Solid-state interlocking (SSI): an integrated electronic signalling system for mainline railways

A.H. Cribbens

Indexing terms: Railway electrification and transportation, Signalling, Electronic circuits

Abstract: For a number of years, British Rail (BR) has been working towards an electronic replacement for the electromechanical interlockings which are at the heart of railway signalling systems. This work has led to the successful development of the BR solid-state interlocking, an all-electronic signalling system for mainline application which has been in operation at Leamington Spa, Warks., UK, since September 1985. The paper describes the problems confronting railway administrations wishing to exploit new technology and discusses some of the options available to the designer of safety-critical systems. The solid-state interlocking is described, with particular emphasis on the techniques used to ensure safety and reliability, its software and data structures, and the methods used to communicate with trackside equipment. The specially developed scheme design language is illustrated and details are given of support facilities such as data compilers and simulation equipment. The salient features of the Leamington Spa pilot scheme are described.

1 Introduction

Railway signalling has had a long history of evolutionary development punctuated occasionally by more significant changes. From the earliest use of the block telegraph, which provided signalmen with a rudimentary means of maintaining safe distances between trains, to the multi-aspect colour light signalling systems of the present, with their centralised control of large areas, complex operating facilities and computerised traffic information systems, change has been gradual and cautious. Caution has been necessary because the safety of railway signalling has tended to reside in properties of the system not amenable to objective analysis, so that trust, experience and engineering judgement have been of overriding importance.

Current signalling technology is based on the use of very high quality electromechanical relays to perform the complex logic required for the safe control of train movements in a system providing considerable operational flexibility. Such systems are physically large, are labour intensive to manufacture and install, and require extensive accommodation. The technology is consequently expensive, and since the mid-1970s a number of railway administrations have been working towards the introduction of electronic replacements for the electromechanical logic systems, which are generally known as 'interlockings'.

The problems confronting these administrations are many, but they tend to be dominated by the difficulty of implementing a uniquely revolutionary change in signalling technology without compromising existing safety standards. There is no single approach to this problem which is obviously superior to others, and a variety of solutions have been proposed. At the time when British Rail (BR) were instituting a programme of research in this field, the very few developments being progressed by the signalling industry and other railway administrations did have one thing in common — they were all hybrid systems in which computers depended to a large extent on the use of signalling relays for the maintenance of safety and for connecting the system to track equipment. One of the primary objectives of British Rail's programme was to study the feasibility of an integrated approach to signalling system design in which the signalling relay would be no longer required. Such a programme was started in 1976 and has grown into a major collaboration with British industry resulting in the development of a computer-based signalling system suitable for application to major routes throughout BR while being flexible enough to cope with the requirements of railways overseas. A pilot installation at Leamington Spa is operational and further schemes are planned.

The paper describes the design of the solid-state interlocking (SSI) system and discusses the philosophical and practical problems which have had to be overcome during the development.

2 The SSI system

Although descriptions of the solid-state interlocking have been given elsewhere [1, 2], this present paper would be incomplete without a brief account of its structure and method of operation. SSI has been developed as an electronic replacement for current relay-based signalling technology with the aim of providing, at lower cost, all the operational facilities available in British Rail's most recent power signalling installations. SSI is fully compatible with present signalling principles and operating practices and does not alter the appearance or behaviour of the signalling system so far as the railway operators are concerned. It does, however, have the flexibility to operate in conjunction with new display technologies and higher-order control systems, and to accommodate future changes in signalling principles. The design aims to satisfy the broad objectives of equipment modularity,

Paper 5252B (P2), received 17th December 1985

The author is with British Railways, Research Division, The Railway Technical Centre, London Road, Derby DE2 8UP, United Kingdom

high system availability, ease of application, good maintainability and cost effectiveness in both small and large applications.

The essential features of an SSI system are illustrated in Fig. 1. At the control centre are located:

(*a*) one or more microcomputer interlockings, the number depending on the size and complexity of the area to be controlled

(*b*) the control panel, which may take the form either of a VDU installation or of a conventional signalling control console equipped with a multiplexing system giving the interlocking access to the many switches and indications

(*c*) a maintenance terminal providing diagnostics, event logging and facilities for placing temporary restrictions on interlocking operation.

The interlocking is linked to specialised interface equipment at the trackside via a duplex data highway carrying signalling information in the form of discrete messages protected by two levels of information coding.

Two types of interface equipment are available: a points module, which is designed to connect directly to clamplock point machines; and a signal module which, although being optimised in design to provide an efficient interface to multi-aspect colour light signals, is sufficiently flexible to handle all other input and output functions. Both types incorporate solid-state power switching under

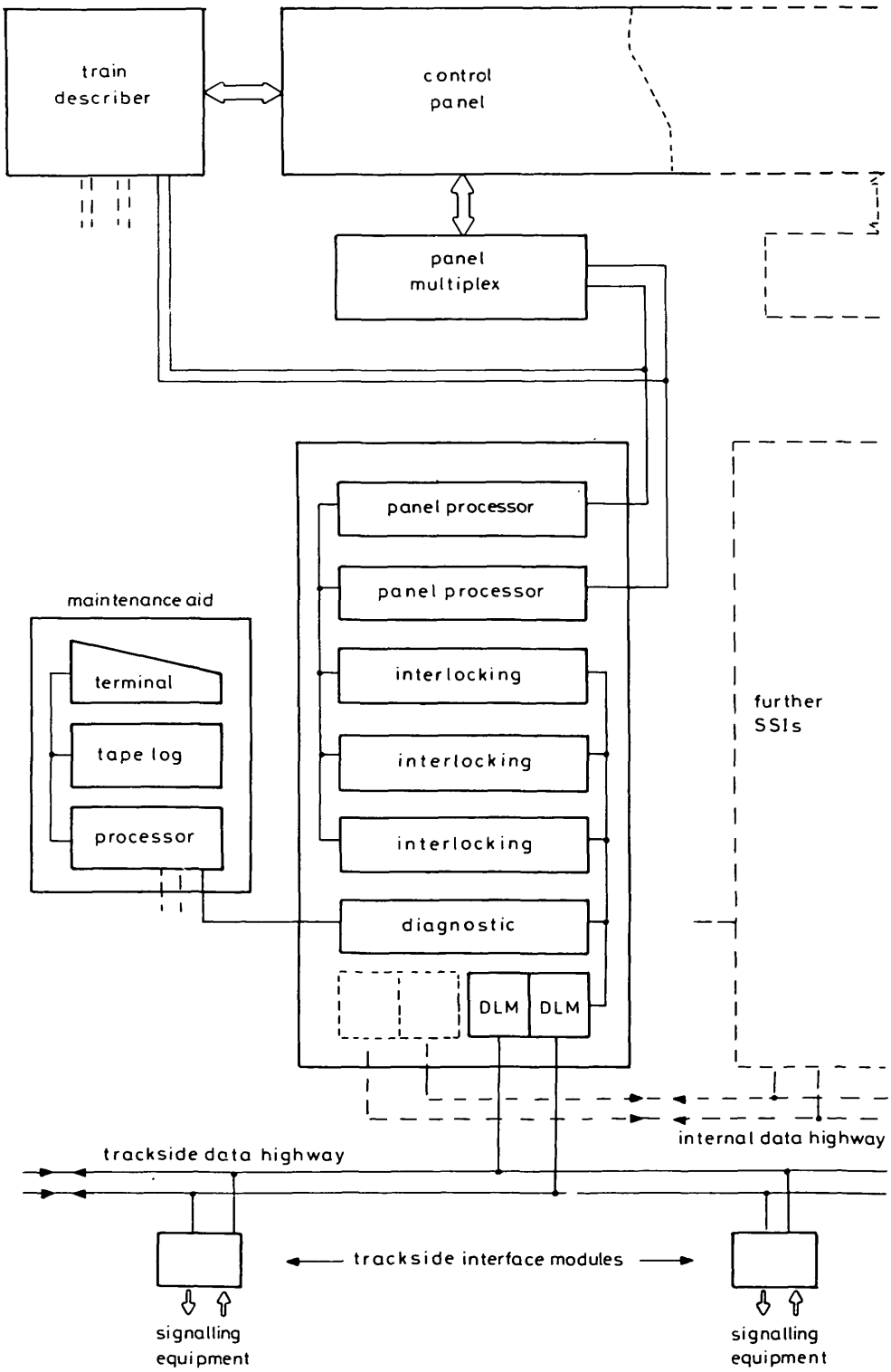

Fig. 1 *Principal features of the SSI system*

the control of a duplicated microcomputer. A maximum of 63 interface modules may be connected to one interlocking.

The interlocking itself is a multicomputer system containing two panel processors, three interlocking processors and a diagnostic processor.

The three interlocking processors operate as a repairable triply redundant system providing the necessary processing integrity with a degree of fault tolerance. They are the central controlling element of the system and are responsible for the safe execution of all signalling logic and the issuing of correct instructions to lineside equipment.

The two panel processors relieve the interlocking of the nonsafety task of servicing the control panel, the train describer and any other higher-order control systems. They operate as a duplex system in which failure of one processor does not degrade overall performance.

The diagnostic processor acts as an interpreter between the SSI and the maintenance terminal, providing installation-specific diagnostic information to the maintenance terminal processor. The diagnostic processor is equipped to diagnose with accuracy all but the most obscure faults, both in the SSI system and in the associated signalling equipment.

The maintenance terminal provides the technician with a powerful means of monitoring the performance of the SSI system, through which the fault status of the interlocking, its data highways, its lineside interface equipment and the associated signalling equipment can be determined at any time. The keyboard may be used to request specific status information or to make permitted alterations to the behaviour of the interlocking — the barring of particular routes, for example. A tape cassette data recorder logs all changes in the state of the system, providing a continuous record of operations. One maintenance terminal has the capacity to serve six interlockings.

In addition to the trackside data highway, a separate highway is provided for carrying safety level information between the several interlockings of a large installation. Up to 30 interlockings may be connected in this way.

3 Safety assurance techniques

3.1 Performance requirements

The dominant requirement of a railway signalling system is that it should be safe. Safety is a property of the system as a whole, being influenced by factors other than the behaviour of signalling equipment, and human behaviour, ergonomic design, and operating and maintenance procedures are all factors in the safety equation. Because the SSI system does not change the operating characteristics of the signalling system, the relative significance of such factors is unlikely to change, except possibly in the case of maintenance.

Safety is also influenced by reliability, in that a railway operating without signalling under emergency procedures is more prone to human error. Of course, poor reliability also has economic consequences, causing disruption to traffic, customer dissatisfaction and loss of revenue. Reliability is therefore an important consideration in signalling system design.

The requirement for safety and reliability is easy enough to express qualitatively, but is very difficult to quantify. Because current signalling technology is conventionally regarded as 'fail-safe', very little information exists on which to base a quantitative assessment of safety. Norton [3] proposed that the probability of unsafe failure of signalling interlocking should be in the order of 0.001 per annum over the whole of the BR system, a figure based on the frequency of major railway accidents and the total amount of signalling equipment in service. Norton included in this figure a further factor of ten to account for lack of experience with new technology.

On the other hand, figures published by the UK Department of Transport [4] for the period 1972 to 1981, for example, indicate an average rate of about four accidents a year due to defective signalling equipment (most of them very minor). As the probability of unsafe equipment failure leading to an accident is observed to be rather small, this figure may be regarded as a conservative estimate of the annual rate of unsafe equipment failure, and might be taken as a reasonable indication of the equivalent unsafe failure rate of those parts of the system which would be displaced by an electronic signalling system.

The fact that two possible approaches yield results differing by nearly four orders of magnitude illustrates the difficulty of setting realistic safety targets for a system which is normally regarded as 'fail-safe' in some absolute sense. This uncertainty is not as inhibiting as it might seem, however, because to meet any sensible safety target it is necessary to employ design techniques which are capable of providing levels of integrity which exceed low estimates of the requirement by a large factor.

Assessing the reliability requirement is also problematical, because it is difficult to deduce from available information how much of the total unreliability of present installations is associated with equipment displaced by an electronic signalling system, and how much is associated with power supplies, signals, point machines, track circuit equipment, tail connections and other sources of unreliability common to both.

It is clear, however, that to match the availability of a conventional relay interlocking, a computer-based interlocking needs to possess a degree of fault tolerance. Because signalling relays are individually very reliable (mean time between failures (MTBF) in the order of 1000 years) and because the distributed logic of a relay interlocking provides considerable independence between functions, total failure of an interlocking system is rare. On the other hand, performing the interlocking logic for an extensive area in a computer system carries the penalty of total loss of facilities whenever the system fails. On any reasonable estimate of the reliability of computer and data transmission equipment, the design of an interlocking and accompanying communications system has to be fault tolerant to provide adequate availability.

The use of such techniques in trackside interface equipment is more difficult to justify. Apart from the technical problems of introducing fault tolerance at the interface with signals, point machines and other signalling equipment, the limited consequences of failure do not make high availability design imperative. The approach taken with SSI has been to design trackside interface equipment to a target MTBF of 10 years, at which the overall effect on system availability is expected to be acceptable.

3.2 Available techniques

To achieve acceptably small probabilities of unsafe failure, there is no alternative to the use of redundancy

techniques. The techniques available range from the conceptually simple device of hardware replication to conceptually more difficult approaches enabling the use of nonreplicated (but not necessarily nonredundant) hardware.

The very high integrity requirements of railway signalling also demand that the problem of design errors be addressed. Straightforward replication using identical subsystems, for example, gives no more protection against design errors than would a nonreplicated system. Some design philosophies attempt to deal with this problem inherently, whereas others require design correctness to be demonstrated explicitly.

3.2.1 Duplication: A duplex system, in which two independent subsystems perform the same function and are required to agree as to the result, is potentially capable of providing safe operation. Such a system conventionally involves the use of a comparison device which is regarded as inherently safe and is responsible for imposing a safe set of output states when a disagreement is detected.

This conceptually simple scheme has weaknesses which must be overcome before it can be of practical use. For example, the concept of a fail-safe comparator implies use of the sort of technology which the system is designed to replace, and presents serious difficulties if the number of outputs is large or if the output is in the form of serial data. Fault detection coverage is poor, as faults which are detected only when they manifest themselves as output state errors may lie dormant for a long time. The system has no protection against divergence, by which is meant the inevitable tendency for the two subsystems to become out of step as a result of transient differences in their perception of input states.

3.2.2 Software duplication with self test: The use of two independent software systems within a single computer has been described [5]. This approach relies very heavily on the principle of diversity to prevent hardware faults and design errors affecting the redundant processes in the same way. Not only is the software diverse, but input and output data are usually arranged to be complementary. Comparison of partial results and a high degree of self testing are used to detect errors at an early stage, and a final comparison of output states is carried out in trackside interface equipment. Proof of independence is a potential difficulty, and the technique does not avoid the problems of errors in the specification and identical misinterpretations of it. Design of the self-test software demands detailed knowledge of the computer architecture which may not be available in the case of VLSI components.

Another technique which has been described [6] in connection with railway signalling uses information redundancy to detect faulty operation of a single software system. In carrying out its function correctly the software produces a sequence of check words which uniquely identify the logical path taken in calculating a result and prove the correctness of each logical step. The check words are processed by a second computer which, using similar techniques, produces a fail-safe dynamic output signal which in turn is used to energise one or more safety relays protecting the system outputs. This approach has the merit of avoiding either hardware replication or the design and production of diverse sets of software, but it is doubtful whether the ultimate complexity and cost of the system is less than for other methods.

3.2.3 Fault tolerance: Whatever means are used to satisfy the primary requirement of safety, the addition of a degree of fault tolerance requires yet more redundancy. An obvious approach, and one which is forced if the safe system is based on a single processor, is to provide a second safe system as a standby should the first fail. Fault survival in this case requires the spare system to be run as a hot standby in such a way that no unacceptable system perturbations occur at the time of change-over. Prevention of divergence and rapid fault detection and change-over are therefore essential. Furthermore, if it is required to repair the system without interrupting its operation, arrangements must be made to update a replacement at the time of installation.

Alternatively, a redundancy technique may be used which inherently provides both safety and fault tolerance. The class of redundant systems commonly referred to as 'fault masking', of which triple modular redundancy (TMR) is the simplest example, are potentially capable of satisfying this requirement. A TMR system will continue to operate so long as two of the three subsystems remain fault free; the failure of one subsystem is masked by the majority voting process. A TMR system designed such that a failed module can be removed and replaced without any disruption to the process being controlled is capable of providing very high levels of availability.

3.3 Choice of techniques for SSI

The methods used in the SSI system to ensure safe operation were chosen in the belief that they would be effective without being excessively difficult to implement or maintain. Diversity has been avoided, as the advantages of that philosophically attractive approach were not considered to outweigh the anticipated difficulties and cost of implementation. The preferred alternative of identical redundant subsystems accompanied by rigorous and formal demonstration of design correctness was expected to provide the necessary confidence in the integrity of the design at lower cost.

It was decided that the system should be (at least) single fault tolerant from the control panel multiplexer to the level at which trackside equipment accesses the data highway. The nonsafety function of interfacing the interlocking to the control panel is therefore duplicated, using two panel processors, each with a serial link to the panel multiplexer, part of which is also duplicated. The interlocking is a TMR system designed to permit online replacement of a faulty module, and the duplicated data highway linking it to the trackside interface equipment is operated in such a way that loss of either path has no effect on the performance of the system. Fault tolerant design has not been applied to the trackside interface equipment as the effects of failure are limited and the additional cost and complexity is thought not to be justified. A development of the duplication technique has been used to ensure a safe response to failures.

3.3.1 Duplication for availability: The two panel processors operate as a duplex system in which each acts as a hot standby for the other. Fault detection and redundancy management arrangements consist of simple self tests and a watchdog timer. Failure of one module leaves the other in full control with no performance degradation. Liebowitz [7] gives an expression for the mean time between system failures (MTBSF) of a duplex

system with repair:

$$MTBSF = \frac{1}{\lambda} + \frac{1}{2\lambda[1 - L(\lambda)]} \quad (1)$$

where

$$L(s) = \int_0^\infty e^{-st} f(t)\, dt \quad (2)$$

and $f(t)$ is the probability density function of the repair process, which has mean repair time $1/\mu$. Mine *et al.* [8] show also that if $\lambda/\mu \ll 1$, the MTBSF is not strongly influenced by the form of $f(t)$. The assumption of an exponential repair distribution leads to the simple result

$$MTBSF = \frac{1}{\lambda} + \frac{\mu + \lambda}{2\lambda^2} \quad (3)$$

For a module MTBF of 10000 hr and a mean time to repair (MTTR) of 10 hr, both of which are pessimistic in the present context, the above expression predicts a MTBSF of 572 yr. An optimistic assumption embodied in this result is that fault detection and redundancy management are perfect.

8.3.2 Duplication for safety: The development of the basic duplication technique which has been applied to the SSI lineside interface equipment is illustrated in Fig. 2. The two processors are maintained in loose synchronism and are prevented from diverging by the exchange of perceived input states and the adoption of a common strategy in case of disagreement. The regular comparison between processors of program memory contents and selected system states greatly improves fault detection coverage. The output comparison function is performed redundantly by the two processors independently monitoring the final system output states.

The redundancy management device provides a redundant and testable means of enforcing safe output states, enabling either processor to restore safe conditions should it detect a fault. Faults affecting the power interface alone result in a degraded form of operation in which outputs are held in a safe state while input processing and data highway message processing continue. Faults affecting the correct operation of either processor result in complete shutdown with all outputs automatically reverting to the safe condition.

The safety of this technique can be expressed in the form of a mean time between 'wrong side' (i.e. unsafe) failures (MTBWSF) by applying Liebowitz's result for the duplex standby case with $f(t)$ redefined as the probability density function of the fault detection process, assumed to have a mean fault detection time τ. Thus:

$$MTBWSF = \frac{1}{\lambda} + \frac{1}{2\lambda^2\tau} \quad (4)$$

If the MTBF of one half of the duplex system is 10000 hr and the mean time to detection of a fault is 1 s, for example, this expression gives a figure for the MTBWSF of 2×10^7 yr.

The use of such a model to estimate the probability of unsafe failure implies certain assumptions about the design of the system which must be justified as part of any design approval process. These are:

(*a*) that there are no design errors which might cause an unsafe failure which the system redundancy cannot detect or cope with. This is optimistic

(*b*) failures of the redundant parts of the system are independent. This is also optimistic

(*c*) all first failures, if undetected, would cause an unsafe malfunction of the system. This is pessimistic

(*d*) any subsequent failure would render the first, and itself, undetectable or leave the system unable to impose a safe state. This is very pessimistic.

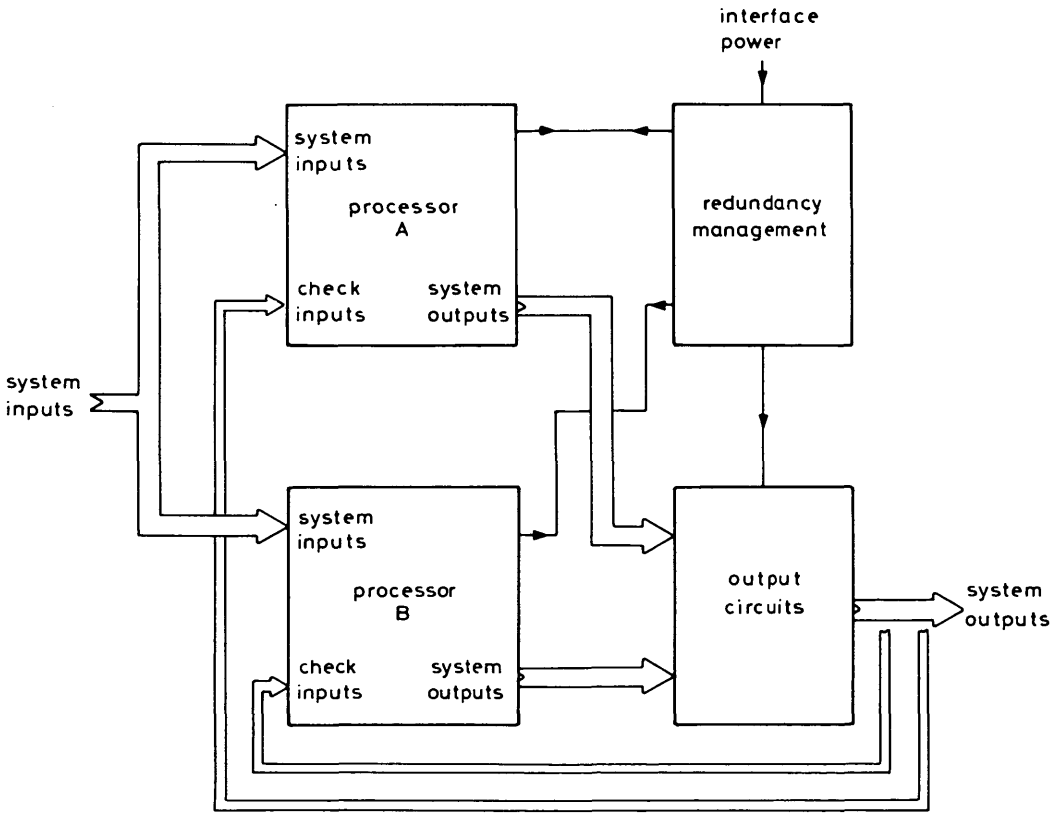

Fig. 2 *Duplication technique used in lineside interface equipment*

3.3.3 Repairable TMR: The triplication technique applied to the interlocking is, in many respects, an extension of the duplication technique described above. The majority voting process is performed redundantly within the three modules, both by monitoring output states and by comparison of program memory contents and selected system states. Each module (Fig. 3) includes a redundancy management device which provides a redundant and testable mechanism for disconnecting a module in the event of a majority vote against it and enforcing safe output states if no majority opinion exists. This mechanism can be activated by the parent processor acting alone, or by the other two modules acting together, and the design is such that an isolated or absent module appears to be voting against the other two.

As the safety level output of an interlocking consists only of the two data highway message streams, the maintenance of safe output states involves preventing the transmission of correctly coded data highway messages carrying incorrect information. Output from a disconnected module is prevented by the hardware design, but the first line of protection against incorrect data output is achieved by checking each transmitted bit and, if the data is incorrect, forcing the remainder of the message to be Manchester invalid.

System repair simply involves replacement of the faulty module. When power is applied, the replacement is updated independently by the two existing modules before being allowed online.

An expression for the MTBSF of a 2 out of 3 system with repair is given by Downton [9]:

$$MTBSF = \frac{1}{2\lambda} + \frac{1}{3\lambda[1 - L(2\lambda)]} \quad (5)$$

Applying the previous assumption of an exponential repair distribution with $\lambda/\mu \ll 1$, and assuming once again a module MTBF of 10000 hr and a MTTR of 10 hr, the predicted MTBSF is 191 yr.

As with the duplication technique, the MTBWSF for a repairable TMR system can be obtained by applying the above expression with $f(t)$ redefined as the probability density function of the fault detection process, assumed to have a mean fault detection time τ. Assuming once again an exponential distribution and recognising that

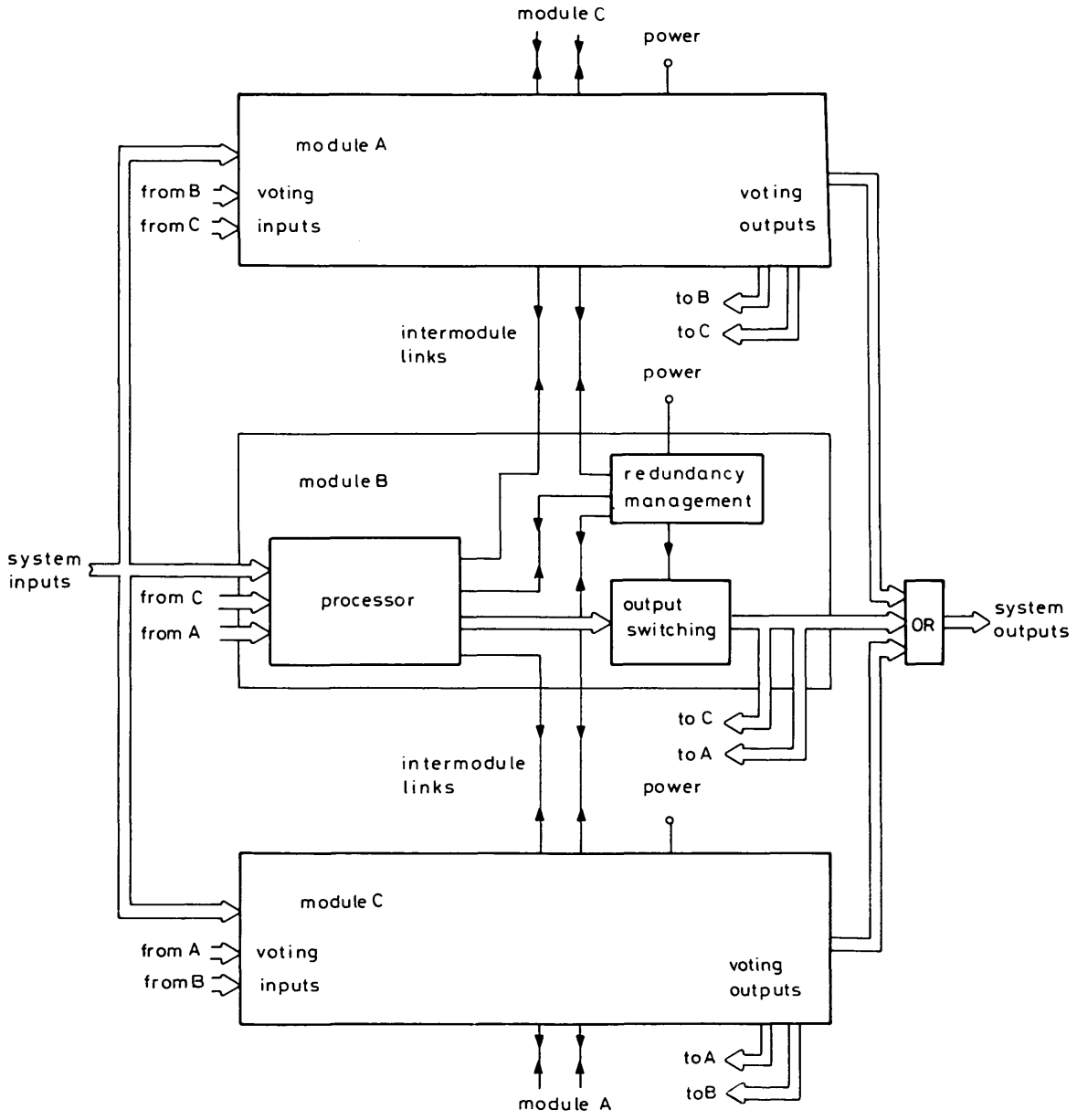

Fig. 3 *Triple redundancy technique used for interlocking processors*

$\lambda\tau \ll 1$,

$$MTBWSF = \frac{1}{2\lambda} + \frac{1}{6\lambda^2\tau} \quad (6)$$

For a module MTBF of 10000 hr and a mean fault detection time of 1 s, the figure obtained for the MTBWSF is 6.8×10^6 yr, with qualifying assumptions as before.

4 Communications

4.1 General requirements

The feature which most of all distinguishes the solid state interlocking from other electronic signalling interlocking systems is the direct linking of the interlocking to electronic trackside interface equipment by means of a data highway. Because of its importance to the success of the system, the behaviour of the data highway has been studied both theoretically and experimentally to assess its performance, range and transmission reliability.

The need is for an omnibus bidirectional data highway capable of linking the interlocking to a maximum of 63 trackside interface units and capable of working reliably in the harsh electromagnetic environment of a railway. For reasons of overall availability it is necessary for the data highway to be fault tolerant, and the data path is therefore duplicated. The protection given to the signalling information content of messages has to provide a high level of security under any credible fault condition, and demands a cyclic polling protocol in which loss of communication is detectable within a short time and is interpreted as indicating the most restrictive system state. The timing of polling messages and replies on the bidirectional highway needs to allow for propagation and repeater delays equivalent to a range of at least 60 km.

4.2 Baseband data transmission

The baseband data highway used for SSI is a low bit-rate extrapolation of techniques previously described in connection with the control of fly-by-wire aircraft [10–12] and now established as the basis of the MIL-STD-1553 data highway. Information is transmitted in the form of discrete messages of fixed format, carrying address, signalling control and status information, protected by two levels of coding. The first level of coding adds five parity bits to form a truncated (31, 26) Hamming code, and the second level is provided by transmitting the message in Manchester coded biphase form. The start of the message is uniquely identified by a synchronising pattern and three Manchester coded '1's which are used by the receiving equipment to form an accurate estimate of the message timing. Additional protection is provided by the use of a dedicated screened cable carrying relatively large signal levels. The format is illustrated in Fig. 4. The data rate chosen for the baseband data highway has been influenced by a number of conflicting design requirements, including the minimum acceptable polling rate for trackside equipment, the size of a single interlocking area in terms of the number of input and output functions, the requirement to encode information in real time using safe processing techniques, and the need for an acceptable range without repeating. The data rate chosen was 20 kbit/s (after Manchester coding), and the transmission protocol used requires trackside equipment to reply immediately after being addressed by the interlocking.

4.3 Modelling of data distortion

Early studies of data link behaviour were based on 'text book' models of low-frequency transmission lines, using the published parameters of the screened twisted pair cable which it was intended to use. These studies predicted an attenuation of about 2 dB/km and a distortion limited range of about 10 km, from which it was deduced that one interlocking would be able to cover a range of 20 km via a centre-fed data highway. Longer ranges were to be achieved by adding repeaters to the baseband data highway or by interposing a suitable long distance transmission medium.

Initial trials with an experimental installation suggested that this simple analysis did not provide an adequate understanding of baseband data transmission. In particular, it was found that the expected range of a long centre-fed transmission line was not achievable. A better understanding was sought by modelling the transmission process without the usual simplifying assumptions. The model developed can be used to study the data distortion produced by a wide range of transmission system topologies and includes a modelling of the properties of the data receiver, enabling the timing of the recovered data to be predicted.

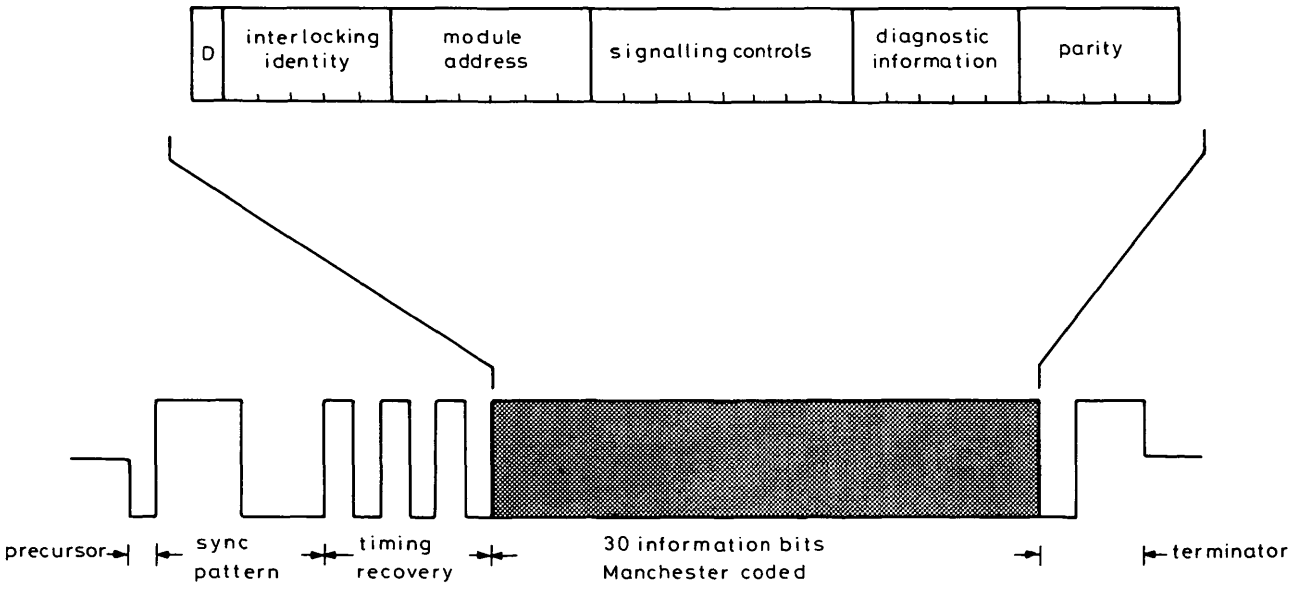

Fig. 4 *Baseband data highway message format*

The important spectral components of a 20 kbit/s Manchester coded baseband data stream occupy a frequency domain in which cable parameters vary considerably with frequency, and the ability of the model to produce results consistent with the performance of a real baseband transmission system depends upon the correct modelling of this variation. In the region of interest, r is in transition between its DC value and the $\sqrt{\omega}$ characteristic applying at high frequencies, and l is influenced by the incomplete containment of the magnetic field within the cable screen. To enable an assessment to be made of the dependence of data highway performance on cable type, the parameters of a number of cables have been measured over a range of frequencies and empirically derived expressions for r and l obtained for use in the model.

Modelling the cable used for the trials showed that the timing of recovered data is not affected by waveform distortion provided that the total line length does not exceed 8 km. For cable lengths greater than 10 km distortion causes timing errors which cannot be tolerated without compromising the security of message acquisition. The model also explained the lack of success in operating a long centre-fed highway, because the distortion caused by long lines is shown to degrade transmission between points separated by very much less than the total line length.

Fig. 5 shows some examples of the results produced by the model when applied to the synchronising and timing recovery portions of the biphase waveform. Fig. 5*a* is the model's reconstruction of the waveform output by the transmitter into a terminated line of zero length. Figs. 5*b*, *c* and *d* are the waveforms arriving at a receiver 10 km from a transmitter driving lines of length 10, 15 and 20 km, respectively. The receiver has a threshold device which switches at the levels shown.

4.4 Data link modules

The interlocking and lineside equipment are linked to the data highway by data link modules consisting of a data transmitter and receiver designed to satisfy the special needs of the high integrity baseband transmission system.

The transmitter couples the Manchester coded bipolar data signal to the line at a level of 2.5 V peak. The receiver contains a data filter and a threshold device which switches at line voltages of ± 0.25 V. Additional data switching and transmitter control logic is provided which enables a pair of DLMs working back-to-back to be used as a baseband repeater.

4.5 Error performance

The error performance of the baseband transmission technique has been studied in both 750 V DC and 25 kV 50 Hz electrification environments using an experimental installation consisting of 6 km of cable with a message generator at one end and a data receiver at the other. The received data have been analysed for various categories of error, and the results have shown a very high degree of immunity to electromagnetic interference provided that the data cable is fault free. During two years of operation, no errors were recorded at the 25 kV site, whereas the 750 V DC site recorded occasional message loss (typically 1 message in 10^6) due to breakdown of the lightning-surge arresters terminating the cable. Although certain deliberately induced cable faults have been found to corrupt as many as one message in four, the first level of coding (i.e. the Manchester code) has been broken only twice, a fact which reflects the preponderance of 'stuck at' errors in a baseband system and the improbability of inverting a Manchester coded bit without destroying the Manchester validity of the rest of the message. These results reflect the security provided not only by two levels of protective coding, but also by the use of large signal levels and a correspondingly large receiver threshold. They give a high degree of confidence in the security of the SSI transmission system.

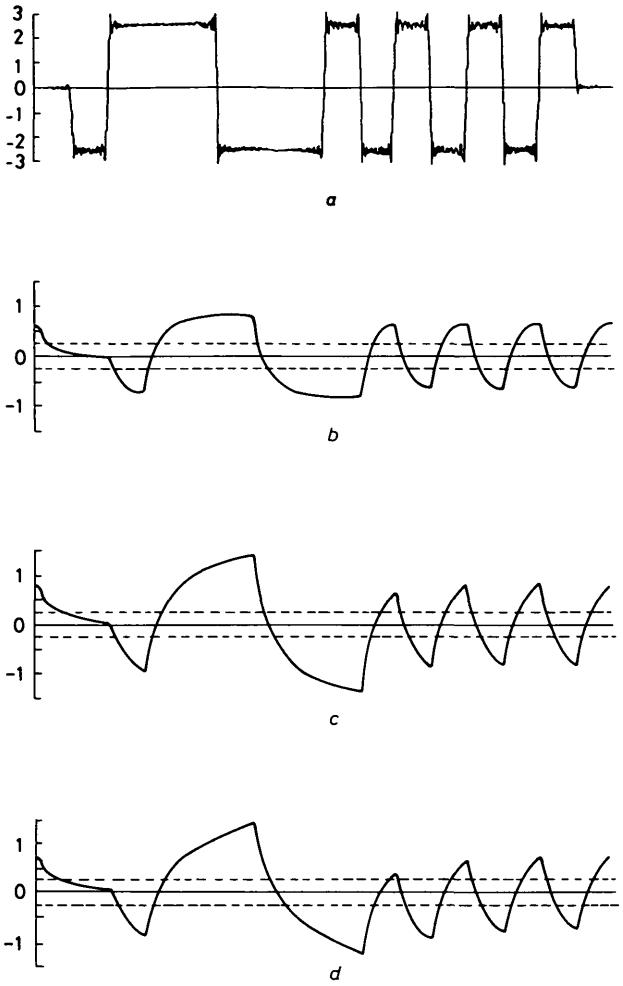

Fig. 5 *Examples of data highway model distortion predictions*
a Transmitter output into zero length terminated line
b Pathlength = 10 km; line length = 10 km
c Pathlength = 10 km; line length = 15 km
d Pathlength = 10 km; line length = 20 km

4.6 Long distance transmission

The SSI concept embodies the concentration of all interlocking logic at the signalling control centre, requiring long distance data transmission to link interlockings with their baseband data highways. For long distance transmission SSI data highway messages are labelled with a unique system identity, further encoded and converted to a data rate of 64 kbit/s. The resulting data stream has sufficent coding security to be sent over any standard 64 kbit/s data channel. A trend towards the provision for general lineside telecommunications purposes of fibre-optic systems with frequent drop/insert nodes makes this approach particularly attractive.

5 Software and data structures

5.1 Software organisation

Every signalling scheme is unique in terms of track layout, arrangement of track equipment, routing of trains

and the interlocking logic required. The cost of software development and validation, and the sheer amount of time involved, would be a severe disadvantage to any design which required software to be rewritten for each such application. SSI has therefore been designed as a data-driven system, in which a program of quite general application operates on a database unique to each installation. This technique is applied to the interlocking, panel and diagnostic processors, and also to the simulation equipment used for functional testing (see below). The data is compiled from a specialised design language with which the signal engineer can specify the signalling controls and indications required and their logical relationship. The relationship between the general purpose software and the database is such that the more commonly found functions are supported by the software and require the minimum of application data, whereas less common functions may be specified explicitly through the use of logical data constructs.

The standard software operates also on a set of variables representing the state of the signalling system. In both the interlocking and panel processors, for example, a variable is reserved for each of 128 signals, 64 sets of points, 256 track circuits and 256 routes. Other variables are reserved for latches and timers and for maintaining an up-to-date record of the system's input and output states. Two examples of interlocking variables are given in Table 1. The structure of the interlocking signal variable reflects the complexity of the interlocking function, as much of that complexity is associated with the manipulation of the various attributes of signals and the control of signal indications.

Table 1: Examples of interlocking variables

a Signal memory variable

Byte number	Bit number	Function
1	7	= 1 if train operated route release test passed
	6	= 1 if signal module not disabled
	5	= 1 if aspect control set
	4	= 1 if signal stick set
	3	= 1 if aspect not disconnected
	2	= 1 if temporary approach control not applied
	1, 0	train in section proving code
2	7	= 1 if lamp proved lit
	6	= 1 if signal in automatic mode
	5	= 1 if free of approach locking
	4	= 1 if route indicator proved lit
	3	= 1 if route entrance button pulled
	2-0	signal aspect code
3	7-0	approach locking timer

b Track circuit memory variable

Byte number	Bit number	Function
1	7	= 1 if track circuit clear
	6	= 1 if technician's control clear
	5-0	spare
2	7-0	track circuit timer

With the sole exception of the technician's terminal processor, in which interrupts are used, all software is organised on a cyclic basis. The interlocking software is organised around the concept of a major cycle, corresponding to one complete cycle of the whole interlocking system, which in turn consists of 64 minor cycles, each of which involves the processing of one incoming data highway message and the preparation and transmission of one outgoing message. The interlocking minor cycle includes the following processes:

(*a*) redundancy management: state comparisons, self tests and strategies for maintaining safety and availability

(*b*) interfaces: exchange information with external processes and antidiverge incoming data

(*c*) update timers: updates a subset of track circuit, signal and general purpose timers

(*d*) process incoming data highway message: operates upon each bit of incoming data according to its associated geographic data and updates the record in RAM of the state of the system

(*e*) process flag data: processes a subset of the geographic data for general purpose flags

(*f*) process panel requests: interprets any panel request code received from the panel processors according to the associated geographic data.

(*g*) process outgoing data highway message: the data for the next outgoing data highway message is prepared according to the associated geographic data. If the message is addressed to a points module the process is simple, but the preparation of messages for signal modules embodies much of the logical complexity of the interlocking and involves some or all of the following processes:

(i) train in section proving
(ii) signal stick unsetting
(iii) route step-up
(iv) aspect control
(v) temporary approach control
(vi) route indicator control
(vii) aspect sequencing
(viii) AWS control
(ix) approach locking release
(x) route release.

The interlocking is designed to survive short power supply interruptions without loss of vital information. The safe and reliable implementation of this feature has required complex comparison and decision making strategies to be built into the initialisation software.

The panel and diagnostic processor software is similar in that it is also organised around the interlocking's major and minor cycles. Trackside equipment software is designed to handle redundancy management, message acquisition, message transmission, input processing and output control as part of a continuously executed cycle.

5.2 Geographic data

It is impossible here to give a comprehensive account of the structure and syntax of the geographic data language, but it is hoped that a simple example will serve to illustrate the principle. The following construct is a database entry for a panel request for the route 11(2M).

```
*QR11B  if    R11(2M) a, P103 qnf, P105 qnf,
              U56AB f, U60AB f
        then  R11(2M) s, U44BA 1, U48CB 1, U52CA 1
              U54BA 1, U56BA 1, U58BA 1, 060BA 1,
              P103 qn, P105 qn, S11 clear bpull \.
```

*QR11B is a label used by the data compiler which translates this design language into machine-readable code. The construct consists of the logical statement 'if', followed by a set of conditions which must be true for the route to be available; and the logical statement 'then', followed by a list of actions to be taken if the request can be executed. In English it reads: 'If route 11(2M) is available (i.e. not already set) and points 103 and 105 are

normal or free to go normal and Subroutes 56AB and 60AB are free, then set route 11(2M), lock subroutes 44BA, 48CB etc., lock overlap 60BA, normalise points 103 and 105 and clear the "button pulled" bit for signal 11'.

The above compiles into 34 bytes of machine readable data. The panel processor database uses similar data constructs, whereas the databases for the diagnostic processor and simulator are closely related to the physical connectivity of the system and are largely compiled from a database containing the allocation of system inputs and outputs. The size of a typical interlocking processor database is 12–15 Kbytes.

As already intimated, the SSI design philosophy has required design correctness to be demonstrated explicitly, and those parts of the software intimately concerned with safety have been subjected to a rigorous programme of validation. The general approach to this task and the procedures used have been described by Short [13].

6 Support systems

The provision of support systems for aiding the application of the system to particular installations has been regarded as an essential part of the SSI development programme. The two principal application tools are a set of aids to geographic data preparation and a controlled area simulator. The latter has also been an important system development tool.

The simulator consists essentially of a computer which responds to information received over the trackside data highway as if it were some or all of the lineside interface equipment of the simulated installation. It is attached to a colour display system which indicates the state of the simulated railway in the form of a track diagram, through which the state of system inputs such as track circuits, point detection and signal lamp proving can be manipulated. Facilities are provided for simulating the various modes of failure of the data highway and lineside interface equipment, and for simulating the movement of trains through the area. A second display system is provided to take the place of the signalman's control panel, enabling the functions of an interlocking to be fully exercised in the laboratory or design office. As with the interlocking, the simulator software is of general application and is designed to operate with a database representing the physical arrangement of the installation concerned.

A second essential design tool is the set of four data compilers which translate scheme design information into the machine readable databases for the interlocking, panel, diagnostic and simulator computers. The data compilers and the simulator are currently being combined in a special purpose design aid for electronic signalling systems known as the SSI design workstation. The workstation is based on a proprietary multi-user microcomputer system, and provides a comprehensive set of design tools intended for use in the signalling design office. Also included is a single channel (i.e. nonredundant) interlocking and a simulator computer. Among the facilities provided are:

(*a*) prompted input of equipment, track section and control panel identities and the allocation of functions to system inputs and outputs. The database so established provides information for the data compilers and for the automatic production of scheme documentation in various formats

(*b*) input and syntax checking of geographic data design language statements

(*c*) compilation of machine readable databases for interlocking, panel, diagnostic and simulator computers

(*d*) interpretation of machine readable interlocking data for checking against signalling requirements

(*e*) design of screen layouts for simulator displays and automatic generation of application-specific display data

(*f*) downloading of geographic and display data into single-channel interlocking and simulator for functional testing.

(*g*) downloading of geographic data into EPROMs for final installation

(*h*) selective interrogation of tapes from the technician's maintenance aid event logger.

The design workstation is expected to reduce scheme design costs significantly, and the simulation facility will considerably reduce the amount of testing which has to be carried out on the final installation. At present the primary source of information from which geographic data statements are prepared is the signalling control tables, which are themselves an interpretation of the scheme plan and a standard set of signalling principles. Opportunities for further automation are perceived, possibly leading to a knowledge based approach to scheme design.

7 The pilot scheme

The first solid-state interlocking scheme was commissioned at Leamington Spa on 8th September 1985. The contractors for the installation were GEC-General Signal and Westinghouse Signals, who have collaborated with British Rail in the engineering development of the system.

The choice of site was influenced by a number of factors, including size, complexity, traffic density, operating features and the condition of the existing signalling infrastructure. Leamington Spa was a modern layout equipped with colour light signals and electric point machines, but operated from an ex-Great Western Railway mechanical lever frame. It also included examples of most types of signalling requirement, and was of ideal size for a first scheme, extending to about 15 route km. It has 35 signals, 15 sets of points, 48 track circuits and 71 routes, and the 40 lineside interface modules required amount to about two-thirds of the capacity of one SSI.

The interlocking and lineside equipment was installed at the beginning of 1985. A temporary overlay of multicore cables and a set of dummy loads and inputs was also installed, enabling the complete system to be operated in traffic simulation without any connection to the working railway. As part of an extended period of testing and monitoring all the connections to the real railway were individually exercised, and in the later stages the system was connected to the real track circuits and run in parallel with the existing signalling. Throughout this operation the use onsite of a controlled area simulator and the comprehensive monitoring facilities of the maintenance aid proved invaluable.

It is to be expected that a pilot scheme should reveal unforeseen problems and design weaknesses, and the Leamington scheme has been no exception. However, the number of problems has been small, and none has required any fundamental reappraisal of the SSI concept. Plans exist for the installation of SSI schemes at Inverness, which will be the first multi-interlocking system, and at York, Newcastle and Glasgow North.

8 References

1 CRIBBENS, A., FURNISS, M.J., and RYLAND, H.A.: 'The solid state interlocking project'. *IEE Conf. Publ. 203*, 1981, pp. 1–5

2 CRIBBENS, A.H.: 'The solid state interlocking'. Proceedings of IRSE International Conference on Railway control and automation towards the 21st century, London, UK, 1984, pp. 24–29

3 NORTON, D.J.: 'Safety by redundancy', *Proc. Inst. Railw. Signal Eng.*, 1978/1979, pp. 129–139

4 Annual reports on 'The safety record of the railways in Great Britain'. HMSO, 1972–1981

5 VON LINDE, O.B.: 'Computers can now perform vital functions safely', *Railw. Gaz. Int.*, Nov. 1979, pp. 1004–1007

6 RUTHERFORD, D.B.: 'Failsafe microprocessor interlocking with safety assurance logic — establishing a vital benchmark'. Proceedings of IRSE International Conference on Railway control and automation towards the 21st century, London, 1984, pp. 72–76

7 LIEBOWITZ, B.H.: 'Reliability considerations for a two-element redundant system with generalised repair times', *Oper. Res.*, 1966, **114**, pp. 233–241

8 MINE, H., OSAKI, S., and ASAKURA, T.: 'Some considerations for multiple-unit redundant systems with generalised repair time distributions', *IEEE Trans.*, 1968, **R-17**, pp. 170–174

9 DOWNTON, F.: 'The reliability of multiplex systems with repair', *J. R. Stat. Soc., Ser. B*, 1966, **28**, pp. 459–476

10 BALLIET, L., and HOCKENBERGER, R.: 'A wideband data distribution system'. IEEE International Convention and Exposition, New York, USA, 1973, II

11 GROSS, J.P.: 'Data bus techniques for digital avionics'. Proceedings of IEEE National Aerospace Electronics Conference, New York, NY, USA, 1973, pp. 230–237

12 BELLO, L.M., and BERG, T.C.: 'LSI data bus for avionics'. Proceedings of IEEE National Aerospace Electronics Conference, New York, NY, USA, 1973, pp. 238–244

13 SHORT, R.C.: 'Software validation for a railway signalling system' *in* BAYLISS, J.A. (Ed.): Proceedings of IFAC Conference on Safety of computer control systems, 1983, pp. 183–193