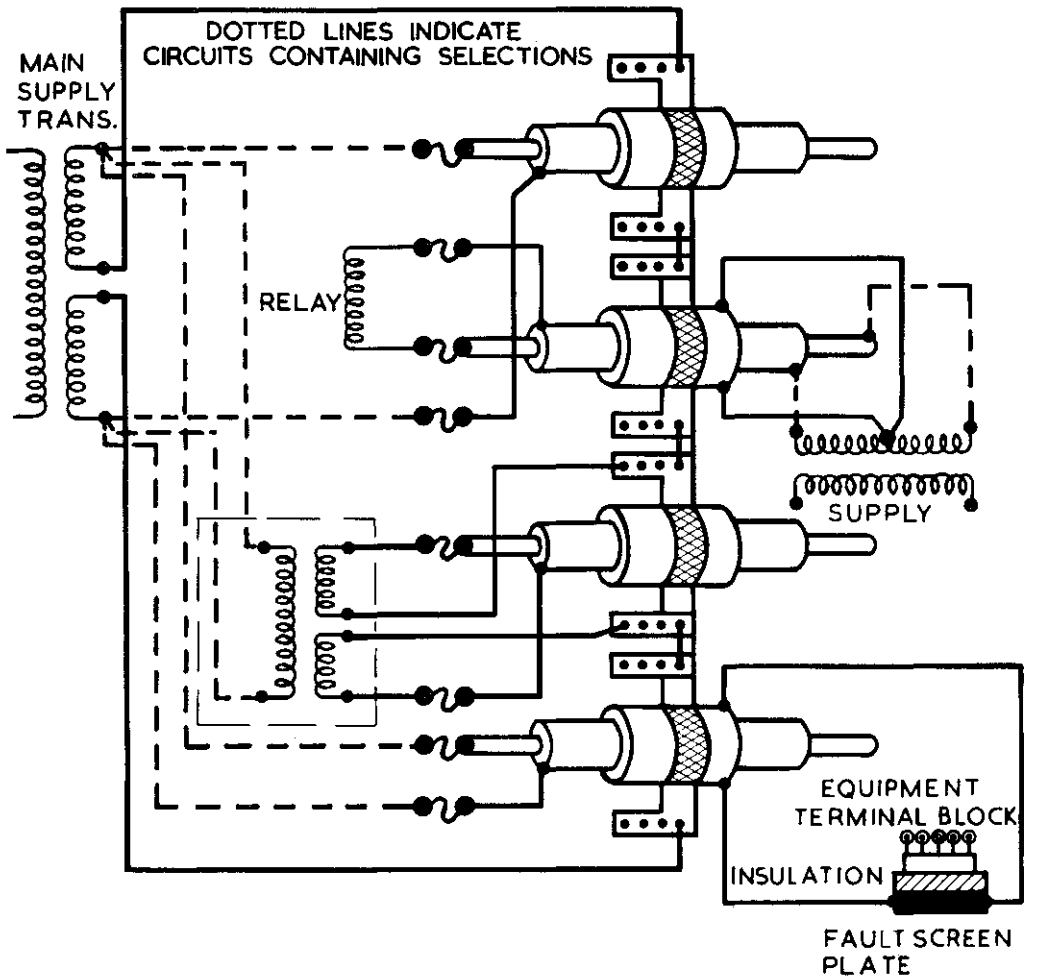

Fig. 16. Fault Screen Connections to Cable and Equipment for Circuits isolated by Transformer or Code Feed Units.

circuit is similar, and were the values of the rail to earth leakage resistance the same for each section no adverse effect would be found. Where, as so often happens, the leakage resistance of a particular section of the common rail is lower than in the neighbouring sections, then the track circuit current in the common rail is a summation of the feeds from adjoining track circuits. In the diagram it is shown that the feed current from track circuit A passes to earth from the section rail and to return to the common rail takes the path of lowest resistance, shown to be track circuit E on the diagram. The return path then includes the common rail for track circuits B C D in addition to track circuit E. With a coded track circuit it is then obviously dangerous to allow this to happen as it would then be possible to

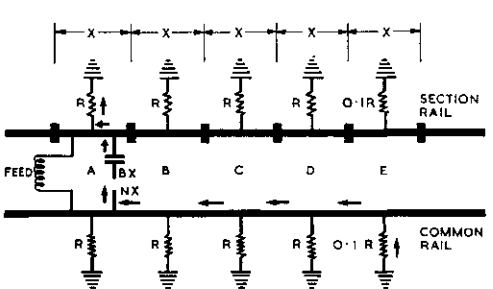

Fig. 17. Single Track Circuit Earth Leakage Effect.

inject a false code into track circuits B C D and E giving rise to a possible wrong side failure condition. Accordingly, double-rail track circuits are used.

6.7. Protection against Traction Earths.

The common or continuous rail has been used on London Transport with its fourth-rail traction system to give protection to personnel in the event of an earth fault appearing in the insulation of the train system. An earth fault on the positive pole of a train on one part of the system will pass fault current to another train with a negative pole fault in another part of the system. This fault is intended to trip the circuit breakers in the sub-station and reduce the voltage level between the train bodywork and surrounding surfaces of tunnels and platforms and so on, with which passengers or staff may come into contact. With the use of double-rail track circuits and the abolition of the continuous rail an alternative method of circulating traction earth leakage fault current is to be employed.

6.8. Double-Rail Track Circuit Form.

6.8.1. Traction Fault Protection.

Fig. 18 shows the use of a traction current fault wire to provide for traction leakage currents. It is most important from the track circuit point of view to prevent the circulation of D.C. traction current in the track signalling equipment. One connection only is made on each track circuit to the fault wire and it is made at the entering end of each track circuit. The connection from the track circuit rail is proved by using the wire as part of the track circuit connections, and should it become severed then the track circuit will be effected and made to fail. The fault wire connection to the track circuit is made at the relay end of the track to prevent code interference to the train should a failure of block joint occur.

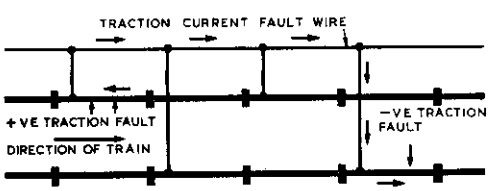

Fig. 18. Double Rail Track Circuit with Traction Current Fault Wire.

6.8.2. Effect of Blockjoint Failures.

6.8.2.1. Effect on Track Circuit Operation.

Fig. 19A shows the effect on track circuit operation of blockjoint failure and in the diagram the blockjoint in the top rail is assumed to be shorted. The feed of track circuit B is then given a short circuit path through the top rails of tracks B and A to the fault wire on A track. The current continues towards the fault wire on B track and returns on the bottom rail to the feed unit. BTR is therefore shunted.

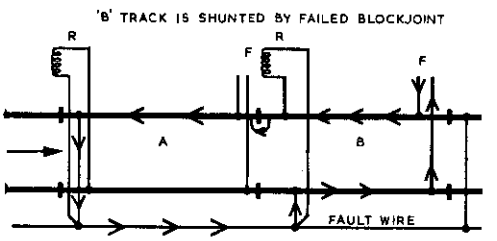

Fig. 19A. Double Rail Track Circuit Effect of Blockjoint Failure (Top Rail) on Track Circuit Operation.

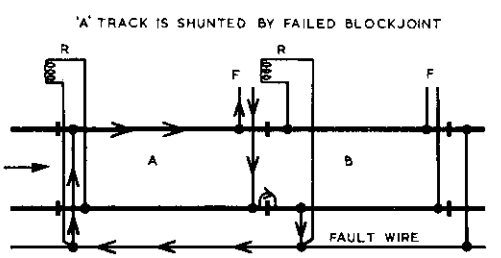

Fig. 19B. Double Rail Track Circuit Effect of Blockjoint Failure (Bottom Rail) on Track Circuit Operation.

Fig. 19B assumes the bottom rail blockjoint to have failed and in this case A track is short circuited via the fault wire connection on B track.

In the event of both blockjoints becoming short circuited simultaneously, both tracks A and B would be made to fail. It is also to be noted that the relay unit is made to be phase conscious so that the feed of A track will not energise

the relay unit of B track when both track circuits are operating on a common code.

6.8.2.2. Effect on Train Code.

Fig. 19C shows the effect on the pick-up code on the train with a blockjoint failure in the top rail of the diagram. For this position to be reached it must be assumed the blockjoint failure occurred after the train had occupied A track. If the blockjoint failure had occurred before the train had reached A track then the signal selection arrangements would place a 120 or " trip " code on the previous track circuit and the train would have been stopped. It is to be expected therefore that a blockjoint failure would generally be observed by a track circuit failure preventing a train from reaching the failed track circuit. The possibility of the train attempting to read the code of B track when occupying A track is therefore small. Although a small risk the matter is provided for. The feed of B track flows along the top rails in the diagram of B and A tracks and returns to B track via the fault wire. No current flows in the bottom rail of A track and as the train code receiver unit requires

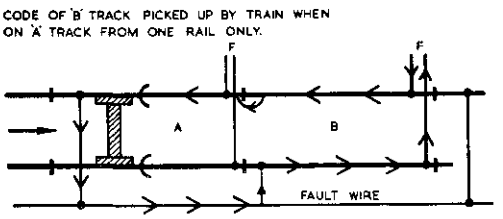

Fig. 19C. Double Rail Track Circuit Effect of Blockjoint Failure (Top Rail) on Train Code.

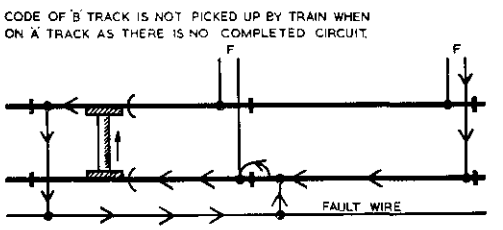

Fig. 19D. Double Rail Track Circuit Effect of Blockjoint Failure (Bottom Rail) on Train Code.

to read current as being present in both rails the train will be " tripped " and brought to a stand.

Fig. 19D shows the effect of a blockjoint failure in the bottom rail. Again the current of B track flows in but one rail of A track resulting in the braking of the train.

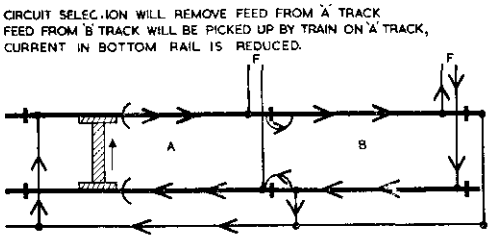

Fig. 19E. Double Rail Track Circuit Effect of Blockjoint Failure (Both Rails) on Train Code.

Fig. 19E shows the effect of the failure of both blockjoints. B track feed then flows in both rails of A track but the current in the bottom rail is reduced by the alternative path offered through the fault wire.

It is likely that the effect of the reduced current coupled with the resistance effect through the blockjoints will produce a " tripping " of the train. This cannot entirely be relied upon, however, and other assurances are necessary.

The four code rates in use are 120, 180, 270 and 420 codes per minute. The higher the code rate observed by the train the less restrictive is the effect on train control. The effect of the code of B track appearing in A track is only of a serious character when the code of B track is higher than that of A track. Circuit selection for each of the track feeds is arranged to include all track circuits, point detection, etc., required for safety of train spacing, etc. For the general case, therefore, no danger will arise should the level of the signal of B track to the train on A track not cause a trip operation.

It is possible for track circuits to be coupled by blockjoint failure at crossings and junctions and the code on the adjacent track circuits be unrelated, also sections of line where speed restrictions are enforced by the use of a lower code will be exceptions to the general case.

In such cases the use of a rail circuit as shown on Fig. 20 will be considered. Four blockjoints will be provided with a metallic short section between them. These blockjoints may be of a pattern commonly used on London Transport where the short section of rail is 11′ 6″ in length or in junction work where there is difficulty in positioning the blockjoints a design may be used of a special pattern where the short metal section will not exceed some inches in length. The two relays will be normally energised from a D.C. supply and the detection of the relays arranged so that with one relay de-energised an alarm is given, but with both relays de-energised tracks A and B will be de-energised and prevent train movement on both main roads. A failure of blockjoints W and X will shunt Relay No. 1 and a failure of blockjoints Y and Z will shunt Relay No. 2 through the track circuit ballast leakage and track circuit equipment windings.

7. SOLID STATE CIRCUITS

7.1. General.

The application of solid state circuitry to "safety" type circuits has been the subject of papers read to the Institution particularly that in February 1962 by Messrs. Heald and Gore, but so far their use has been very limited. The inability to devise a form of test that will give the same degree of assurance of reliability of operation as can be obtained for the conventional circuit and equipment form prevents greater use of forms of electronic circuit, attractive as they may appear to be in other ways. Particularly is this so for semi-conductors which despite continued consideration of testing techniques at present remain in the eyes of the Signal Engineer largely unpredictable for length of life required and generally unsuitable for "fail safe" purposes.

A form of circuit using semi-conductors was explained in a paper given earlier in this session in a Paper by Mr. V. H. Smith on Victoria Line signalling principles, and it would seem that given suitable design of card form assembly and terminal connections as meeting "fail safe" requirements, the circuit principles may prove themselves to be of this standard.

Research very rightly continues to examine forms of development of systems to replace the conventional track circuit as the basic train detection device. I have seen in America a very expensive and highly ingenious test project using "wiggly wire" for train detection and a computer system to control spacing and speed and so on. The safety of the system was said to be guaranteed by redundancy methods.

7.2. Programme Machine and Remote Control Equipment.

For various reasons electronic circuits are essential in their use when concerned with methods of signal and route operation required to replace the "non-safety"

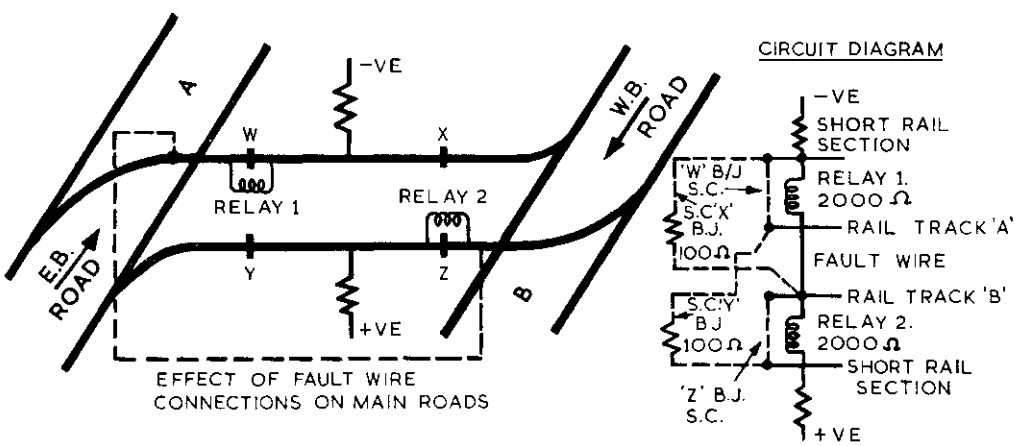

Fig. 20. Blockjoint Detection Rail Circuit.

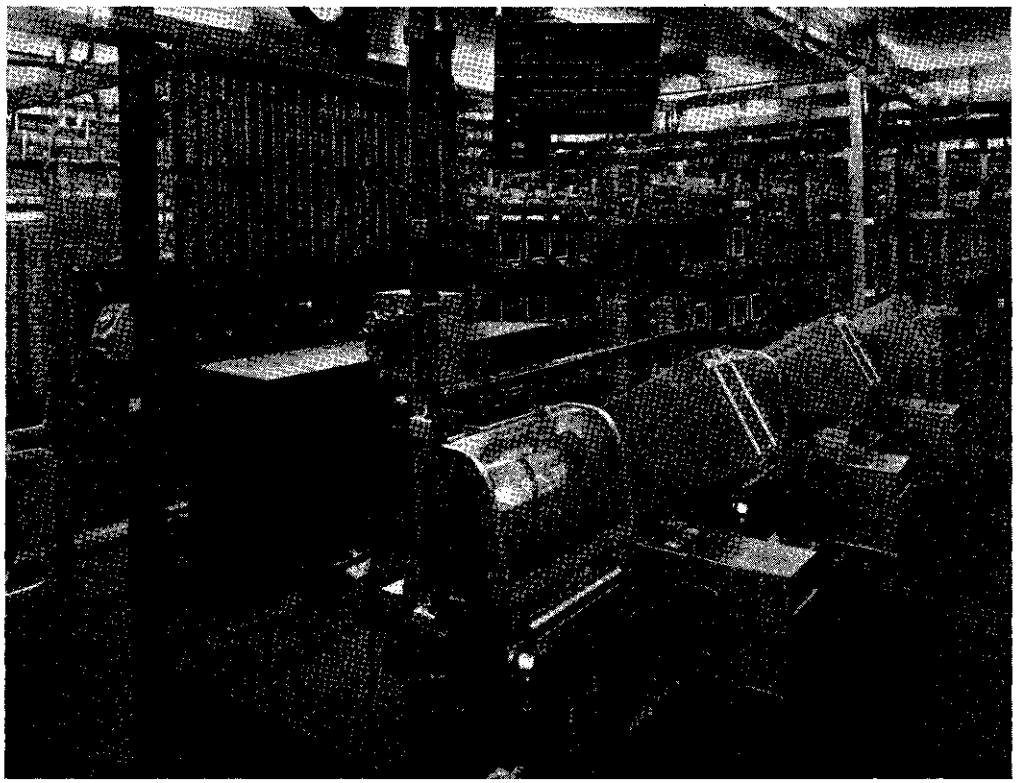

Fig. 21. Separation of Safety and Non-safety Equipment in Relay Room.

lever movement function of the signalman. This then results in there being two classes of circuit standard 'safety' and 'non-safety.'

Fig. 21 shows a relay room layout used to preserve the clear demarcation between the two systems. A layout of apparatus and wiring is used that separates into independent physical groups the parts of the system associated with safety and non-safety requirements. By this means it is possible to gain the maximum economical benefit in reduction of size of equipment, use of standard commercial apparatus, wires of reduced insulation and size, and so on, for non-safety purposes and to easily observe that the required standards are maintained on the safety equipment.

7.3. Coded Track Circuit Relay Acceptance Unit.

A magnetic amplifier, whilst having the advantage of a solid state circuit, embodies characteristics of design that with proper test and inspection is able to be used for "fail safe" purposes. An iron circuit and its magnetic response to a control current to give impedance change of an A.C. winding can be relied upon once the necessary quality of design, test and inspection have been determined. The use of magnetic amplifiers for the track relay of a code acceptance unit is shown on Fig. 22. The coded 125 cycle supply from the rails supplies power to the control winding of magnetic amplifier No. 1 provided the correct phase is obtained in relationship with the 125 cycle supply obtained from one winding of the supply transformer. With the impedance so reduced of this magnetic amplifier's A.C. windings, current is then raised in this circuit to pass D.C. power into the control windings of magnetic amplifiers Nos. 2 and 3. With the impedance of their A.C. fed windings also reduced, power is then fed via a second and similar stage of amplification to pick up two Style 'Q' Relays in series. The

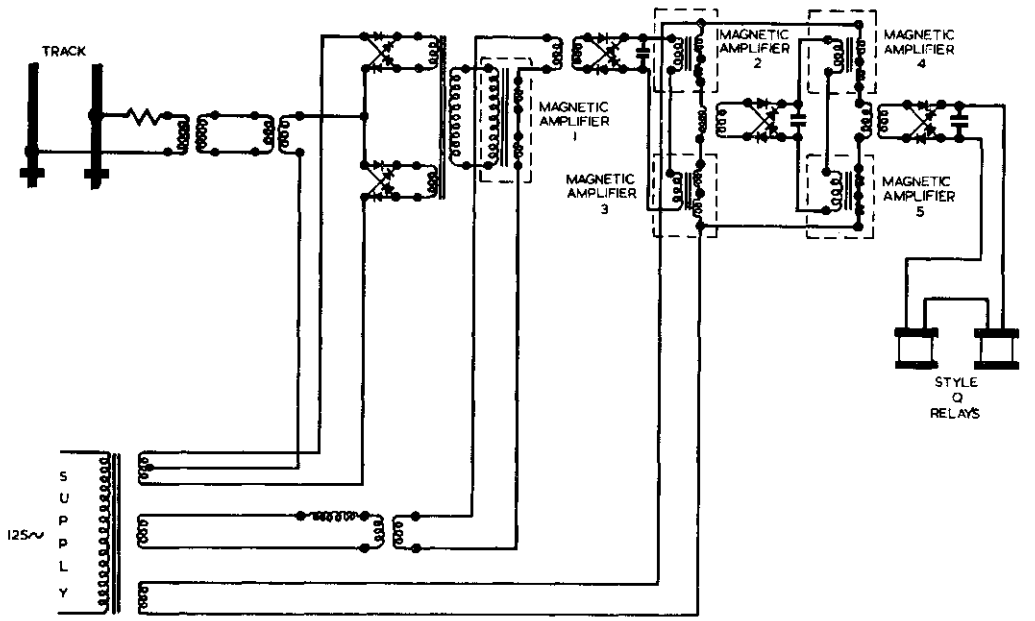

Fig. 22. Track Relay Code Acceptance Unit.

A.C. windings of the magnetic amplifiers are wound with approximately ten turns of P.T.F.E. insulated wire and with so few widely spaced turns, protection against the possibility of short circuiting of this winding, which would be a wrong side failure condition, can be assured. In addition to this, each magnetic amplifier's A.C. winding in the amplified stage is duplicated so as to give a double cut circuit effect and further circuit protection.

7.4. Train Code Acceptance Safety Unit.

Fig. 23 shows the circuit form used for the unit used on the train to give the safety controls to the train operating circuits. It again shows the use of magnetic amplifiers in double cut circuit form and this also includes the output from the pick-up coils into the amplifier. Code must therefore be present in each rail and at a required level in order to transmit the power to the emergency brake valve operating circuit at the output stage.

8. FAILURE OF EQUIPMENT

8.1. Statistics.

Effort is constantly maintained to reduce the numbers of failures of signalling equipment and the delays to train service and passengers that they cause. One of the most rewarding methods to lead to such a reduction is to keep a careful record and category analysis of all failures as they occur. The lessons learned from this study enables designs to be amended, maintenance methods to be improved and also for the procedure for dealing with failures to be considered and possibly reduce the delay time for future incidents. There is much to be learned therefore from such studies. I believe it would help to reduce the failure rate if information was to be made generally available to railways at large, detailing failure statistics for all railways in this country. The opportunity this would give for comparisons to be made between systems, conclusions to be drawn and action to be taken would be most beneficial. Fig. 24 shows the manner in which failures in the L.T.B. system have been reduced over the years, despite a large increase in the number of units in operation. For such comparisons as I propose to be made it would first be necessary to use a standard procedure as to failure analysis, and in my view this Institution would serve a useful purpose if a report could be made by a committee to recommend the adoption of such a code of

practice, and for an annual review to be made of the results. American technical journals publish in some considerable detail the annual record for failures of signals and systems for their railroads. Each railroad is named and under three main groupings of (i) " False restrictive failures," (ii) " False proceed failures," and (iii) " Potential false proceed conditions," failures are listed of the types of signalling system concerned. It is of interest to note that for 1965 there were 28,082 false restrictive failures, 52 false proceed failures and 5 potential false proceed conditions. The track mileage for which these figures apply would seem to be approximately 172,000 and there would therefore be approximately one failure per six track miles per annum. A similar figure for the L.T.B. system for 1965 is approximately one failure per track mile per annum. It is, of course, also relevant to consider the number of train movements made during the given period since, I suggest, it is likely that the number of failures are closely related to this factor.

The American figures suggest that one " wrong side " failure occurs for approximately every 4,600 " right side " failures. In terms of L.T.B. failure rate this would represent about one " wrong side " failure every nine years ; and within the very rough comparisons made this figure gives a measure of agreement.

8.2. Measurement of Safety.

From the statistics obtained by such methods it is obviously possible to calculate the factor of safety obtained by the working of the system.

To what extent is it possible to prophesy the safety factor for future working of a system ?

I have seen a description of a statistical method used in the design of equipment employed for blind landing of aircraft, published in a technical journal, that went on to criticise the London Transport system proposed to be used for the Victoria Line. The article stated it was believed the signalling system was based on the judgment of the Signal Engineer to satisfy absolute safety, instead of a method of calculation that would not only satisfy the requirement of safety but achieve this result with economy. The logic of this argument proceeded to suggest that the financial savings would produce lower fares, and thereby reduce the number of people using cars and so in turn reduce the number of road deaths.

I entirely agree with the suggestion that statistics should be used in an

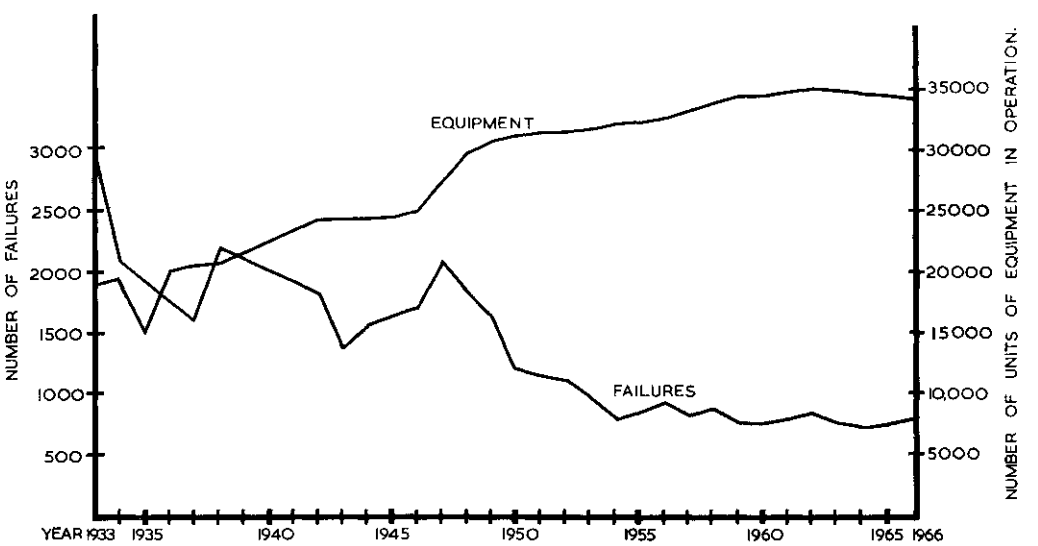

Fig. 24. L.T.B. Signalling Equipment Failure Record.

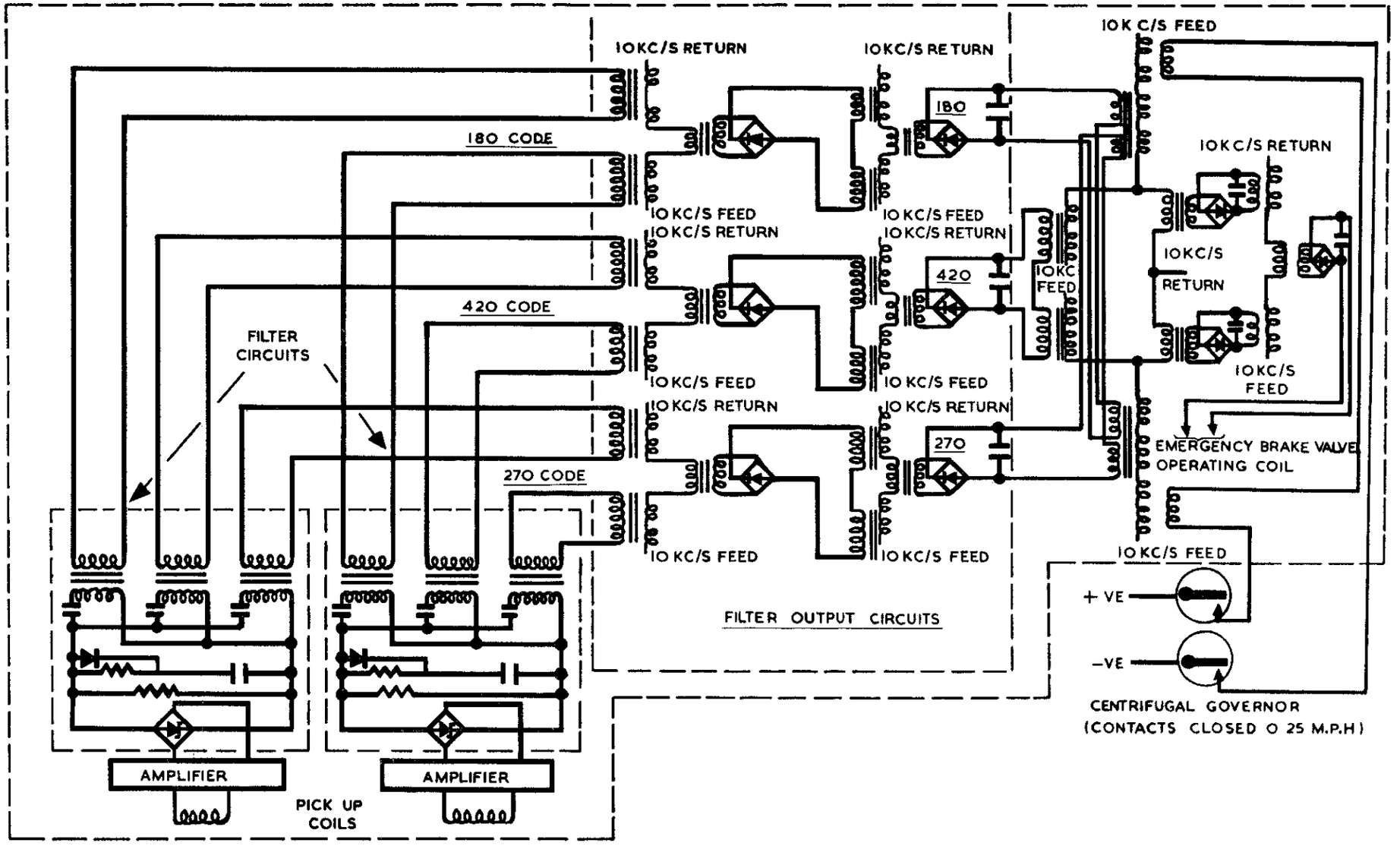

Fig. 23. Train Code Acceptance Safety Unit.

endeavour to assess for design purposes the failure rate of a system. Where I think the article completely misses the point is that such processes can be no substitute for the judgment of the engineer, and only by judgment can statistics be employed as an aid to calculate the future failure rate.

The method is based on obtaining a known failure rate of basic items of equipment, resistances, condensers, and so on, and from these values to assess the overall failure rate of equipment assemblies. Allowances are also included as to the proportion of failures that are right side to wrong side and incidents resulting, non fatal to fatal.

It is my experience that equipment failures of simple resistances can be quite random and dependent upon a considerable number of variables. When applied to system use the failure rate found in the aircraft industry would I suggest be quite different from that found for the same component when used on an Underground Railway system, due to change of environment and conditions. I would also expect to obtain different failure rate results if a similar piece of equipment was purchased from two differing manufacturers, although to the same specification. There may also be anticipated a variable failure rate if a similar piece of equipment was obtained from one manufacturer but delivery was from differing batches, or with a time interval between deliveries.

It is my view that the forming of statistical information can only be done by particular service experience, and cannot be done by blind adherence to mathematical formulae. Judgment must be applied to make comparison between the circumstances. Much of the statistical data now available has been gathered as result of developments in the computer, guided-missile and similar spheres. A life expectancy of 1,000 hours for such equipment is often quoted; a signalling installation is made on the basis of a 30 to 40-year life. The working conditions of a railway are very different from those normally found for the usual form of electronic equipment, and the results obtained in service as to failure rate may be quite different. Vibration, temperature variation, atmospheric conditions and air pollution cannot be controlled under railway conditions to nearly the same extent as I imagine will be found is done in general forms of industrial use.

This leads me to say that the basic statistical data required for railway systems can only be positively obtained against the background of railway conditions, and this is difficult to do with a life cycle of some 30 years. It is also an important feature that changes in technical design are now so rapid that it is very unlikely that installations made at intervals of, say, a few years apart will bear sufficient resemblance between one another to allow the experience gained on one to be used on another without a considerable measure of judgment to be used in the process.

The application of the statistical method to the blind landing of aircraft may well result in obtaining a higher standard of safety. There can be no quarrel with such a result when the apparatus is dealing with, and judged by rail standards, an operation of high risk. Here there is, therefore, much to be gained. There is, inherently within the railway system, a standard of safety obtained by bringing trains to rest in the event of failure of equipment which unfortunately the aircraft system cannot employ. The whole basis of equipment reliability and acceptance of failure form is I believe therefore different. The air is mainly concerned with the provision of "back up" and duplicate services, whilst rail generally requires an accuracy of communication, and alternative services are generally for convenience rather than safety. I would find great difficulty in bringing myself to use a process of design that had been statistically proved to be of lower safety standard than had been formerly used, and for conditions as found on London Transport I believe it would be quite wrong to do so.

Before leaving this aspect of "fail safe" I would like to pose a question to the author of the article. When the so-precisely-calculated and appointed day arrived on which an accident would happen with a signalling system designed and installed in the statistical fashion, and the author was in the position of Signal Engineer and bearing full responsibility, what would he do? If he had

faith in the system surely he dare not ignore it, nor could he prevent it. I would not care to face such a dilemma.

Records show the greater part of accidents arise in some way from that great variable the human element, and I do not believe there would be any resulting benefit in attempting to design to a failure rate statistics of 10^9, 10^{10} or 10^{11}, as suggested. For all practical purposes, as distinct from a mathematical exercise, this standard is as near 100 per cent., or absolute safety, as I could get despite the fact that the author of the article refers to these terms, hallowed though they be by Signal Engineers at large, as meaningless noises and a mental block.

Statistics cannot be a substitute for the Signal Engineer's judgment only at best a management aid.

9. REDUNDANCY

Papers have been given to this Institution describing unconventional proposals for new signalling systems, for example, that by Professor Barwell and Mr. H. H. Ogilvy in January 1966. To a question "Does the system meet 'fail safe' requirements," an answer has been given "Yes" by the use of redundancy methods. So far as I am aware no detail to amplify what is meant by the application of redundancy methods to signalling systems has been given.

My purpose in raising this issue is not to propose a solution, for this I am unable to do; but to bring to the notice of the members the important need to recognise that the subject of redundancy, and its application to signalling will, in the future, of necessity have to be resolved. The use of computers, radar and "wiggly wire" systems as being now experimented with for safety functions are said to include redundancy methods to achieve the required safety level.

In a limited way redundancy circuit forms have been used on signalling circuits where a signal relay of the two-element type has had one element controlled by contacts of track relays, and where the other winding of the signal relay is in series with the track winding of one of the track circuits appearing in the normal signal selection. By this means protection is given should a track relay be falsely held in the energised position. In this case the arrangement is done, not to recognise that the equipment is inherently below "fail safe" standards, for this is not the case; but to raise to even higher standards the "fail safe" level and for a minimum of extra cost.

Double cutting of circuits is also a form of redundancy, and as I have already described in this paper the use of two Style "Q" Relays for circuits on the Victoria Line is a further application of the principle. Where it is possible to use two relays, the use of their contacts in series gives an increase in the safety factor to guard against "wrong side" failure, should one relay remain falsely energised. The reliability of the circuit is decreased as the contacts in the circuits are doubled. This is equally true of the double-cut circuit using one relay. It would also be possible with the use of the double relay method to connect the contacts of the relays in parallel. The reliability of the circuit would then be increased against the "right side" failure but also decreased for the "wrong side" failure.

In the limit it is possible to provide complete duplication of the whole of the signalling system, including duplicate signals and cabling, and signal boxes with signalmen. This is obviously impracticable and indicates that the methods as now used are very limited in application.

To what extent is it possible to reduce the safety standard of equipment and hence cost by using redundancy methods?

To what extent can a system not based on fundamentally "fail safe" principles be restored to the required level of safety by the use of redundancy methods?

I do not know the answers to these questions, but I hope that future papers on this subject to the Institution will assist the Signal Engineer to make a decision on the matter.

10. CONCLUSION

Within the limitations of the scope of this paper I have endeavoured to explain what is meant by the term "fail safe" as I see it, and as a result of my experience on London Transport.

I am well aware that my treatment of the subject is indeed only scanty.

I believe that the matters I have mentioned regarding failure analysis and the use of failure statistics, together with solid state circuits and redundancy methods will justify their selection as single subjects for future papers purely in the context of " failsafe." This takes almost as granted that there are other points of view, and ways of achieving " fail safe " of which I may be unaware.

Finally, I wish to express my appreciation and thanks to Mr. R. Dell, Chief Signal Engineer of London Transport, for permission and no little encouragement to prepare the paper, together with my colleagues in the department who have very generously given of their time and helpful advice.

DISCUSSION

Mr. J. F. H. Tyler opening the discussion said that Mr. Hadaway had given them a most interesting paper. He did not recollect one on the subject before. He thought they should agree that no piece of apparatus was absolutely safe, and the art of designing safe equipment was a matter of lengthening the odds against false operation. One might get so far, but to go further was going to be very expensive. The only protective measure in the early days of railways was time interval working. They went from there to signals—to lever frames—to block telegraph working—to track circuits. Each stage was introduced as a result of a mishap, or some mistake which could lead to a mishap. When that happened retrospective action was begun, but because of the size of the railway system the signalling could never be said to be fully up-to-date.

There had been a very great change in outlook. It was not so long ago that they were saying, " The signalman has the Rule Book ; he has the Block Telegraph Regulations—with these we should be quite safe."

In a modern installation, the signalman could not make a dangerous mistake until there was an equipment failure, and then it was once again necessary to rely on the rules if traffic was to be kept moving.

He thought it would be interesting to look at main line failure rates. Incidentally, they kept very detailed statistics of failure, and they looked for trends of failure. Mr. Hadaway had touched on that towards the end of his paper. He thought the failure statistics on one of their installations were typical of all the bigger installations of British Railways. At Waterloo there were roughly 1,200 trains a day, or 430,000 a year. Last year the trains per attributable failure were 4,800 odd. That was not bad. They distinguished between failures attributable to signalling equipment failure, and failures due to other causes. Roughly, half the total failures were attributable to signalling equipment failures. It gave some idea of the reliability of the equipment that there were only 4 chargeable and 3 non-chargeable failures of point machines during that period. At that installation there were 10,000 point machine movements a day—or, in a year, 3.5 millions or 32 years per machine per failure, and they changed them every seven years.

One of the most interesting things which occurred when one moved from railway to railway in pre-nationalisation days was that when one went to a new one, one found that practice which was regarded as standard by one's old employer was regarded by one's new employer as something that really should not be done.

At first he was inclined to see it as personal preference, but in the end he became convinced that it was perfectly true. He recollected that one particular piece of equipment used on the Southern for years was not liked by another railway, and there was very good cause for the latter view due to differences in methods of maintenance. To make what he was saying a little controversial, he would suggest that Mr. Hadaway's paper illustrated the point. On the main lines they had used multi-core cable for at least thirty years, and in many places longer. They had good service from it, and he thought it had justified its choice so far as they were concerned. The L.T.E. experience he knew was quite different. Their experience with the type of multi-

core cable which they used had not been good. The result had been that they adopted the single and twin lead-covered cable. When Mr. Hadaway returned to multi-core cable he maintained the same principle by surrounding each pair of conductors with a copper-braided screen. Now that was very sound indeed; and on the main lines they would like to adopt it in their installations—if they could do so economically. He would like to ask if, assuming that Mr. Hadaway had had no trouble with multi-core cables in the early days, he would have felt it justified to put braided screen round each pair of conductors in the multi-core cable.

Another point he might remark on was that Mr. Hadaway used relays in duplicate to avoid the possibility of wrong-side failure. Would it not have been better to tackle the design of the relay, rather than to accept that possibility? He did not use the larger relays in duplicate.

Lt. Col. I. K. A. McNaughton said he would like to add his congratulations to those of Mr. Tyler on Mr. Hadaway's paper, on a subject very near to the heart of all Inspecting Officers, and to say how much he had enjoyed listening to him. He was sure Colonel McMullen, who was unable to be present, would be sorry that he was not present.

Mr. Hadaway talked about absolute safety; but even Inspecting Officers could not demand absolute safety, and they did not expect to get it. They felt Mr. Hadaway's definition of fail safe would really have been better if it included the phrase "would provide an acceptable standard of safety" instead of, as he put it "would provide safety for traffic." He said that they did not mention fail safe in their requirements; well, they did not. It was not easy to define the acceptable standard in every case where the full circumstances were not known. In any case their requirements were only discretionary. They were deliberately left reasonably open to allow freedom for signal engineers to invent new techniques and develop new methods which they could then examine to find out whether they were acceptable to them, after listening to the explanations of the expert. They did not hold themselves to be experts.

As far as the calculations of the probable failure rate of any equipment was concerned he agreed with Mr. Hadaway absolutely that although it was possible to calculate that for an electric or an electro-mechanical mechanism under controlled conditions, he did not believe it was possible to extend those figures over the full life of a railway signalling installation with any reasonable hope of an accurate answer. The installations were affected by the vagaries of weather, the carryings-on of other departments and the periodic attentions of that one article of equipment which was certainly not fail-safe, which they called man. In that connection he would like to draw attention to a report which was published the previous day by Colonel Robertson on a derailment that took place at the end of last year near St. Helens in Lancashire. A perfectly acceptable fail-safe installation, that of a power-operated point machine, caused a derailment when the points moved under a train. The chances of that happening were entirely unpredictable, using any method of calculation that one could consider. A minute crack, a hair-crack in the base of a cell causing a slight leak of electrolite and hence an earth; another very small defect in a taped joint causing another leak to earth, and finally a maintenance or installation error—a long screw securing the cover of timber cable boxing holding a number of separate insulated cables had penetrated the interior of the boxing and frayed the insulation on two cables thus effecting an intermittent bridge between them which occurred with the vibration as a train went past. It was all explained. It might not have been the right answer, but it was an hypothesis which had taken the signal engineers of London Midland Region and Colonel Robertson a considerable amount of time to work out, and if anyone had a better answer Colonel Robertson was ready to listen to it.

That was just an example of the kind of incalculable result which could arise, and showed that one could not regard fail-safe as an absolute standard. He expressed his thanks once again to Mr.

Hadaway, for an extremely interesting paper.

Mr. J. P. Coley continuing the discussion said: "This really is a splendid paper, and one which is most difficult to comment on because it is so very complete."

One point which he had related to Figure 7 and the connection which was made from the lead sheath to the NX Terminal on the transformer. For safety that connection had to be in existence, but there was no continual proving of the connection, and therefore he felt doubtful whether that feature should be included as a fail-safe sircuit. Mr. Hadaway had hinted that the arrangement was checked. He was not quite sure what was meant by this, and would be glad if he would elaborate on the checking means which were employed, and why he considered it fell within the scope of being a fail-safe circuit.

Referring to the double relay, Mr. Hadaway had mentioned that it was a development from the detachable-top relay. The detachable-top relay was essentially a fail-safe device, in as much as it prevented relays being taken out of circuit and replacements put in and then incorrectly wired up, thus resulting in possible dangerous conditions. The detachable-top relay, however, had the advantage that not only did it increase the safety but increased the speed with which a relay could be changed. It did seem to him that in the new relay the quick-change feature had been lost, in view of the large number of screws which had to be undone in order to remove one of those plug-in relays.

A lot had been said, and a lot more would be said in the future, about the matter of redundancy. That was a matter of philosophy of operation. On the railways the philosophy was—and that was acceptable to the top management—that if something went wrong, then a train or number of trains, could be brought to a stand-still. If the control system of an aeroplane went wrong, quite clearly the same principle could not apply, and the control system therefore had to be designed so that in the event of a failure the control would continue to operate. A similar philosophy was applied to the operation of nuclear reactors, because there again the principle was to maintain the reactor running under as many fault conditions as possible, due to the very high cost of shutting down and starting up these reactors. Triple path redundancy techniques were used to ensure that operating circuits would be available when required. Such techniques, it seemed to him, were only likely to be required in railway signalling if the time should come when Management said that it was no longer feasible to stop trains when faults occurred because the cost of such stoppages might become extremely high. It was not conceivable that such a philosophy might begin to gain ground when there was an extremely intensive service of high-speed trains using any one particular line, with the result that the stoppage of one of these would cause so much dislocation that the cost of the resulting disorganisation would become excessive.

Mr. E. A. Rogers said that in their search for safety they often found they had to compromise a little in that they must consider the question "How much can we afford to pay for safety in hard cash?" It had been said in high quarters that they should take a cold-blooded view of that—calculate how much so many more accidents would cost and make an equivalent saving on signalling installations. Now he did not think anyone in the Institution would support that outlook. They wanted to get safety to as high a degree as they could justify. The other price they paid for safety was a possibile loss of reliability. It meant that they provided more equipment, and more proving, and therefore each piece of proving they did and each duplication that they provided created a further failure point. Failures were not only a nuisance to the operation of a railway, but they could, in themselves, even though 'right-side,' created a dangerous situation. As they were all very well aware, under failure conditions they fell back on the human element, and movements which operated under control of the human element must be less safe than those which operated under the control of the equipment. So they must be very careful, not to look so far for safety that they increased their right-side failure rate and thereby created an added hazard to the operation of the railway.

He would like to refer to that relay of Mr. Hadaway's. Use of the d.c. relay had relaced the original vane relay. He would have thought that the basic d.c. relay of that design would have been, in itself, considerably more reliable than the original vane relay. He was a little puzzled that it had been thought necessary to use two of those relays in tandem. Again it meant more contacts to operate. It seemed to him there was a possibility of irregular operation between the two relays, in time, so that there could be a condition created where one relay had operated a little ahead or behind the other, and that might present problems, in view of the circuit to which Mr. Hadaway referred, which detected any out of correspondence between the two units.

There was an alternative approach possible if one talked of using some degree of redundancy, perhaps not to the extent of the triple redundancy; but instead of signal failures being created by a single relay failure could they not concentrate their thoughts on seeing that the first failure, which by itself was not dangerous, could be detected, rather than that the first failure in itself should cause a right-side failure? In other words, in the cabling arrangements Mr. Hadaway had shown them any failure straight-way blew a fuse and created a failure. Could they not detect any first contact that occurred in a cable, but still keep the job going? He had in mind, and that related to a point Mr. Coley made, that on signal lamps their standard practice now was to use a tripole lamp, and they detected both filaments. When one filament failed, they did not fail the system; they gave a warning that the first filament had failed, and they held back any action until that lamp could be replaced. If both elements failed of course there was a complete failure, and they put the rear signal to red and stopped the train.

Mr. A. A. Cardani said that the term fail-safe and the philosophy behind it was, he thought, well known to the signal engineer; at least intuitively. But he was not surprised that there was no generally accepted definition, nor that not until now had there been a paper presented on it to the Institution. He himself had found the concept of fail-safe a very elusive one, and he admired Mr. Hadaway for having attempted the task of defining it, and having done it so well. The paper was certainly most interesting and informative, and he also admired his spirited defence of the signal engineer's approach to that vital problem. The paper had been commended to the students. He also commended it to the Examination Committee, but he would attempt to make things a little more complex by trying on Mr. Hadaway an alternative definition.

He thought there was a slightly more restrictive way in which one could talk in terms of fail-safe, and he would call that 'fail to safety.' The reason was that, as had been mentioned, in reading the Author's definition of fail-safe he too immediately felt impelled to put in the word 'acceptable' or 'acceptable level' next to the word safety; but he found that begged the question as well, mainly because there was no such thing as an absolute level, or absolute safety. Putting in that word 'acceptable' also admitted of any arrangement in fact that had any pretence to reliability, as well, of course, as any redundancy method, whether of the majority or unanimous decision kind.

In the more restricted sense of "fail to safety" the Author had given several illustrations of that, and he also thought that had been the signal engineer's classical approach to the problem. So he would submit the following definition; that "a fail-to-safety design is one which maximised the inherent possibility that if the design fails it will fail in the least unsafe condition, and preferably in an entirely safe condition." Thus when there was a choice of design features the one that appeared to have the best probability in that respect was the one which would be selected.

Having done that and organised one's system, then it must still be subjected to a very searching analysis for all the possible modes or ways in which it could fail, as well as making an assessment of the likely frequency of it failing. The non-dangerous kinds or modes of failure one would simply evaluate against the tolerable level of interference one was prepared to accept; that was interference with the normal working of the system. But for the unsafe modes one could not avoid an evaluation of the risk of that

kind of failure occurring, mainly by drawing on experience and extrapolating it to the new conditions by the exercise of judgment. It was a pity it could not be quantified, but he thought one could not get away from that fact. If in one's judgment the risk was too high, then one would have to do something about it, like adding back-up protection or going one stage further along the road. But he thought that was the sense in which the signal engineer had hitherto designed his systems in the fail-to-safety sense, and he would be glad to hear what the Author made of this definition. It was probably open to all sorts of objections.

He thought that was the approach that was brought out in several of the illustrations, and in particular the semaphore signal arm analogy. In that case both the lower and the upper quadrant relied on the design of the spindle bearings to the same extent, and the likelihood of the bearing seizing could only be judged on the basis of experience. In the design it was possible, to use the words of his definition, to maximise the likelihood of gravity returning the arm to the danger position by a suitable design choice in affording the return torque.

Mr. Tyler had mentioned that the counter-weight was used only to return the wire, and with the lower quadrant semaphore signals with which he was familiar, it was certainly the case that the return of the arm was assured independently by the spectacle casting, which was integral with the arm. He suggested that gave an equally good fail-to-safety design.

There were one or two points in the paper he would like to mention. He rather took issue with Mr. Hadaway when on page 161 he talked about the complications required to substitute for the trainstop to give system-safety. He went on to talk about lamp proving, but he would suggest that the provision of the trainstop itself was a complication, and indeed did they not have to test for the presence of tripcocks and so on ? Surely that again was an example of the exercise of judgment ; of how far along the road one went before feeling that an adequate or acceptable standard of safety had been achieved.

In section 5, 2.3 he would like to hear Mr. Hadaway comment on the reliance which could be placed on the fuse blowing to protect the circuit in the fail-to-safety sense. It was really the general question of the use of fuses for clearing potential wrong-side failures in circuits. It seemed to him one could never judge *a priori* when the fuse would blow when called upon to ; indeed he thought that again was where one relied on experience and judgment, if one incorporated such a system of protection.

On page 169 the Author mentioned the decision to duplicate contacts or relays when progressing from a system in which there was a driver and a signalman, to one of automatic train operation. He would like to ask him if he would be good enough to amplify the grounds for this a little more. It seemed to him obvious that one was increasing dependence on the equipment and he thought it seemed prudent to take one further step along the road to ensure safe operation. But he wondered if there were any additional statistics that were brought into consideration when arriving at that decision.

In section 7 would Mr. Hadaway clear up what appeared confusing, as to whether he was talking about the life of semi-conductors in much the same way as one talks of the life of a lamp, or whether he was talking of the probability of them failing in an unsafe manner. He thought that if in the first sense of the meaning, the life, that was of course merely a question of reliability ; the other mode of failure he thought was amenable to consideration as he indicated earlier. An example was the ferrite core when used for interlocking purposes, where from a fail-to-safety aspect one had to consider the probability of a hair crack developing which could lead to a wrong side failure. So perhaps Mr. Hadaway would make it clear for him whether he was talking about life in the one sense, or safety.

With regard to the logging of statistics of failures ; whilst that was very desirable he thought it would be necessary to define strictly how they were arrived at, and exactly what equipment was covered so that a true comparison could be made. He had made a quick calculation relying

on his recollection, and he thought that on the Western Region they too came out to one failure per track mile, or something of that order. But obviously the equipment and system concerned was certainly very different from that of the London Underground. In that connection he would be interested to know what the units were which were referred to in the ordinate of the graph which was shown, where the failure per-unit had so pleasantly decreased steadily over the years in spite of the increasing number of units.

Mr. Cardani concluded: "I seem to have done my best to obscure the issue that Mr. Hadaway had so well clarified. All I can say is that I make fully confident use of London Transport and that I place complete reliance on their safety system, which I think is obtained at a very reasonable price for all that it achieves!"

Mr. R. A. Hope (Assistant Editor, The Railway Gazette) said he hoped they would forgive him for speaking as he was only a visitor; but he had been asked a direct question, towards the bottom of page 181 in the paper. He was the blind-landing expert in question, rather wishing he had never seen the original article! As regards the question "What happens when the precisely calculated day comes?," there was only one solution: arrange one's annual holiday accordingly!

But more seriously, the context in which he wrote about absolute safety being a meaningless noise was, if he remembered rightly, when he was referring to catch points. He was not a signal engineer; but there was a tendency among signal engineers, if he might say this, to say: "If there is a safety device we must have it; if one thing is safer than another we must have it, because human life is sacred."

He mentioned catch-points as an example. Catch-points placed on rising gradients to throw wagons off the line if they broke away from a train were a safety device, but he would question whether more accidents were not caused by catch-points than were avoided by them. If one thought about it catch-points merely turned a possible accident into a certain accident. He mentioned two accidents, one at Inverkeithing and another at Pitsea, which were caused by catch-points, and would not have happened if they had not been there.

On the question of road deaths: he agreed it was a bit of an exaggeration to say that if the Victoria Line signalling were more economical less people would be killed on the roads, but there was a point here. Signal engineers did not operate in a closed world of their own; they had not got complete control over what the public was going to do, and undoubtedly if the very high standards of the signalling which London Transport was able to apply over its system were applied over the whole of the railways in this country, the railway system in this country would be very much smaller than it was today and the number of people travelling by train would be less.

It was perhaps instructive to remember the fate of the County Donegal system, which used railcars with a driver to drive and a guard to collect the tickets. They were getting a bit hard-up so they decided to do without the guard, and in due course the inevitable happened: they had a head-on collision with a goods train. Somebody was killed and the driver said that he could not avoid the accident because he was at the back of the railcar collecting fares at the time. So the Eire Government said "Guards must be provided," the Donegal management said "We can't afford it," and they closed. Whether the people of Donegal were statistically safer because they now had to go by road was open to question; but he was quite sure nobody ever worked it out before they took the decision that closed the line.

Turning to the question of delays to trains on a system like the Southern, or London Transport, if one had too much fail-safe, if one had a system which was so set on stopping everything when a failure occurred, one could quite easily get to the point where passengers were driven away from the railway on to the roads simply because of delay caused by excessive safety. It was not just a question of measuring human life in cash terms; there was stiff competition over the fence, and it was very important that should be remembered.

Mr. M. Birkin said that Mr. H. H. Ogilvy, who was at present abroad on duty had asked him to read, with the President's permission, his contribution

to the discussion on Mr. Hadaway's paper. It went as follows :

" Like the Author I have never seen a formal definition of fail-safe, but have always assumed that it means precisely what it says, namely, that if failure occurs there is no possibility of danger. At least this is the impression gained after many discussions with members of this Institution, although I have never believed that this Utopian situation has ever been realized in practice.

" After reading this paper I am more than convinced that the Author shares my belief. In fact, at the top of page 161, right hand column, it is stated quite clearly that there may be several levels of fail-safe. Perhaps the Author could explain precisely what he intends to indicate. Am I right in suspecting that what he really means is that the probability of wrong-side failure can be made less and less but never zero ? If this is his meaning then I am in full agreement and hope that this Institution will recognise this important principle. We can now discuss and calculate failure possibility in more strictly scientific terms, that is, 1 in 10^6, 1 in 10^7, 1 in 10^8 and so on. This is quite meaningful and it is used extensively in other spheres where safety is of paramount importance. It is rather disappointing therefore, to find the Author dismissing such ideas by implication in the statement on page 181 ; I quote ' equipment failures of simple resistances can be quite random and dependent on a considerable number of variables.'

" Mr. President, the calculation of reliability is based *entirely* upon the random occurence of failures and in theory only becomes invalidated when the failures are not random ! To be precise, reliability $= e^{-\frac{t}{\theta}}$ where θ is the reciprocal of the mean time between failures (m.t.b.f.). Thus, if the mean time between failures for a man is 70 years, as has been stated on an earlier occasion, the probability of reaching such an age is $\frac{1}{e}$, or about 37 per cent. Similar reasoning can be applied to equipment. It is true of course, as the Author says, that variation occurs with different manufacturers but like man, where basic manufacturing techniques are everywhere indentical, control of environment can help to reduce the variations.

" I hope this otherwise excellent paper will not lead to a renewed suspicion of statistical techniques. It would indeed be a pity if such techniques should be dismissed lightly in the expedient manner of politicians. The intelligent use of statistical methods has in many other fields yielded substantial rewards and it would surely be inappropriate to assume that the railways are a special case.

" Another point I would like to make, and indeed emphasise, is that the so-called ' wiggly-wire ' system referred to in section 9 provides a degree of safety beyond any form of control at present available and this is accomplished without introduction of redundancy. Redundancy is required for the purpose of transmitting additional safety information which is *not* provided at present. Therefore, I would like to reassure members of this Institution that the installation of a wiggly-wire system can only show an improvement, even without redundancy.

" Finally, when redundancy is used it is important to distinguish between coding and equipment redundancy. In the various speed supervisory systems at present under examination by an O.R.E. Committee, (including the wiggly-wire system), a Hamming distance of four is used. It would appear that only a Hamming distance of 1 is used on the London Transport automatic system. Would the Author please confirm this, and say it is sufficient for safety.

Mr. R. J. Post said he was particularly interested to hear Mr. Hadaway say that he had considerable difficulty in producing the diagram in Fig. 6b, in which he had discarded all the fail-safe principles with which he had been inculcated, because every time he drew it he found he was including fail-safe features.

A difficulty which someone who had been trained in railway signalling would experience in going into another field was that he would find himself automatically using the fail-safe principles, and producing the circuits as in Fig. 6a. He would then be faced with explaining just why he had done that, to a group of sceptics who were not easily convinced that the techniques were necessary. That happened to him 25 years ago, on leaving

Mr. Hadaway's influence (where he had been very carefully soaked in fail-safe principles), and becoming a safety engineer in connection with particle accelerators.

Now those who were still working in the railway signal field were very lucky for several reasons. Firstly, as had been pointed out, an aeroplane would fall down if one stopped it, so that plain fail-safe techniques were not fully applicable in aircraft, whereas on a railway they were; secondly one could nearly always arrange detection so that an unsafe condition would result in loss of signal. That, of course, was a fail-safe principle firmly based in fail-safe philosophy. But those conditions did not always obtain in other fields. If one was exposing a human subject to a beam of radiation from a particle accelerator, for example, one needed to integrate the amount of radiation the subject received, and the signal there was a positive signal of the presence of current from an ion chamber, which had to be continuously integrated. The dangerous condition was reached when a given amount of signal had been integrated. That was the area where redundancy completely came into its own, as the only way to guard against loss of signal was to have more than one detecting system, and check that they all agree to within a specified tolerance.

Mr. G. D. Miller said he was interested in the discrepancy circuit between the two relays and the way in which it was indicated. He wondered if Mr. Hadaway could give a little more information on the way in which the alarm was indicated. Was there just one indication for a complete relay room, or if on the other hand there was some attempt to break that down a little in order to help the maintenance man to find the fault reasonably rapidly.

Also he assumed there was no automatic means of locking the relay out of circuit if that sort of fault was indicated. It just depended on someone getting in there fairly quickly and sorting out the trouble.

On the question of comparing reliability figures and failures on various railways, it might be interesting also to consider some overseas practice. He was thinking in particular of the comparison between safety relays with weldable contacts and those with non-weldable. He felt sure that if one could choose a contact material without regard for non-weldability, a more reliable relay could be produced. He felt quite sure that silver impregnated carbon was not by itself the ideal contact material, looking at it just as contact material.

He had some information relating to one continental safety relay. That was an 8-contact relay with metal-to-metal contacts typical of its type. He was told that about 13,000 of these had been put into service since about 1964 and since that time there had not been a single failure of a relay recorded, either right side or wrong side. One particular interlocking, where there were 5,800 of these relays, was handling 800 train routes a day and this same statement applied—that there had not been a single relay failure at all. With this in mind he would like the Author's opinion on whether it would be interesting to keep a check on the performance of relays with weldable contacts.

Mr. H. W. Hadaway, replying to the discussion, said that Mr. Tyler referred to the signalman who now made mistakes, a most important theme on railways generally. But it had greater significance in the present situation on London Transport in the trend towards automation and less use of the human element. Therefore, although Mr. Tyler thought there was a case for further provisions of safety of equipment, recognising the deterioration in operating standards of the human element and its ability to safeguard the system, that was not entirely why London Transport had felt it necessary to go to the additional measures in the new signalling system for the Victoria Line. That was not because they recognised there was a falling standard, and he would not comment on that, but that primarily there were no longer the people supervising and watching the system in the same way as the driver, and the signalman once did and had to do. Because they had to do it in the past, and experience had borne it out, the signal engineer had on many occasions been very thankful that there was such vigilance, because warning was given when system equipment was apparently not doing all that it should. By that means occasions of failure of

equipment were brought to light, giving opportunity for action before any unfortunate results could arise. As to Mr. Tyler's comment about the failure chart displayed, that the highest failure rate had been when he was with London Transport, Mr. Hadaway had not looked at the failure chart in that light before, but it was a very valuable suggestion. Perhaps he would visit them more often to give opportunity for further improvement.

On the question of deciding what a failure is, whether chargeable or non-chargeable, and the relation of other departments ; he agreed with Mr. Tyler's statement that there must be common understanding in that. The present system had much to recommend it. He thought it had its weaknesses, and one of those, concerning the charging of failures, was the very human weakness of always wanting to charge one's failure to another department. By that means one's own department was put in the clear, and a good record could be shown. That, of course, was a very short-term attitude. What everyone on the railways should be interested in was the question of the effect on the passenger. If there was a failure it ought to be stopped at all costs, and not be allowed to continue. The signal engineer ought not to sit in his chair, content that the failures that happened were the shortcomings of the civil engineer and his permanent way. He ought to be knocking on the civil engineer's door and saying : " This is not good enough ; you have got to make your permanent way better." That was one of the aspects of failure prevention. It should be in the minds of all staff that a failure was a failure, and the more people who were interested in it, and who committed themselves to do something about it the less likelihood there would be of there being a failure of that kind in the future. The railways and the passengers would consequently be the better because of it.

Mr. Tyler had spoken of the multi-core cables, which had been used for many years ; and he asked if it was justified to use the new screen cable, when from his experience the multi-core cables had given very good service. He asked if they had had his experience would they now be introducing the type of cable they had done. There were a number of assumptions in that question which he found it difficult to comment on ; but as he said in the paper itself the safety aspect they had considered on London Transport was applicable particularly to their conditions, and he would not in any way challenge the thought that Mr. Tyler put, that the safety that they had on their system was quite adequate with their multi-core cable. But he still thought that under their particular conditions of 40 trains per hour—automatic trains, in effect no-one on the front of the train, in effect no-one watching from the signal box—justified the step forward in taking every step that they reasonably could, towards absolute safety. Might he also answer the points raised by other speakers, if he said that on the question of statistical analysis he entirely agreed that such analysis was a necessity. An engineer had to be able to measure, and for that to be done facts must be available. The problem of " fail-safe," was that it was not measureable, and did not allow presentation.

However, statistics were essential, in order to know by fact failure trends and results obtained. But he would never advocate using those statistics in such a way that the end result would be a factor of safety in operation, which in his view gave a lower standard than he believed was obtained when pursuing a policy of reason with absolute safety. When he was in America last year, BARTD in San Francisco were preparing specifications for their new signalling. The specifications prepared were based on mathematical formula and were to be offered to contractors to specify the factor of safety to be obtained. Whilst he was there, and discussions were in progress, the specification was amended to demand instead absolute safety. The Americans had studied the subject very closely ; and having carefully examined the results they were likely to get, and the manner in which manufacturers could apply the specification in the design and installation of the signalling system they decided that it was not the right answer and substituted it by the tried term ' absolute safety.'

Mr. Tyler further asked if it would not be best to concentrate on the design

of the relay, and improve that design, rather than have two relays. Statistically, he had no doubt the research people from Derby would be able to help him out with that one. He believed the factor of safety from the combination of those two relays would be much higher than a factor of safety obtained from a single relay, whatever was done to improve it. This was also a question of philosophy. They on London Transport had accepted that relay, as designed and used by British Railways, and as yet with no experience of its use. They had accepted that the relay had been produced on the basis that it met fail-safe requirements in the British Railways terms. The London Transport Board also accepted that, but in applying it to their conditions, as described for the Victoria Line operating without supervision, he thought it was right that the factor of safety would be greatly increased by the doubling-up of the relay; particularly as they were able to justify it on the basis that the relay which they would have used in its place, cost no more than the double relay that they now had: increased protection for no greater cost.

Referring to Col. McNaughton's comments, in which he spoke of definition and said he would like to put in a qualification on the question of providing safety for traffic, Mr. Hadaway thought he had qualified that by not stating absolute safety. He would not quarrel with him on that point. In fact he offered the definition tentatively, but whilst it was of some value it went only so far. It was unlikely in itself to help in designing equipment and systems. If talking of the term he thought he should say what it meant to him, and he thought it was satisfactory, although he did not quarrel with others who wished to have their own particular definitions. He thought that again was something they could debate at great length.

Col. McNaughton had referred to the calculation of the failure rate. He was very pleased to note that the Ministry were thinking in that way, and at that time they would not be agreeable to installation of signalling equipment solely on a basis of calculation of wrong-side failure rate. That the Ministry believed it was a matter of judgment comforted Mr. Hadaway, although he was prepared to think that in time to come that might well be changed, and experience could well give another answer. As they were at that time he did not think it was possible to accept that it was purely a mathematical process.

Col. McNaughton had described the movement of a set of points under a train, and all the multitude of events that could produce such a result. He did not know about the particular event described; he was only hoping that members present had not got the impression that in these circumstances was a kind of failure nobody could do anything about: it was " just one of those things." He thought on the question of failures the gospel was: " There shall be no failure, and all failures are preventable." He believed examination of all failures and their causes would inevitably result in their saying: " This should not have happened." So he did not believe there was any failure which could be accepted, as one that nobody could do anything about; they were all preventable.

Mr. Coley had asked for some confirmation on figures of passenger fatalities. Mr. Hadaway had wished to make comparison with the railway system in Great Britain, and hence the figures for road and air were confined to operations also within that country. Referring to Fig. 7, Mr. Coley had asked if it was ' fail-safe ' to have such a connection for the NX to the lead sheath ? Mr. Hadaway believed it was. The connection made was recognised as being a very essential part of the system, and in fact the line which was drawn from the NX to the lead sheath of the cable was a very heavy cable used in the signalling installations in the interlocking machine room. It was usually of a 19/.064 conductor sweated to lugs, and the lugs were then bolted to the main transformer terminals in such a way that they were not readily removed. The connection made to the mass of lead sheaths in the cabin was plumbed to them, so that it could not become disconnected. In recognising the essential character that played in making it a positive and permanent connection at both ends—a connection that could not be removed inadvertently—then within his

experience it was found that it provided a very adequate method of making that connection.

Mr. Coley spoke of the double relay and compared it with the detachable top type and he commented on the terminals that they had for the new 'Q.' Their philosophy on that was that the relays would not fail, so they did not envisage the necessity of having to change relays in service. He was reinforced in that thought, because it was Mr. Coley's firm who were making the relays, and they would not make relays that fail. So far as changing relays for the 5-year overhaul was concerned, they thought the time taken for the relays to be changed was quite acceptable, on a basis of once in five years; because they believed it would eliminate the failures that they knew had happened, small though they were, caused by the spring loaded contact on the detachable top.

Mr. Coley had commented on the various aspects of philosophy of 'fail-safe' in various spheres. He was talking of the atomic pile and the air system. He had said that perhaps at some time the signal engineer would be commanded that there must be no failures that would stop the trains. He had quoted the question of lamps and replacements. Mr. Hadaway thought that in a large measure, and as far as one could economically go, things of that sort would be covered on the Victoria Line system. Specifically mentioning a lamp, of course, was touching upon one of the most fallible parts of the system in giving information to the driver. He thought most people were aware of the steps taken to provide alternatives; costly steps, and in themselves sometimes producing failures. His comment there was that in making the step to the automatic train they were getting towards the position that Mr. Coley wanted, in that failures of lamps and signal aspects would not be bothering them in the future, because there would, in effect, be no signals and no one to look for them. So although they might not have done it for the reason that Mr. Coley mentioned, they were on the way to eliminating from the cause of failure one of the factors, lamp failure, which was so bothersome to signal engineers.

Mr. Rogers commented on how much could be spent on safety and asked whether it was best to pay for accidents from the overall cash saving made by economising on the signalling. At different times, of course, they had heard sentiments of that kind. Certainly on London Transport he was convinced that policy had never prevailed and in considering future possible methods that might be employed to replace the conventional signalling, he was sure that such a policy would never be allowed to influence the result.

Mr. Rogers touched on the important point that when failures did occur something had to be done about it, and the human element then took the responsibility. That was true enough. That was one of the things required from the signal engineer, to exercise judgment as to where to stop using additional equipment, because on balance such additions might be likely to be adverse in their effect and not make a good contribution. That was something that he felt convinced the slide-rule alone was never going to tell, and that was why there must always be a measured judgment by the signal engineer. Mr. Rogers had questioned whether it was necessary to have the two relays when, in his view, the single relay was better than the a.c. relay. On London Transport they had very good service from the a.c. relays—as yet he did not know about the 'Q' relay. It was to be assumed that the 'Q' relay was at least as reliable as the a.c. relay; and indeed they were looking for something better. He was not in a position to comment as to whether that relay was better than the a.c. relay. In 30 years time the full results would be known. Mr. Rogers had referred to the coincident circuit and the question of relays operating a little out of time with each other. The coincident circuit had to take that into account, and there would be a timing feature in it to prevent the small difference in time of the relays, possibly giving an alarm indication.

Mr. Rogers' last point had been: "why not detect the first contact failure and not cause a failure under this condition." Mr. Hadaway was not sure if he had understood the point correctly. In some measure he thought that was achieved, at least in the respect that if one relay

stuck up falsely they still had the safety; there was no failure, but still a warning of the situation. In that respect the situation was known before the train was stopped, and with safety in the meantime. That was a very valuable feature. It gave time for action.

He had great difficulty with Mr. Cardani's definition of fail-safe. He had spent so long in considering his own, and in altering it in various ways from time to time, scrapping it and starting again, that he felt sure Mr. Cardani would be prepared to extend some tolerance and give him some time to consider that new one! He would not comment on it at this stage. He mentioned about the spectacle casting being integral with the arm in giving full safety. That very point emphasised the higher levels of fail-safe. Although it was quite true that the casting was integral he was going to say that the casting could be cracked; it could break and fall off, in which case the arm would lower to clear. That, he agreed, was highly improbable, but in the question of levels of safety, that illustrated one of the fundamentals to be considered in assessment of fail-safe.

Mr. Cardani had challenged his claim on page 165 where he said that without a trainstop and a tripcock, the provision of alternatives, with proving of red light circuits which then became vital, were a burden on the system. They introduced in their way further failures and problems, and as an end-result did not give the same standard of fail-safe, as compared with the tripcock and trainstop. In section 7, where he was talking of reliability, he was referring to the electronic circuits which were at present not used in fail-safe circuits, but which were giving experience to gather information, as to how reliable those forms were. In the way in which they were used at present they could cause only right-side failure. The experience with electronic components in non-safety functions, would provide information, step by step, to enable them at some stage to make judgment for full safety use.

Mr. Cardani had asked what were the units on the graph. The 35,000 units were made up of 10 types of unit; 1. Colour-light signals, 2. Mechanical signals, 3. Electric shunt signals, 4. E.P. Disc signals, 5. Trainstops, 6. Points, 7. Track circuits, 8. Block joints, 9. Working levers and 10. Point heaters. That gave a breakdown of the main fundamental parts of the signalling apparatus.

Referring to the use of a fuse on the circuit for protection, as shown on diagram 7, that was one of the difficulties that faced all maintenance people; to make and use a fuse which was going to blow at the first sign of a fault current, however low it was, but at the same time must be so reliable in service that it was not going to fail due to tiredness under the normal working conditions. They had set the standard in their own system with two levels of fuses, 3 amp. and 5 amp. Generally speaking the 5 amp. was used on the feed fuse at a transformer, and the 3 amp. on incoming fuses at the relay room. That level they found gave a reasonable answer to the problem.

Mr. Hope confessed that he would go on holiday on "that appointed day." Signal engineers did not have holidays, by and large, so he was afraid that recourse would not be open to them! He quoted in his article about catch points, and it was quite true that in making reference to that article Mr. Hadaway specifically avoided all matters which he thought were used in reference to British Railways. Mr. Hope had also talked about level-crossing protection and things like that. Mr. Hadaway confessed he was not qualified to defend British Railways; he thought they could do that very well themselves, and he had confined himself to those matters where Mr. Hope had cared to say that London Transport were not doing the right thing. He talked of looking at the world at large, and not having too narrow a view. Mr. Hadaway wondered if he would be prepared to sponsor a campaign to stop all those road deaths and put everybody on the railways. There was a simple answer which only needed to be got home to the people, and Parliament, and that was, do not charge to travel on the railways. Nobody would go on the road then! No fares—no road deaths, and everybody on the railways; a simple answer. He would be very grateful to Mr. Hope if he would put some such article in his paper.

Mr. Berkin had spoken for Mr. Ogilvy regarding the levels of safety. In that

respect he had made a reference to this in replying to Mr. Cardani. There were levels of safety which signal engineers recognised, and referred to, and made use of, depending upon the conditions of the traffic they were dealing with. Because of heavy traffic conditions they would say: "We require a level of safety to meet those conditions." Nobody could measure it, or put a value against it; that again came from experience. In other places, and talking of a railway in remote parts, the signal engineer might say that another level of safety was quite satisfactory to meet those conditions. That, he thought, was what was meant by levels of safety, considered as part of the philosophy of fail-safe.

Mr. Ogilvy had suggested a formula showing how it was possible to calculate failure rates. Mr. Hadaway would regard an answer given by a formula as suspect, unless he knew how the values on which the constants and so on were obtained, and were put into the formula. In his opinion one could not take convenient charts of figures of failure rates for various types of equipment, and fit them into a formula, and say: "That provides a signalling system which is going to give a particular failure rate." It was living in a dream-world to think that way. In that respect statistics were only as true as the particular constants that were used, and in the circumstances considered from values arrived at under particular working conditions. The full answer to that might not be known until 30 years had elapsed for the life of the equipment. Tests which simulated life conditions, to give a quick answer, are in themselves open to suspicion, and did not give an answer as from a table of logarithms or a slide-rule. Much as he respected the value of statistics—and they were valuable and no signal engineer could function without them—the fact was they could not be accepted blindly.

It has been asserted that the 'wiggly-wire' system was in itself fully fail-safe, and did not require redundancy. He had heard the lectures that had been given—Professor Barwell gave one—and at the end of it Mr. Hadaway said he did not really appreciate the point, and did not think it was made clear. He would very much like Mr. Ogilvy to come to that platform, and give such detail, so that it could be seen to be fail-safe, in terms accepted by signal engineers. He did not think that had yet been done. As Mr. Hadaway had seen it as experimented with in America, it had yet to be proved as satisfactory. He must confess, and he thought most of the members present would have already seen this, he did not know what a Hamming distance was, and he would be very happy to sit with Mr. Berkin sometime to be educated in this process.

Mr. Post had also made a pretty little chart, and he believed he knew the intent behind it. But he doubted if he could ever say, having drawn a chart like that, that he was installing a signalling system on one of those lines and that was giving him an answer. There just seemed a gap, between what that said and something that existed on the ground. It was the bridging of that gap that he would like to see.

Mr. Miller had referred to the discrepancy circuit. The thought they had on this was that for the Northern Line and the Victoria Line there would be one regulating room at Coburg Street. There would be one indication at Coburg Street for 2 relays somewhere which were not in accord. That would cause an alarm and would be passed to the signal department for investigation of the system between Victoria and Walthamstow. Each interlocking machine would have its own individual warning circuit. By that means the finding of the fault would be dealt with before it became a serious matter.

On the subject of weldable and non-weldable contacts, he had seen what the continental people did; he had heard descriptions of how those relays never failed. He could only accept what he was told, because he did not know. They had experience of silver contacts on their own system through using standard commercial relays in some thousands for non-safety controls. They had experienced a number of those contacts which had welded. Why they should get different results, in using these relays in non-safety circuits, from other people who did not have such failures in safety circuits was more than he could say. His experience did not persuade him that safety could be invested in weldable type contacts.

He believed that part of the continental practice was that wherever such relays were used then it was proved. In his experience proving of circuits was limited and expensive. But that was a question where there was no ' yes ' or ' no.' If there were people in the world satisfied with this method there must be something in it. And he would not therefore condemn without further experience.

The President, Mr. R. Dell in summing up the discussion said he thought they were all deeply indebted to Mr. Hadaway for his paper. He believed the paper would be a subject for reference for quite a number of years to come. Mr. Hadaway had been kind enough to say in his acknowledgments that he encouraged him; less generous people might have used a different word for it ! If he had encouraged Mr. Hadaway to write the paper it was because he did not know anyone whom he believed could have done it so well as he had done.

Mr. Hadaway had spent a lifetime in signalling, and to his personal knowledge he had throughout that time given a whole-hearted attention to fail-safe. It was really a feature with him, and he believed he really was the strongest man he knew in that respect.

Mr. Dell concluded by proposing a very hearty vote of thanks to Mr. Hadaway for delivering the paper, and for the way in which he had dealt so thoroughly with the questions asked during the discussion.