THE SIEMENS AND HALSKE T52e CIPHER MACHINE

A series of cipher machines designated T52 was manufactured by Siemens and Halske between 1934 and 1944. They were built around the T36 teleprinter, to which were added encipherment and decipherment mechanisms. The machine could be used like a teleprinter, enciphering its output to the telegraph line and, when it was receiving from the telegraph line, deciphering the message before printing it. So the T52 machines operated 'on-line' and when two machines were connected by a telegraph line (or equivalent communications path) they could be used like standard teleprinters, sending messages in cipher from one to the other. As with teleprinters, only one direction of transmission could be used at a time but the operator did not have to switch from send to receive, or from encipher to decipher. The use of the keyboard established the sending and enciphering mode.

The T36 teleprinter dates from about 1928. A patent for a 'secret telegraph system' based on modifying the T36 was filed in Germany on 17 July 1930 by Jipp, Rossberg and Hettler, and assigned to Siemens and Halske. This became US patent 1,912,983 dated 6 June, 1933. The basic principles of the T52 machines can be found in this patent.

The design of the T52 machines was continually improved, particularly under the stimulus of the 1939-45 war. Models a, b, c, d, e and f have been reported. It is said that a model known as a/b was in use at the beginning of the war and that model T52f was never put into production because the factory was bombed in October 1944.

This report is based on a close examination of two machines, one in Munich at the Werner von Siemens Institute for the History of the House of Siemens and the other in the Science Museum, London. Both machines came from Norway and were probably part of a group of machines in use in Oslo at the end of the war. The assistance of the Siemens Institute and the Science Museum is gratefully acknowledged and so is the help of the Norwegian Technical Museum in Oslo.

Both machines examined are models T52e. They have a three-position control switch which enables them to be set for operation as model e, in clear or as d machines. In this sense, they could be called models d/e. Somewhat surprisingly, the Science Museum machine has a label giving it as T52c. It differs from the Munich machine in a few respects which will be detailed at the end of the report. It seems to have been modified from an earlier model and has vestiges of earlier mechanisms which will be described later.

The Science Museum machine has serial number 43996 and the Munich machine serial number 67323.

There are believed to be similar machines elsewhere in West Germany, at the Norwegian Technical Museum in Oslo and at Crypto AG in Zug, Switzerland.

PHYSICAL LAYOUT

Figure 1 shows the plan view of the machine. It contains 6 sub-units which are attached to a heavy base.

The base contains, at its back, sockets for the tape-reader and punch and large resistors for the motor AC supplies. At the front it has two control knobs operating large multi-contact switches. One of these connects the input of the machine either to the tape-reader or the keyboard. The other switch sets the machine in one of the three conditions T52d, clear or T52e.

The various sub-units except the keyboard connect electrically to the base through jackpoints. Within the base is a mass of wiring connecting the jackpoints and also the control switches mentioned above and a set of capacitors. The six sub-units will next be described, followed by a description of the function as a whole.

Wherever possible in this report the names used for the parts are those originally used or have been taken from documentation of the T36 machine. Where the correct name is not known our invented name will be marked in the report by the symbol (*).

1. The T36 Teleprinter Mechanism

The centre of the machine contains the T36 mechanism on its own base, which can be detached by removing two bolts. This mechanism has a drive motor with a speed regulator, driving 3 camshafts through a gearbox. We have called these the transmit, receive and translate/print camshafts respectively. Each camshaft rotates when a clutch is released by a magnet (AMs, AMe, AMü) shown in the diagram. The translate/print camshaft has, attached to its front end, a type wheel containing raised letters and figures. A magnet DM hits the paper tape against the inked type wheel, on-the-fly. Details of the printing mechanism and its circuit are given later.

2. Keyboard

The keyboard fits into the base and, unlike the other sub-units, is connected by wires to terminal points, not by jacks. It operates five changeover contacts S1-S5 and a trip contact. Its mechanism is linked by a lever and a wire linkage to a cam on the transmit camshaft. Details will be given later.

Together, the T36 mechanism and the keyboard, with relays R1-R5, AR and KLR are the standard mechanism of the T36 teleprinter. The remainder of the units to be described are special to the T52e. The relays Ü and RR3 (*) are not found in the T36 teleprinter and are part of the T52.

3. Coding Wheels and Cams

At the back of the machine is a large frame containing, at the top, ten independently moving wheels which are stepped on by pawl mechanisms. Each wheel has a different number of steps for a complete rotation. For wheels W1-W10 (*) the number of steps is 47, 53, 59, 61, 64, 65, 67, 69, 71 and 73 respectively.

Each wheel has a cam which operates two sets of changeover contacts shown in Figure 2 which we have called A and B (*). The cam profiles generate a pseudo-random binary sequence. The positions of the wheels can be set by operating the large lever shown at the front of the machine. Wheel positions can be read from numbers as shown at the right of Figure 2 where the indicator, the thumb wheel used for setting, the ratchet wheel and the cam are shown. Note that there would be room for additional cam wheels to the right of the existing one.

As shown in Figure 2, the contact sets A and B are spaced about 1/3 revolution apart on the cam. Reading from contact sets A, Figure 3 shows the pseudo-random cam - sequences as taken from the Munich machine. In the figures which follow, contacts A and B are shown in their unoperated or zero position, ie the low condition of the cam surface.

The separation between the A and B contacts is indicated in Figure 3. When the wheels are set at position 1, the A contacts read state 1 of this figure and the B contacts read the state at the black square. The spacing between A and B contacts is given. Note that the output sequence at contacts B is delayed by approximately 1/3 revolution compared with that at contact A.

In the Science Museum model, the pattern of coding on the cams is the same, but the wheel numbering does not agree. Details are given later.

Figure 2 shows the interposer mechanism operated by a magnet M (*) which can inhibit the motion of a cam. Normally, all the pawl carriers PC (*) are dropped by the rotation of the drive shaft DS (*) allowing the pawls to fall and then positively rotate the coding wheels when they return. When M is operated an interposer prevents the pawl carrier from dropping and the wheel does not rotate. Each wheel has such a magnet. For setting the wheels, the unlocking shaft US (*) rotates anti-clockwise lifting the pawl from the ratchet wheel. A sprung roller pressing on this wheel locates and holds the wheel during setting. In the Munich machine, but not the Science Museum machine, there is an additional pawl preventing counter-rotation. This makes the mechanism more reliable but allows the wheels to be manually set only in the forward direction, which is inconvenient.

The movement of the pawl carriers by shaft DS is derived from a cam driven by a motor through a one-cycle clutch which is released by magnet AMC (*). There are other cams on this shaft which operate contacts, to be described in detail later.

The frame containing the motor, drive mechanism and coding wheels can be tilted backwards against stops when two bolts are removed from the front feet, the link to the unlocking lever is lifted off and a safety latch on the left of the machine is released. This gives access to the rear of the T36 mechanism. By removing a clip and a shaft, the coding wheel mechanism could be detached for maintenance or replacement.

4. The Relay and Key-setting Box

On the right of the machine there is a black box with a lockable lid containing 20 relays and 10 rotary switches, shown on Figure 1.

The switches are used to set the 'basic key' of the machine. The 10 switches are labelled A B C D E F G H J and K. They correspond in reverse sequence to the wheels W10 to W1 respectively. Each switch has 10 positions which are labelled 1, 3, 5, 7, 9 followed by the Roman numberals I, II, III, IV, V. The reason for this notation will be conjectured later.

The jackpoints of this relay and key setting box, which can be removed by detaching two bolts, are included in our circuit diagrams using a notation, which is our own, shown in Figure 21.

5. KTF Unit

At the front left of the machine is a small box containing a switch with 10 changeover contacts KT1-KT10. It can be removed by releasing four bolts. The switch is labelled 'with' and 'without' KTF. The meaning of 'KTF' is unknown but its function will be described later. Only contacts KT1, KT3, KT5 and KT7 of the switch are in use but the others have been used at one time then disconnected. The precise way in which the KTF switch is included in the machine's circuits was probably changed from time to time as an additional security feature. This is the reason why all the connections via the KTF jack are shown in the circuit diagram of Figure 10, where the KTF contacts appear.

6. Power Supplies

The machine appears to require three D.C. power supplies as well as 220V A.C. Two of the D.C. supplies come from outside the machine and one is internal. This internal supply was measured as 150 volts in the Munich machine and 120 volts in the Science Museum machine. It provides the source of power for the 20 relays in the black box.

THE CONNECTING PLUG, EXTERNAL SUPPLIES AND CIRCUIT NOTATION

From the back of the base of the machine a flexible cable is joined to a 13 pin plug. We believe that, in operation, this was attached to a line-connection unit to which were attached power units and the telegraph line. This line-connection unit contains additonal relays U, ER,V, D and Th for which we have obtained the circuit from the documentation of the T36 teleprinter.

In our circuit diagrams the notation P1-P13 (*) is used for the points of this connection plug. The function of the 13 connections is shown in Figure 20 together with our notation for other components shown in our circuit diagrams. We also show here our notation for the internal power supply and the two external power supplies which enter through this plug.

All connections to this plug except the earth wire go through filters located in the base of the machine at the right side. The two AC connections have the standard filter and one extra filter each. The DC resistance of each filter is about 12 ohms.

The notation +N and -N comes from the documentation of the T36 teleprinter. The notation for the other power supplies is our own. The cam contacts on the pawl drive shaft have been denoted by Greek letters since we do not know the original notation. The other nomenclature of Figure 20 is authentic.

LOGICAL PLAN OF THE MACHINE

Figure 4 shows, in schematic form, the plan of operation of the machine.

Encipherment and decipherment take place in the contacts of relays SR1-SR10. The keyboard contacts (or tape-reader contacts if this is switched in) generate five signals which after encipherment are sampled by cam contacts F2-F6 on the transmit camshaft. When transmitting, the relay U (which is in the line-connection unit) is operated so that the telegraph signal leaves on 'line a'. At the same time the signal operates the polarised relay ER which generates the copy of the telegraph signal which enters the 'receive' section of the T52 machine. Here, it is sampled by the receive cam contacts F10-F14 and, passing through the 'decipher' contacts of SR1-SR10, the five samples operate the relays R1-R5 which then store the plaintext character. The outputs of these relays operate the translate and print unit.

When receiving, the U relay is released, the ER relay operates from 'line a' and a repeated signal enters the receive cams. During transmission, the transmitted ciphertext is received and deciphered to generate the local printout.

Printing locally from a deciphered character checks the correct operation of the contacts of relays SR1-SR10 but does not verify that the correct SR relays are operated.

Details of the encipherment and decipherment method will be given later. The remainder of the system is concerned with generating pseudo-random binary sequences for the 10 channels SR1-SR10.

The sources of the pseudo-randomness are the B contact outputs of the 10 coding wheels W1-W10 shown in the figure. The movement of these coding wheels is controlled by the interposer magnets M1-M10 which are operated by logical functions of the outputs from coding wheel contacts A1-A10. This feedback mechanism generates a long sequence of pseudo-random data from the wheels. Part of the logic of the interposer magnets is provided by the KTF circuits using a relay contact RR3 derived from the third telegraph element of the plaintext as stored on relay R3. Thus, when KTF is switched on, the motion of the coding wheels depends on an earlier plaintext character. In such an operation, errors on the line will affect the wheel motion at the receiver and put the two machines out of synchronism. For this reason, if the line is bad, KTF can be switched off. Without KTF, the synchronism of wheel positions at sender and receiver is dependent on having the same initial setting and then stepping both sets of wheels whenever any character is sent.

The B contacts from the coding wheels (at a different place on their circumference) provide the signals which, after transformation, operate the relays SR1-SR10. The B outputs are first transposed by the key-setting switches according to the setting of the basic key. The transposed channels are called X1-X10 (*). The H relays are logical functions of these channels, and the SR relays are logical functions of the H relays, when the machine is operating as a T52e. In the clear position, the relays SR are set so that the characters are not transformed. In the T52d setting, the SR1-SR10 relays are operated directly by the channels X1-X10.

Figure 4 also shows the relative timing of the camshaft movements. When transmitting, the receive camshaft operates very soon after the transmit camshaft. (When the machine is receiving, the transmit camshaft does not turn at all). Near the start of the motion of the receive camshaft, cam F37 operates the magnet (AMC) which releases the coding wheel pawl mechanism. Near the end of the receive camshaft motion, cam F20 operates the magnet AMü which releases the translate/print camshaft. At the end of these cycles, the motion of the camshafts can be repeated almost at once. Experimentally it was found that about 6 characters could be sent per second. The relays R1-R5 hold the character to be printed during the delayed motion of the print camshaft. The timing will be shown in more detail later.

To summarise, the 10 coding wheels control their own motion by feedback from contacts A through the logic of the interposer magnets. From their contacts B, they produce signals which, after transposition by the key-setting switches and logical operations due to the H relays, generate the 10 pseudo-random binary sequences of the SR relays which carry out the encipherment and decipherment functions. Receiving a character involves the receive camshaft and decipher logic, the relays R1-R5 and the translate and print logic. When a character is transmitted, it is at the same time received, deciphered and printed in clear form.

ENCIPHER-TRANSMIT CIRCUIT

Figure 5 shows the circuit used to transmit an enciphered character. The plaintext character is generated by the keyboard contacts S1-S5 or by the tape-reader if this is used. The circuits involving the tape-reader are not shown. With the voltages shown on the contacts of S1-S5, if they were connected directly through to the contacts F2-F6 they would generate the 5 information-carrying elements of the telegraph signal on the transmit circuit, which leaves the machine on pin P9 of the connection plug.

In the rest state, relay AR is off and a positive signal appears on the transmit circuit. The telegraph signals are derived from a power supply T (*) through current limiters. When any key is depressed, relay AR operates and places the negative or 'start' element on the transmit line through contact F1. At the same time, current goes to the release magnet AMs, starting the transmit cycle, the timing of which is shown in Figure 6. Relay AR is soon released so that at the end of the cycle cam F1 again transmits the stop signal of positive polarity.

Encipherment is carried out by the changeover contacts shown in our diagram in the rectangular boxes associated with each of the 10 relays SR1-SR10. The contents of one box are shown and the particular contacts used can be identified in the plan of the SR relays shown in Figure 7. Each box either transposes two lines or connects them straight through. In the non-enciphering or 'clear' condition, SR6-SR10 are released but SR1-SR5 are operated and for this reason the connection points of the latter relays are located differently in our diagram so that the 'clear' connection is straight through.

The operation of individual relays of the set SR6-SR10 reverses the positive and negative connections to the corresponding send contacts S1-S5. This effect can be expressed as a modulo 2 addition (or exclusive or) of the 5 encipherment channels with the 5 elements of the telegraph code. This is a typical Vernam cipher operation.

The relays SR1-SR5 carry out transpositions of the 5 telegraph elements. The 32 different settings of these five channels produce 32 different transpositions out of the 120 possible.

The combination of Vernam addition with transposition of the signal elements is the principle described in the early patent of Jipp and others. However, in that patent there were 10 binary channels generating transpositions. (This was unnecessary, since 8 channels can easily be made to generate the complete set of 120 transpositions.) In the T52e machine, with 5 transposition channels, the full set of transpositions is not employed.

Figure 6 gives details of the contact timing of the transmit camshaft. A cam on this shaft restores the trip contact and locks the keyboard during the motion of the camshaft. The contacts S1-S5 are allowed to move to their correct positions only when the keyboard has been locked and just in time for the sending of the 5 information-bearing elements by cam contacts F2-F6.

RECEIVE-DECIPHER CIRCUIT

In Figure 7, the received signals pass from right to left so that the SR contacts can be shown in the same relative positions as in Figure 5.

The first negative-going signal on the receive line from P13 operates the receive released magnet AMe through F9 and the camshaft then turns. The five information-bearing elements of the signal are sampled by the short operations of cam contacts F10–F14 of which the timing is shown in Figure 8. These signals are stored as charges on the 5 capacitors shown. The capacitors are in the base of the machine, towards the back.

Near the end of the cycle, 5 simultaneously closing contacts F15–F19 connect the stored charges on the capacitors through the decipherment circuit to the polarised relays R1–R5 shown on the left of the figure. These are bistable relays which hold the value of the received character until the next one is received. The circuits of the relays SR1–SR10 used in this decipher circuit, being identical to the encipher circuit, ensure that a true plaintext character is stored on the polarised relays. The current pulse to set these relays lasts 2–3 ms only.

The timing diagram for the receive camshaft is shown in Figure 8. It includes cam contact F37 which releases the pawl drive mechanism and cam contact F20 which releases the translate/print camshaft, almost one cycle later than the receive camshaft.

Figure 9 shows, for each of the 32 possible settings of the SR1–SR5 relays the way in which the plaintext signal elements 1–5 are transposed to produce the ciphertext elements. Note that the final entry, in which all the relays SR1–SR5 are operated, does not transpose the elements. This is the condition obtained by setting the main control switch to the clear position.

LOGIC OF THE INTERPOSER MAGNETS

Figure 10 shows the circuits of the interposer magnets M1–M10. These magnets are operated by relay logic from the cam contacts A1–A10 together with the KTF switch. Contacts KT1, KT3, KT5 and KT7 belong to the KTF switch and are shown in the circuit in the 'without KTF' position. The circuit also shows the jack points of the KTF unit which we have given the designation E (*).

With KTF off, the magnet operation is dependent only on the contacts A1–A10 and the effective circuit is shown at the top of Figure 11. Also included in the actual circuit of Figure 10 is a cam δ (*) which is on the pawl drive camshaft and releases when the coding wheels are being moved, to protect their A contacts from arcing. There is also a switch contact which releases these circuits when the machine is set for operation in clear. The pawl-drive motor is also switched off in the 'clear' condition. The supply for the M magnets is the +N, -N supply, provided externally.

The timing of the operation of the pawl carriers and of cam δ is shown in Figure 16. All the interposer magnets have their current removed from 90° onwards, but the interposers are effective earlier, when the pawl carriers begin to drop, at about 30-40° . When the current to the M magnets is removed, the force exerted by the pawl carrier extensions on the operative interposers prevents them from detaching and letting the pawl carriers drop.

With the KTF switch on, the operation of magnets M1, M8, M9 and M10 is dependent on element 3 of the coded plaintext character which was last received. This is the character stored on relays R1-R5 from the previous cycle. If there has been a long pause, the character will have been printed but the setting of the relays R1-R5 is not changed until late in the receive cycle so the old setting is effective in the interposer logic circuit. With KTF a plaintext character has no effect on encipherment in the cycle in which it has been sent. In the next cycle it can alter the wheel movements at both sender and receiver. The effect on encipherment and decipherment takes place for the next character, 2 characters later than the one causing the change.

The contact RR3 belongs to an extra relay, the circuit of which can be seen in Figure 21, which slaves the R3 relay. A second contact on RR3 functions in place of the R3 contact in the circuit for translating and printing the stored character.

We remarked earlier that the wiring of the KTF switch had been altered. All 10 contacts have been in use at some time. Some may have been used in the negative supply circuits of M1, M7, M8, M9 and M10 where there are now fixed connections in the KTF box.

Figure 11(a) gives an example of the wheel motion produced by the action of the interposers. In this example, KTF is off and the starting position has all the wheels set at '1'. The M magnet operations are shown, and the consequent output from the A contacts. In all, 25 successive states of the wheels and 24 operations of the pawl-drive mechanism are shown. When an M magnet is operated, the corresponding wheel does not move and, in the next state, the A contact holds its previous position. These wheel positions which are identical with the previous positions are shown by broken lines in the figure. This sequence was verified by experiment on both machines examined, though the numbering difference meant that the Science Museum machine did not start at all ones.

The logic of the M magnets can be verified. For example, M4 operates whenever A2 and A3 are operated, as in phases 1, 7, 8, 9, 10 etc. in the figure. At the right of the figure, the final positions of the wheels in the Munich machine after the 24 operations are listed.

Because of this feedback from the A contacts to the interposer magnets, the motion of the cams is complex and will not repeat for a very long time. A choice of relatively prime numbers for the numbers of steps in the coding wheels is not significant when a complex sequence of movements like this is employed. This 'relatively prime' feature is perhaps left over from an early version in which the stopping of the coding wheel movements by an interposer was not employed.

CIRCUITS OF RELAYS H AND SR

The circuits of these relays are shown in Figures 12 and 13. The logical effect of these circuits is shown in Figures 14 and 15 and the timing of the cams on the pawl drive mechanism which control these operations is shown in Figure 16.

The incoming signals are derived from the B contacts, operated by the coding wheels. In the on state, the outputs from these contacts are from the V+ supply, interrupted by the contact γ to disconnect the B contacts when the wheels are in motion. In the off state, these contacts connect to the V– voltage (when the machine is operating as T52e). These positive or negative signals are applied to the wipers of the key-setting switches, designated A B C D E F G H J and K as shown.

The outputs of the key-setting switches are connected by 10 busbars from the contacts of all the switches. The switches are set to act as a transposition of the 10 channels.

If the setting of the switches is not a permutation, two of the inputs will be connected together by joining to a common busbar and, with appropriate setting of the B contacts, this will connect the V+ to the V- supply. The power supply has been designed to withstand this short circuit, with some overheating, but the relay Ü then releases and prevents the teleprinter operating from its keyboard. To avoid such short circuits causing arcing at the key-setting contacts, the lid of the box containing these switches has a lid contact which breaks the negative supply. For test purposes, the lid contact can be depressed and locked but the switches should never be operated in this condition or arcing on their contacts may damage them. The outputs of the key-setting switches consists of the 10 circuits which we have called X1-X10, which correspond to the switch settings 1, 3, 5, 7, 9, I, II, III, IV, V respectively.

In the T52e operation of the machine, each H relay is connected between two of the X circuits. Since the relay can be operated by a current in either direction, it becomes a modulo 2 sum (exclusive or function) of the two X outputs. The logical expressions thus generated are shown on the left side of Figure 14, for example the first row indicates that H1 = X1 + X2, with modulo 2 addition.

Figure 12 also shows that the X circuits are connected through to the SR relays directly when the machine is operating as T52d. In this case, the H relays do not operate. In the 'clear' condition the relays SR1-SR5 are operated directly and the SR6-10 relays released.

Figure 13 shows that the operation of each SR relay is a modulo 2 sum (exclusive or function) of two of the H relays. These logical relationships are summarised in the right hand side of Figure 14, for example SR1 = H1 + H8, with modulo 2 addition.

Cam contact α on the pawl drive camshaft breaks during the wheel movement, leaving the SR relays held through their make contacts and cam β. Thus the movement of the wheels during the pawl-drive cycle and the release of the H relays when contact γ breaks does not affect the state of the SR relays until late in the cycle when cam β releases and cam α remakes.

The 9 cam contacts μ in the hold circuits and the 9 cam contacts λ in the make circuits are provided to avoid 'sneak circuits' through the H contacts or the hold contacts when the main cams are released.

Combining together the logic of the H coils and the H contacts, the state of each SR relay can be seen to be the modulo 2 sum of 4 of the X channels. These functions are summarised in Figure 15. The functions are such that the modulo 2 sum of all the SR relays is zero, as we would expect, but we find a further linear relationship between the SR relays and a consequent third relationship. These linear relationships are shown on the right hand side of Figure 15.

The logical relations which make each SR relay depend on four X outputs are a new feature in the T52e, not present in the T52d. The purpose of the relations is easily deduced. Even though the coding cam sequences are reasonably random, the outputs on contacts B are not, because the stopping of the wheels makes it more likely that 0 will be followed by 0 than by 1. Such strong statistical properties in the sequences controlling Vernam addition and element transposition are a weakness in the cipher. It is easily seen that the modulo 2 sum of four of those channels has a much better statistical distribution. Evidently the H and SR relays and the logical relations summarised in Figure 15, which were first introduced in the T52e model, increased the strength of the cipher.

Figure 16 shows the timing of the cam contacts on the pawl-drive mechanism and the period when wheel movement takes place. The location of the cam contacts is also shown in this figure.

It is important that the SR relays should not alter their positions before 330° on the transmit camshaft. At this time, the transmit camshaft has completed the sending of its 5th information-bearing element by cam F6. The pawl-drive camshaft is delayed until 5° when its magnet receives current and then, we estimate, until 35° by magnet operation. (The AMs magnet must take 10 mS to operate, if the start pulse is to be of correct length.. The AMC magnet can be assumed at least to take the same time.) This places the break of hold contacts β and μ at 285° + 35° = 320° . Therefore the release of the SR relays must not be faster than 3.3 mS, which is reasonable, but the margins are close.

It is possible that contact β is out of adjustment, since it does not overlap contact α. In slow operation of the camshaft, all the SR relays release. The 'on' period of cam β could be lengthened at both ends by an adjustment. Figure 16 shows the measured values on the Science Museum machine. The timings of Figures 6 and 8, except for cam F37, come from T36 teleprinter documentation.

TRANSLATE AND PRINT CIRCUITS

The circuit used for translating and printing is, with one small change, the same as for the T36 teleprinter. The circuit is shown in Figure 17 and its operation depends on the timing of the translation cams shown in Figure 18.

The purpose of this circuit is to operate the printer magnet DM at the correct instant, depending on the state of the relays R1-R5. In the T52e circuit, a contact of the slave relay RR3 takes the place of R3 in this translate circuit.

When the position of the R contacts and the state of the F cam contacts coincides, a circuit is produced from the negative supply at P11 through to the print magnet. The print current is provided by the charge stored in the capacitor C10, which is re-charged through the cam F27 at the end of the cycle. Parallel circuits are provided for the letters/figures shift magnets Bu and Zi and the bell relay KLR. The magnet VUM also operates in these cases to stop the paper feed. The cam F39 is fitted but the 'who are you' unit is absent.

CONTROL OF THE RELEASE MAGNETS

Figure 19 summarises the control of the release magnets and shows the circuit of AR and other relays in the external unit.

The keyboard trip contact is operated by depressing any key that is active and, if the short-circuit detection relay Ü is operated, AR and the external relay U will operate. When AR is operated, the transmit release magnet is operated and, through the transmit circuit, ER and the receive circuit, the receive release magnet is operated soon afterwards. The operation of the receive camshaft releases the pawl-drive by F37 and magnet AMC and the translate print shaft by F20 and magnet AMü.

The need for the relay ER, which reproduces the telegraph signal for the receive circuits, can now be understood. In the receive-decipher circuits of Figure 7 this signal charges the five capacitors which store the character for printing. It also operates the release magnet AMe. These impose loads on the signal which would distort it if the signal from the line was used directly. In particular, the capacitors demand large initial currents, limited only by the resistors which generate the Ov signal of the N supply, see Figure 20. This distortion would affect incoming signals from the line and outgoing signals, which are also received for local printing. The ER relay ensures that the signal entering the receive circuit always comes from a local, low impedance source, the N supply.

At the same time that ER first operates, during the start element of a transmitted or received character, relay D in the external unit operates and holds. Relay V also operates and shortly afterwards the thermal relay operates. When N has ceased to operate for a sufficient time, the thermal relay will release and thus release relay V. This circuit activates the motors on the first occasion that a character is received and keeps them running for a short while after characters have ceased to arrive.

DIFFERENCES BETWEEN THE TWO T52 MACHINES

There are some minor differences between the Munich and Science Museum machines such as the absence of the reverse motion pawls in the Science Museum machine and a few differences in the electrical noise suppression arrangements.

Functionally there is one significant difference between these two machines. Although the patterns of the 10 coding cams are the same, they are differently placed relative to the cam numbering. Since the wheel settings are determined by the numbering of the cam wheels, these two machines could not be used to communicate with one another except by converting the initial wheel settings from one to the other.

The differences in numbering are in each case close to one-third of a wheel revolution which suggests that they were produced by assembling the cam mechanism relative to the numbering wheel with the three connecting bolts going through different holes.

To produce the equivalent of the Munich machine wheels set all to ones, the Science Museum machine wheels would have to be set to the values:-

32, 18, 1, 21, 43, 44, 67, 23, 24, 49

It is odd that wheel 7 numbering (underlined) is displaced by just one step when it could easily have been adjusted for coincidence.

An important compatability feature for the coding wheels is the set of displacements between the A and B sets of contacts shown on Figure 3 by the black squares. These are identical in the Munich and Science Museum machines.

The Science Museum machine has an unused gear wheel fixed to the right hand end of the shaft which holds the coding wheels. A flat on this shaft, engaging with a bolt prevents it moving. Small bronze cams with one notch in each cam are fitted adjacent to the left side of each indicator wheel. When the fixing bolt was removed, these cams were found to rotate with the unused gear wheel though stiffly. It is therefore possible that they formed part of an earlier mechanism in which the central shaft, instead of being fixed, rotated in the three bearings provided. This would account for the oil holes in two of the bearings which now have no purpose. In the third bearing the oil hole has been replaced by the fixing bolt.

There is a set of radial slots on the inside of each indicator wheel in the Science Museum machine but not the Munich one. Having one slot per step of the wheel suggests that this is not just an accident of manufacture. It is possible that the gear wheel, cams and slots were part of an earlier wheel drive mechanism.

DEVELOPMENT OF THE T52 SERIES OF MACHINES

There are some clues to the way the T52 machine developed between 1934 and 1944 but at present, insufficient information to give definite conclusions. We know about the T52d because the machines examined can work in this fashion.

The 1930 patent described the basic encipherment principle, consisting of Vernam addition followed by transposition of elements. The circuits shown were based on the T36 teleprinter. The transposition scheme in the patent used 10 sets of contacts instead of the 5 sets (SR1-SR5) shown in Figures 5 and 7. Using 10 sets, the patent shows two alternative transposer layouts. The method of obtaining the pseudo-random sequences for operating the 15 sets of contacts (5 Vernam and 10 transposer) is not clearly stated, but depends on cam wheels.

The use of 5 transposing relays in the T52e machine can be traced back to the T52d, where relays SR1-SR5 are operated directly by outputs 1, 3, 5, 7, 9 of the key-setting switchboard (Figure 12). The strange notation 1, 3, 5, 7, 9, I, II, III, IV, V is then probably explained. Roman numbers were used for the Vernam channels and the ten transposer channels were originally numbered 1-10, then the even-numbered transposer units were dropped at some stage. The two transposer layouts in the patent do not, unfortunately, give confirmation since they cannot be related to the T52d/e layout by deleting transposer units.

In Cryptologia, Volume 3, No. 4, October 1979, page 210 a photograph taken by David Kahn shows a T52 machine as displayed in Bonn at the conference on World War II cryptology, in November 1978. It is not known which of the models a-d this was. This machine has no internal power supply and no H and SR relays. The KTF switch is there, in a different place. The key-setting rotary switches were absent and in their place, under a locked black cover, was a set of plugs, inserted into a set of sockets. The plugs and sockets can be seen in a photograph provided by Dr E Hüttenhain, showing a machine of the same type as the 'Bonn' machine though not an identical one. The front two plugs are seen to be labelled E and K in this photograph.

A striking feature of this early T52 model is the presence of two sets of 'B' contacts and four cams. We can guess at the presence of two sets of 'A' contacts, probably running on cams 2 and 4 (counting from the ratchet side). Mounting slots for such extra contacts are present in the T52e.

The Bonn machine photograph seems to show cams 1 and 3 with the same pattern, and cams 2 and 4 also identical, but it is difficult to be sure.

In the absence of the SR relays, the coding wheel cams had to operate 4 changeover contacts. How these were disposed on the 4 cams and how wheel movement was controlled cannot be deduced.

Unfortunately, the information about the T52 from two prisoneers of war, reproduced in the Cryptologia article is so full of errors that it cannot be used to improve our knowledge of T52 development.

ADJUSTMENT AND MAINTENANCE

Most aspects of maintenance, such as the lubrication and adjustment of contacts, are obvious. Possibly the plastic cam surfaces should be lightly greased to reduce wear.

The T36 gearbox contains a helical gear and this needs lubrication, though very little lubricant has been used on it. It can be inspected and greased by removing the lid of the gearbox. The speed regulator rotor is first removed by slackening one bolt. The brush assembly should be left attached to the lid, because its fixing screws also retain the top bearing. One screw on the lid covers an oil hole. When replacing the speed regulator rotor, the brushes must be retracted. Only one or two drops of oil or a small direct application of grease to the gears is necessary.

The speed regulators can be adjusted with a stroboscope. The white patches provided for this purpose pass by at 250 per second on both regulators. To adjust speed while the motors are running, hold still the larger knurled ring then adjust the smaller ring. The speed is not altered by holding these parts still. There is less ambiguity of measurement if the shaft speed is checked, and this is 2500 rpm for the T36 motor and 1500 rpm for the pawl-drive motor. The gear ratios from motors to clutches are 5 : 1 for the T36 mechanism and 3 : 1 for the pawl-drive mechanism, so both camshafts operate at 500 rpm. One sixth of a revolution is the time of one telegraph element, which is 20 mS.

TEST CIRCUIT FOR OPERATION OF THE T52e MACHINE

In the absence of the line-connecting unit, it is possible to test the operation of the T52e machine with one external power supply taking the place of the T and N supplies. The connections to the plug we have called P are shown in Figure 22.

The use of a 240V, 50 Hz, AC supply seems to be harmless because the speed regulators can handle the small increase of voltage. The DC output of the rectifier across the reservoir capacitor should be approximately 120V but is not critical. The resistor in the supply to P12, simulating the coil resistance of relay U of the line-connecting unit, is essential to avoid a short-circuit of the supply.

By connecting P9 to P13 and using a common supply in place of the T and N supplies, the need for relay ER is avoided. This would not be satisfactory for transmission over a pair of lines but it enables local printing from the keyboard to operate correctly.

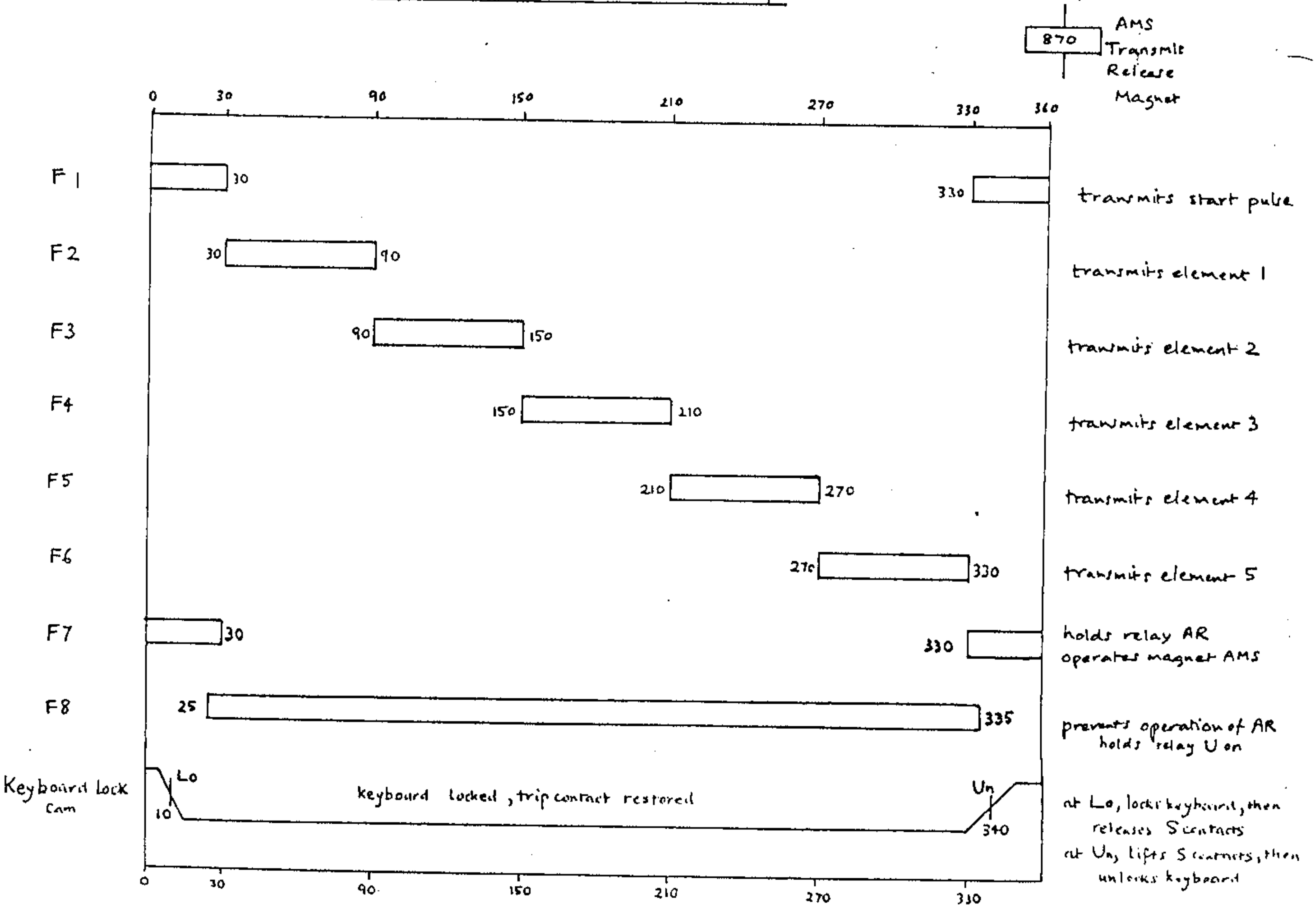
The motors operate whenever the supply is connected, in the absence of the control relays in the line-connecting unit.

ACKNOWLEDGEMENTS

Dr Goetzeler of the Werner von Siemens Institute for the History of the House of Siemens in Munich provided the facilities for examining the T52e machine in their collection. Dr Schoen and Mr Bayer of that institute also gave useful help. Dr Pramm of the Norsk Technisk Museum in Oslo allowed the examination of their machine. Dr Strimpel of the Science Museum provided the opportunity to examine their machine at length, enabling much of the detail to be filled in.

Prof. Randell of Newcastle University provided notes of a conversation with Mr Fricke on the manufacture of these machines and Dr Hüttenhain of Bonn provided useful information about the T52 and a photograph of an early model. The help of all these people is gratefully acknowledged.

Figure 6 Timing of cams on the transmit camshaft



Encipher — Transmit

Figure 5

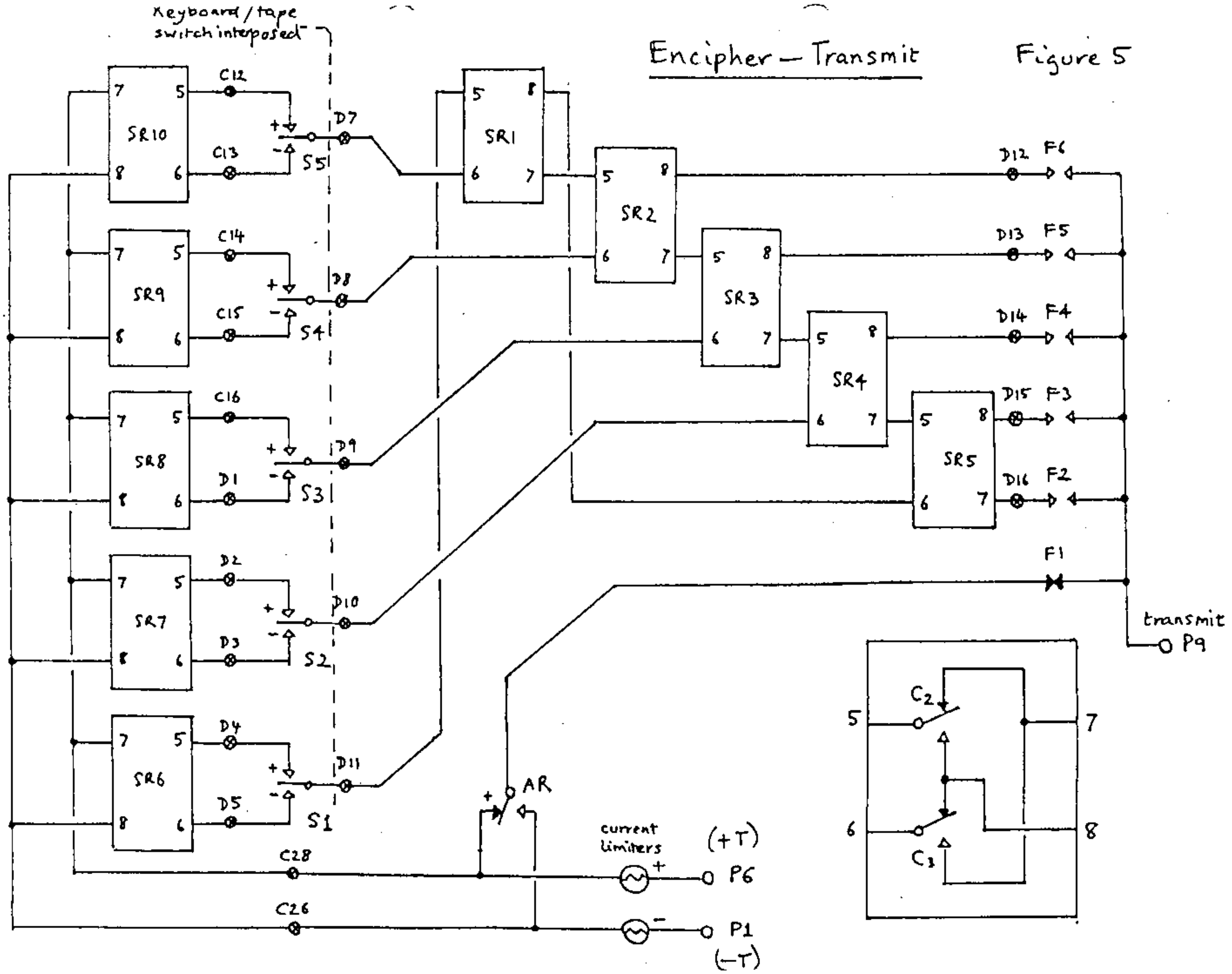
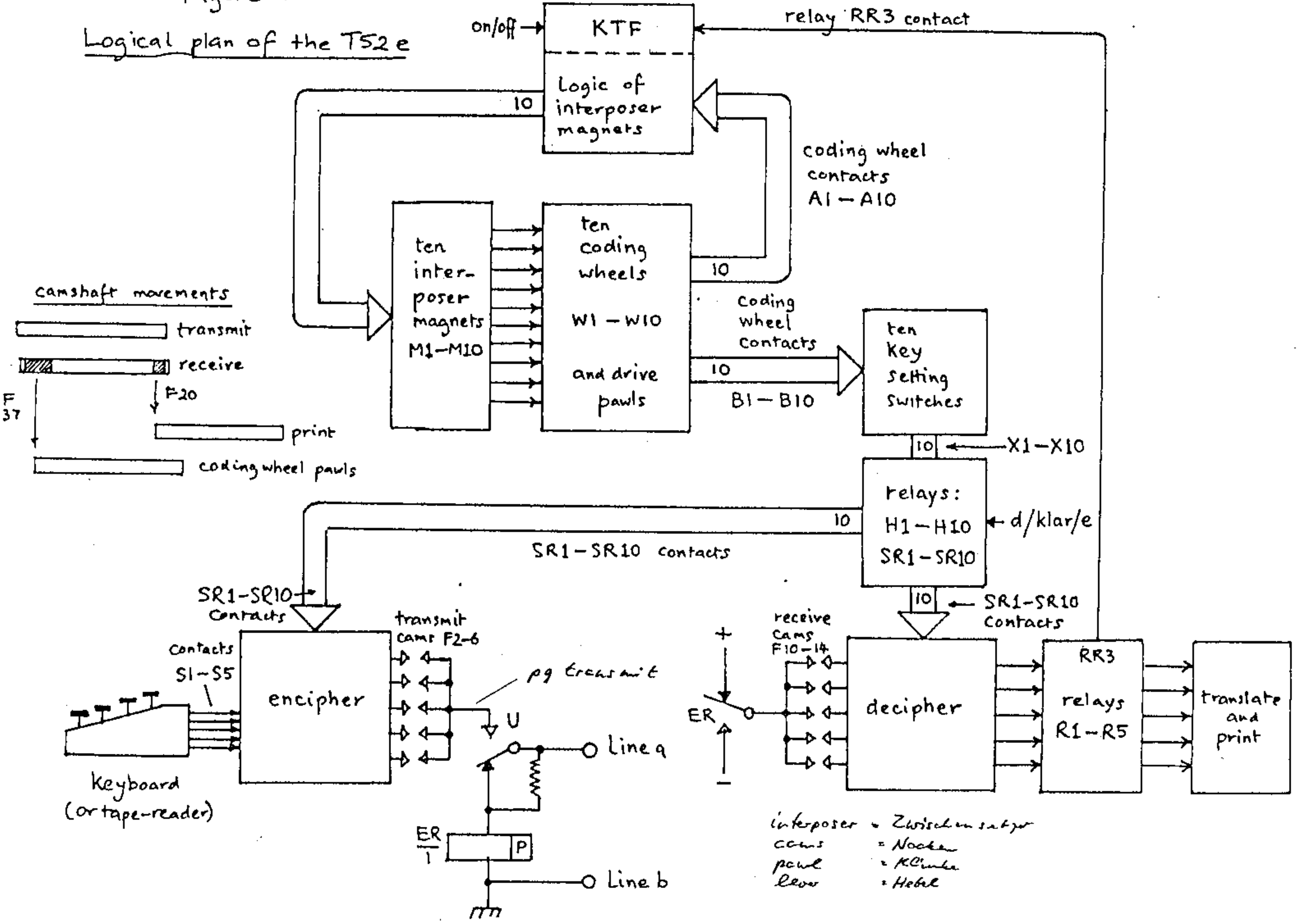


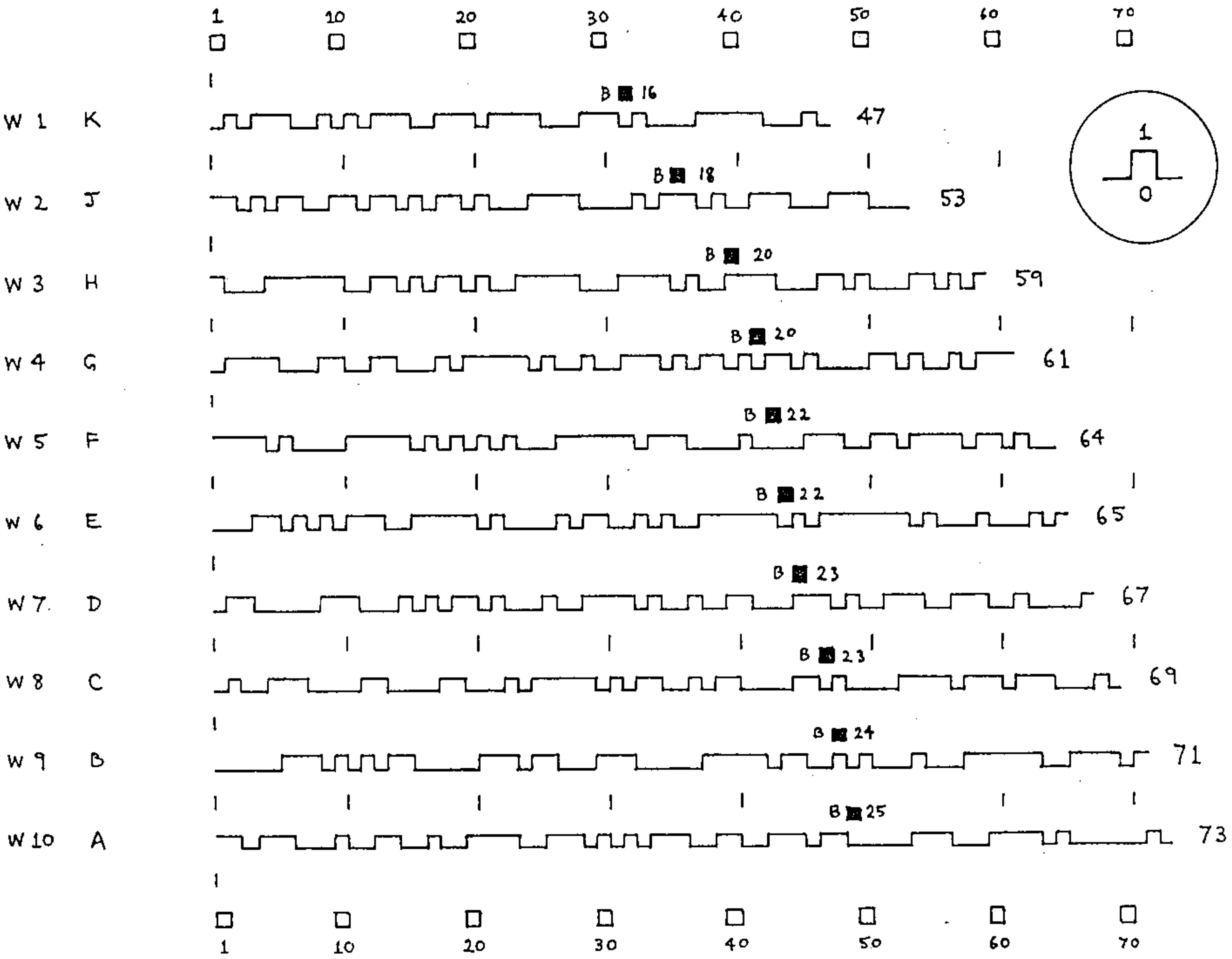
Figure 4

Logical plan of the T52e



interposer	= Zwischensatzer
cams	= Nocken
pawl	= Klinke
lever	= Hebel

Figure Coding cam outputs



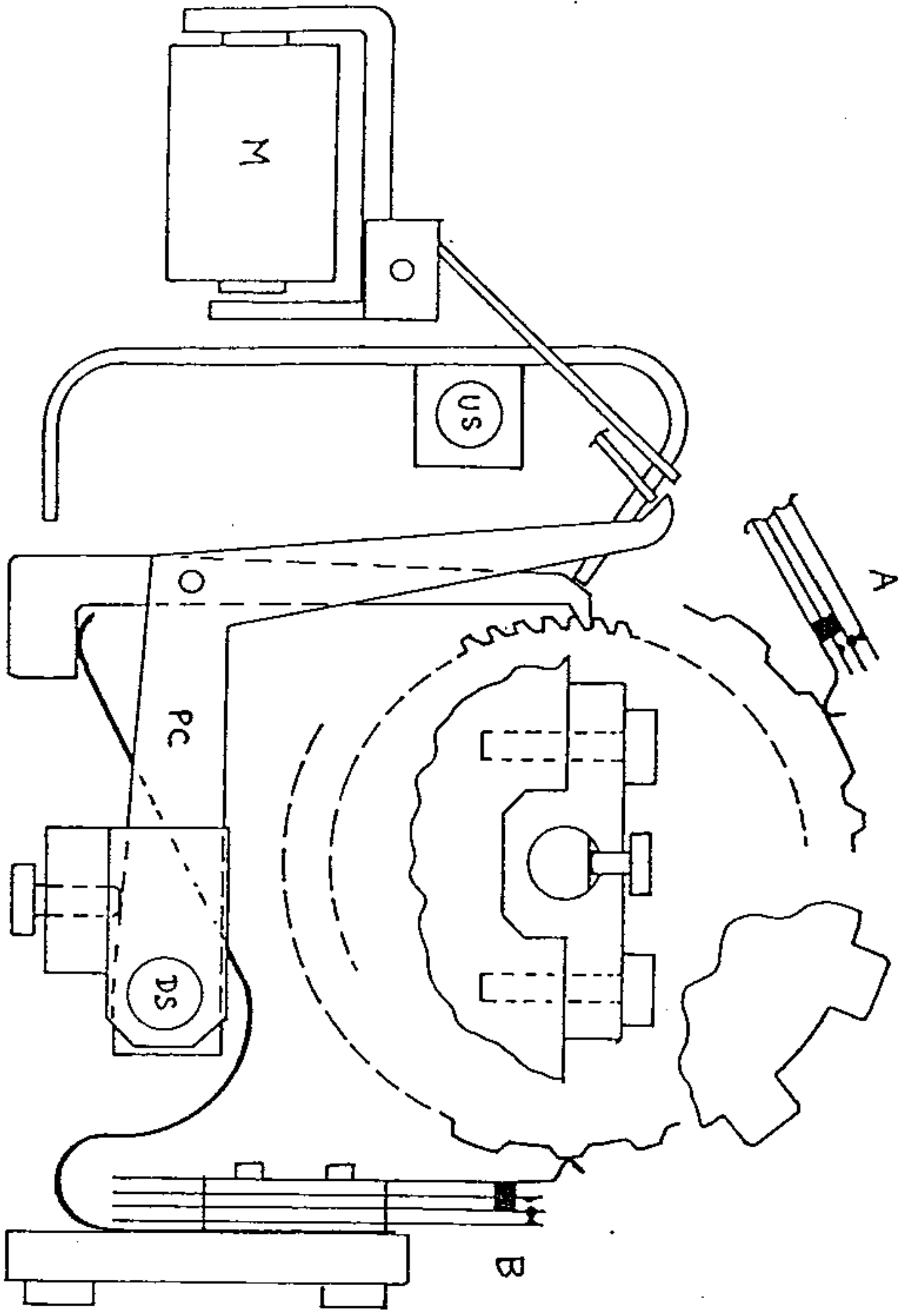


Figure 2
Interposer mechanism, cam-wheels and contacts

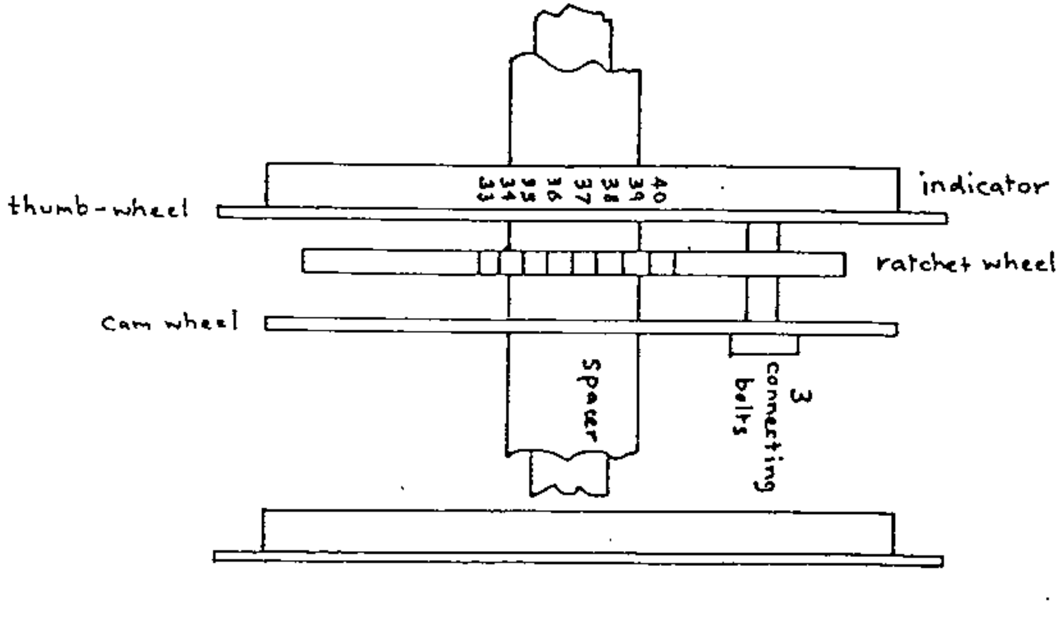
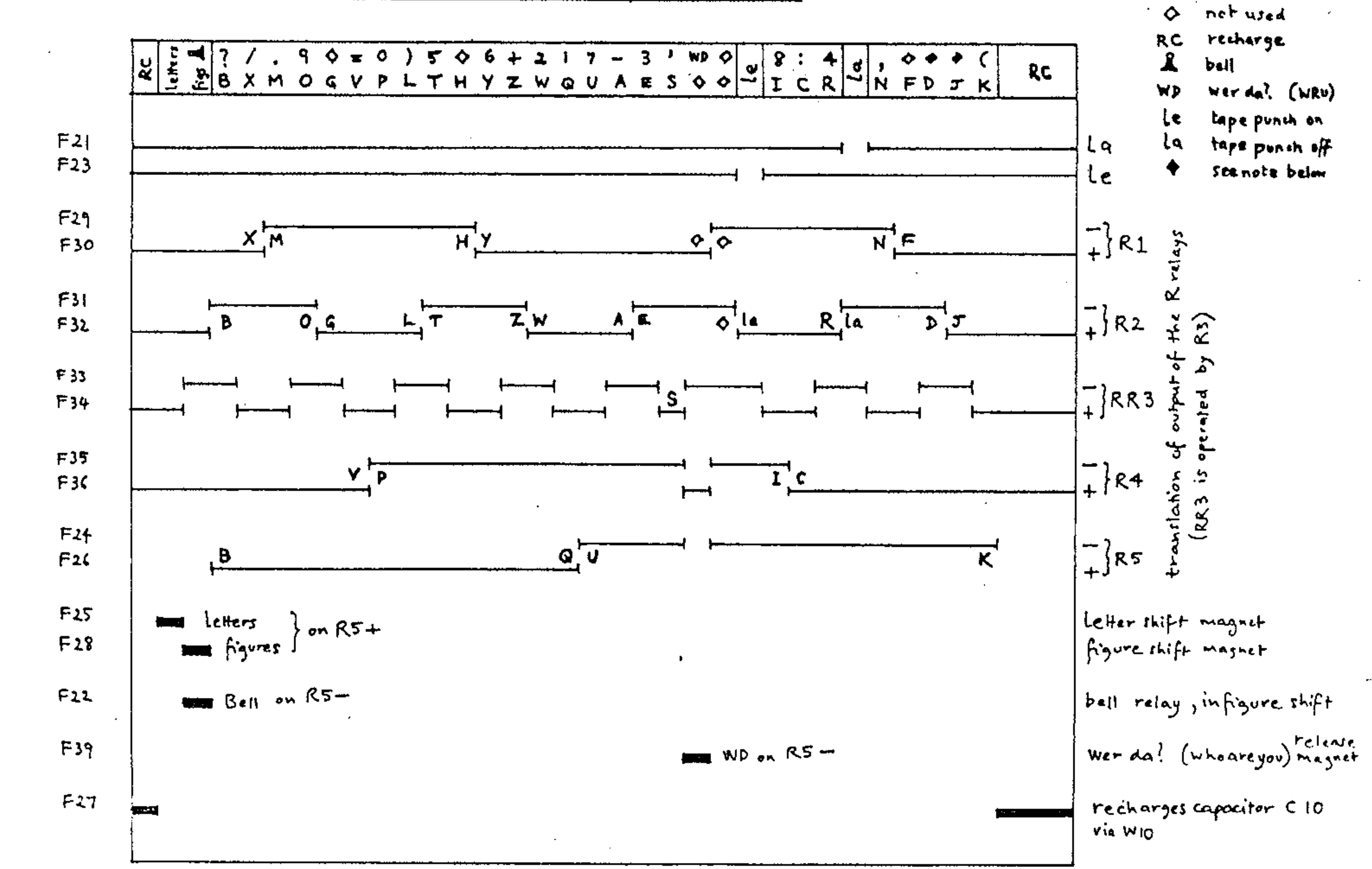


Figure 18 Timing of cams on the translate/print camshaft



RC
letters
fig 🔔
? / . 9 ◇ = 0) 5 ◇ 6 + 2 1 7 – 3 ' WD ◇
B X M O G V P L T H Y Z W Q U A E S ◇ ◇
le
8 : 4
I C R
la
, ◇ ◆ ◆ (
N F D J K
RC
F21
F23
La
Le
F29
F30
X M H Y ◇ ◇ N F
R1
F31
F32
B O G L T Z W A E ◇ la R la D J
R2
F33
F34
S
RR3
F35
F36
V P I C
R4
F24
F26
B Q U K
R5
translation of output of the R relays (RR3 is operated by R3)
F25
F28
letters
figures
on R5+
letter shift magnet
figure shift magnet
F22
Bell on R5–
bell relay, in figure shift
F39
WD on R5 –
Wer da? (whoareyou) release magnet
F27
recharges capacitor C 10 via W10

◇	not used
RC	recharge
🔔	bell
WD	wer da? (WRU)
le	tape punch on
la	tape punch off
◆	see note below

◆ { WD is the 'figures' equivalent of D } these discharge C10
{ Bell is the 'figures' equivalent of J } before it can print D or J

Figure 16 Timing of cams on the pawl-drive mechanism

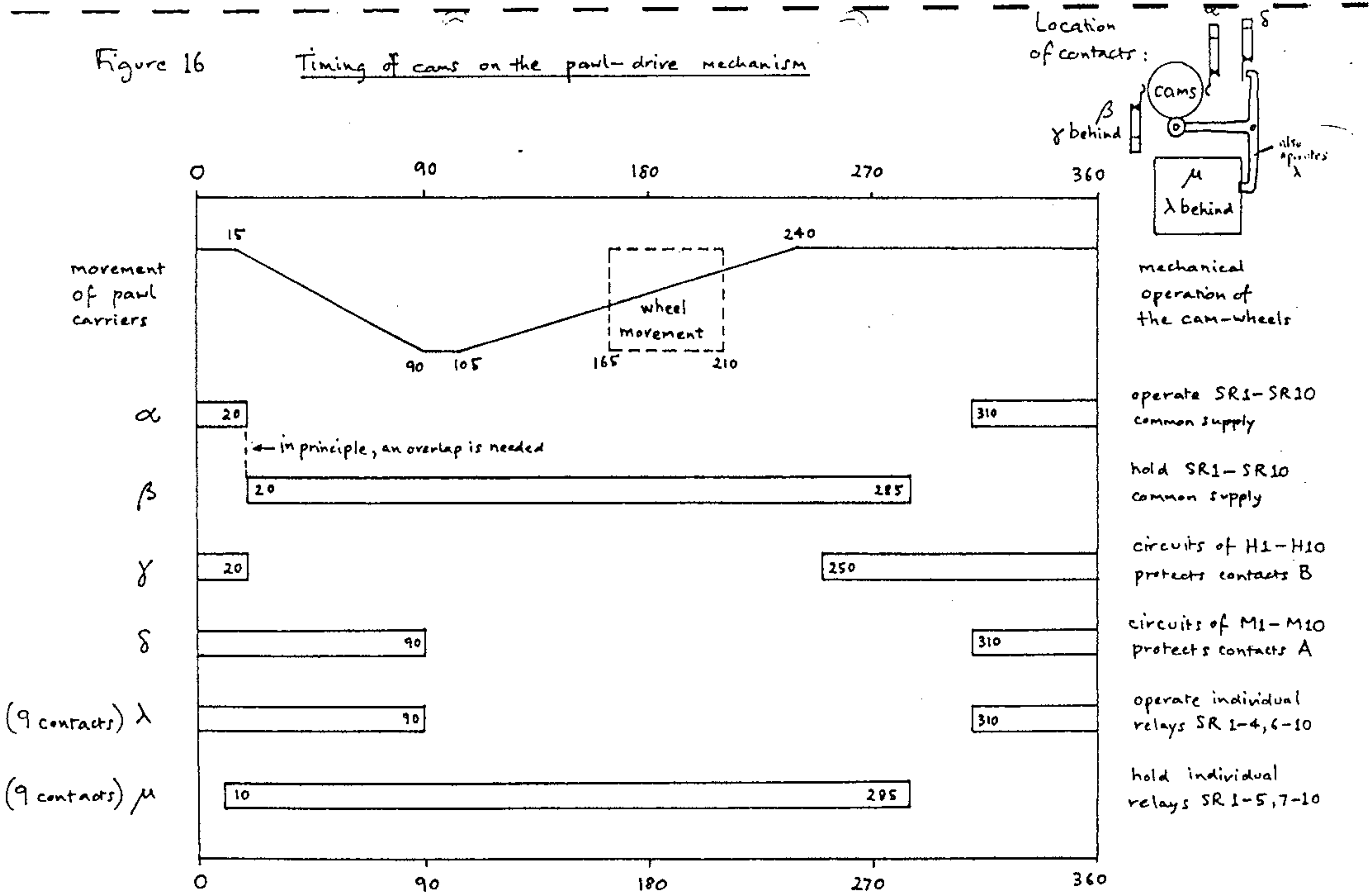


Figure 15 Key-setting switch positions

	1	3	5	7	9	I	II	III	IV	V
	X1	X2	X3	X4	X5	X6	X7	X8	X9	X10
SR1	X	X						X		X
SR2						X	X	X	X	
SR3			X	X				X		X
SR4	X	X	X				X			
SR5	X			X	X		X			
SR6			X	X			X		X	
SR7		X	X		X					X
SR8	X	X				X			X	
SR9					X	X		X		X
SR10				X	X	X			X	

SR – encoding relays

Logical relations X → SR

Two independent linear relationships between SR1-10

X		X
	X	X
	X	X
X		X
	X	X
X		X
	X	X
	X	X
X		X
X		X

↑

$$\sum_{i=1}^{10} SR_i = 0$$

Figure 14 Logical relations X → H → SR

key-setting switch positions

	1	3	5	7	9	I	II	III	IV	V
	X1	X2	X3	X4	X5	X6	X7	X8	X9	X10
H1	X	X								
H2		X	X							
H3			X	X						
H4				X	X					
H5					X					X
H6						X		X		
H7							X		X	
H8								X		X
H9						X			X	
H10	X						X			

H-transfer relays

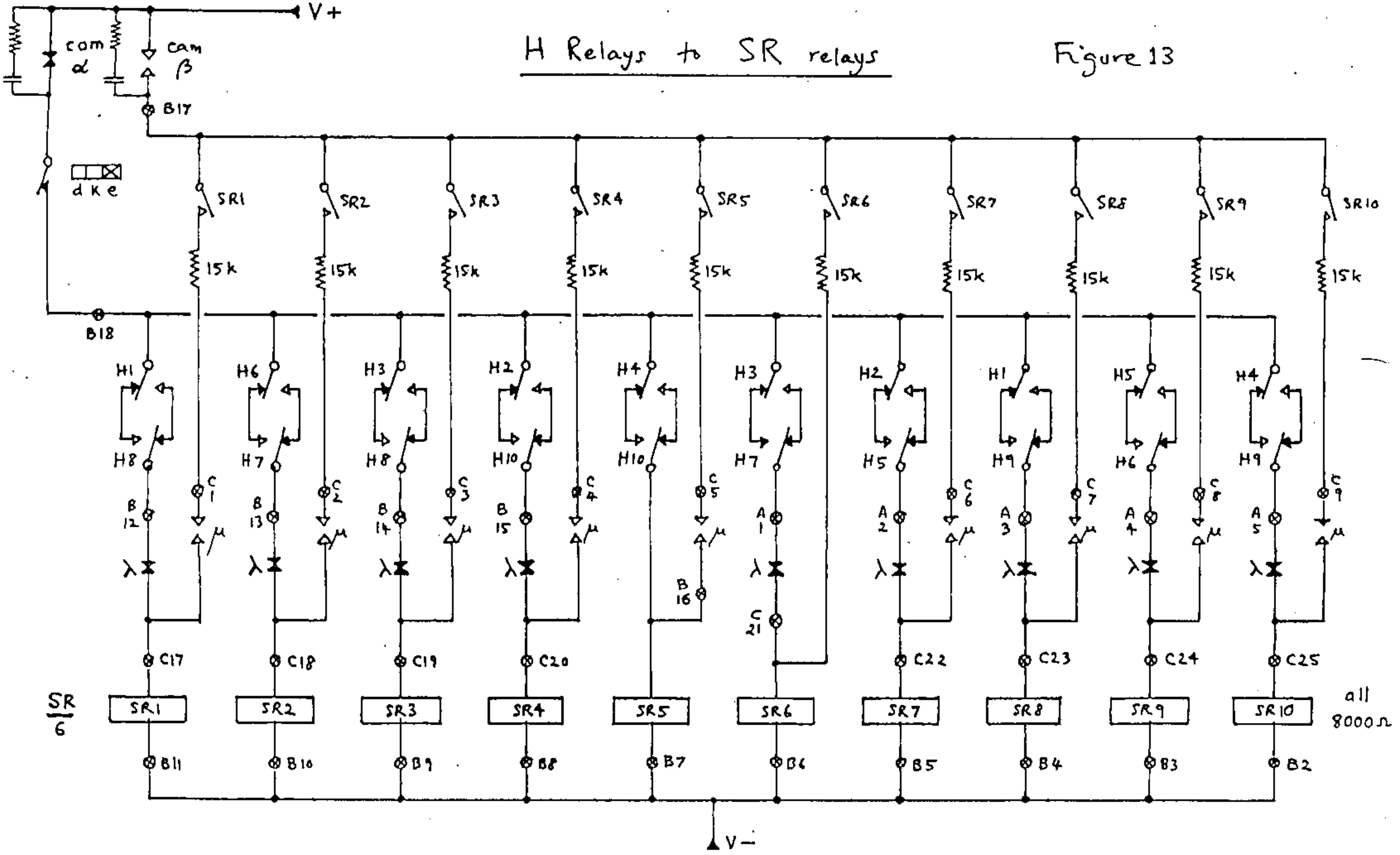
H - transfer relays

	H1	H2	H3	H4	H5	H6	H7	H8	H9	H10
SR1	X							X		
SR2						X	X			
SR3			X					X		
SR4		X								X
SR5				X						X
SR6			X				X			
SR7		X			X					
SR8	X								X	
SR9					X	X				
SR10				X					X	

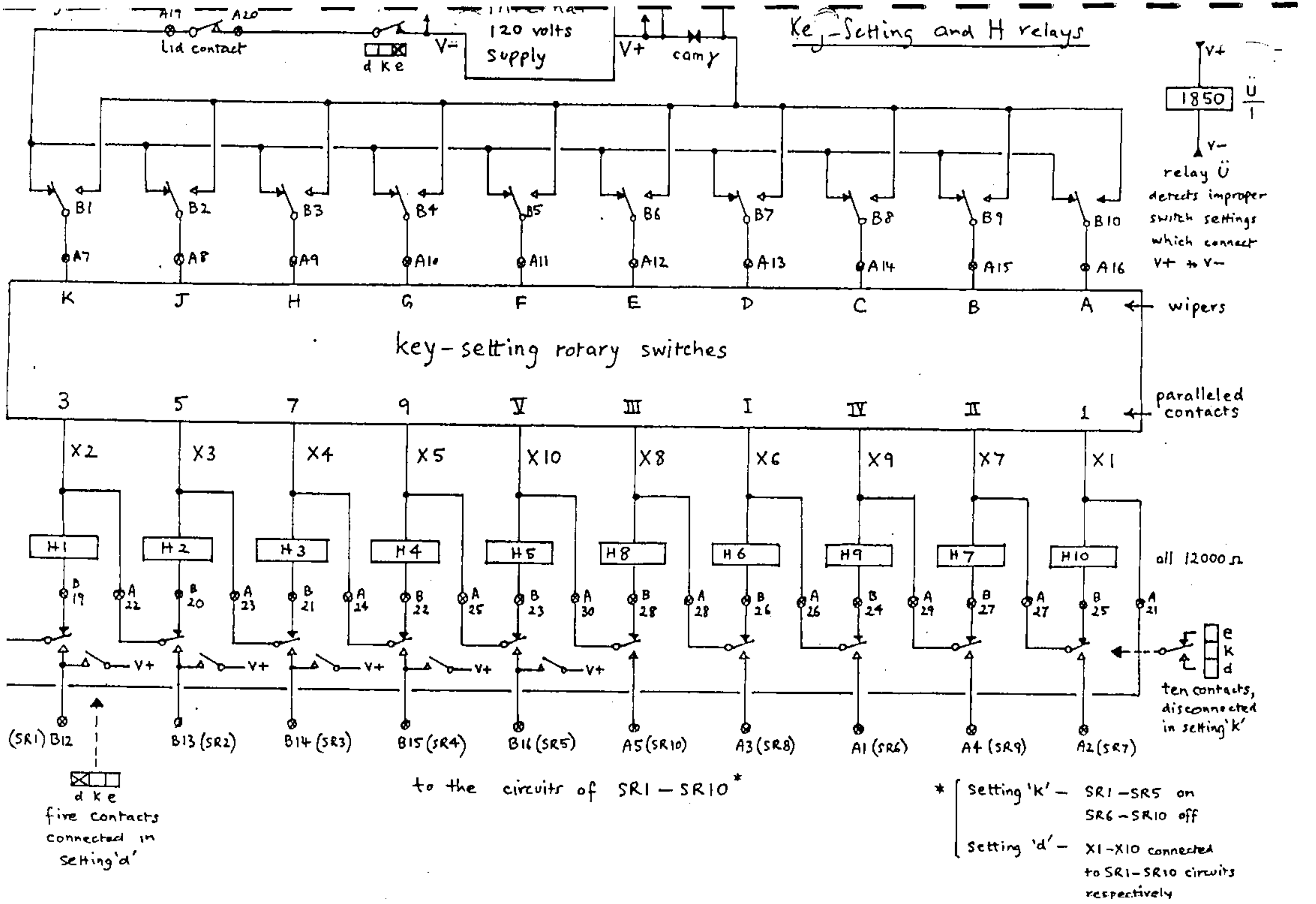
SR - encoding relays

H Relays to SR relays

Figure 13



Key-Setting and H relays



* Setting 'k' — SR1 — SR5 on
SR6 — SR10 off

Setting 'd' — X1 - X10 connected
to SR1 - SR10 circuits
respectively

Figure 11(a) Example of wheel movement, without KTF, starting all ones

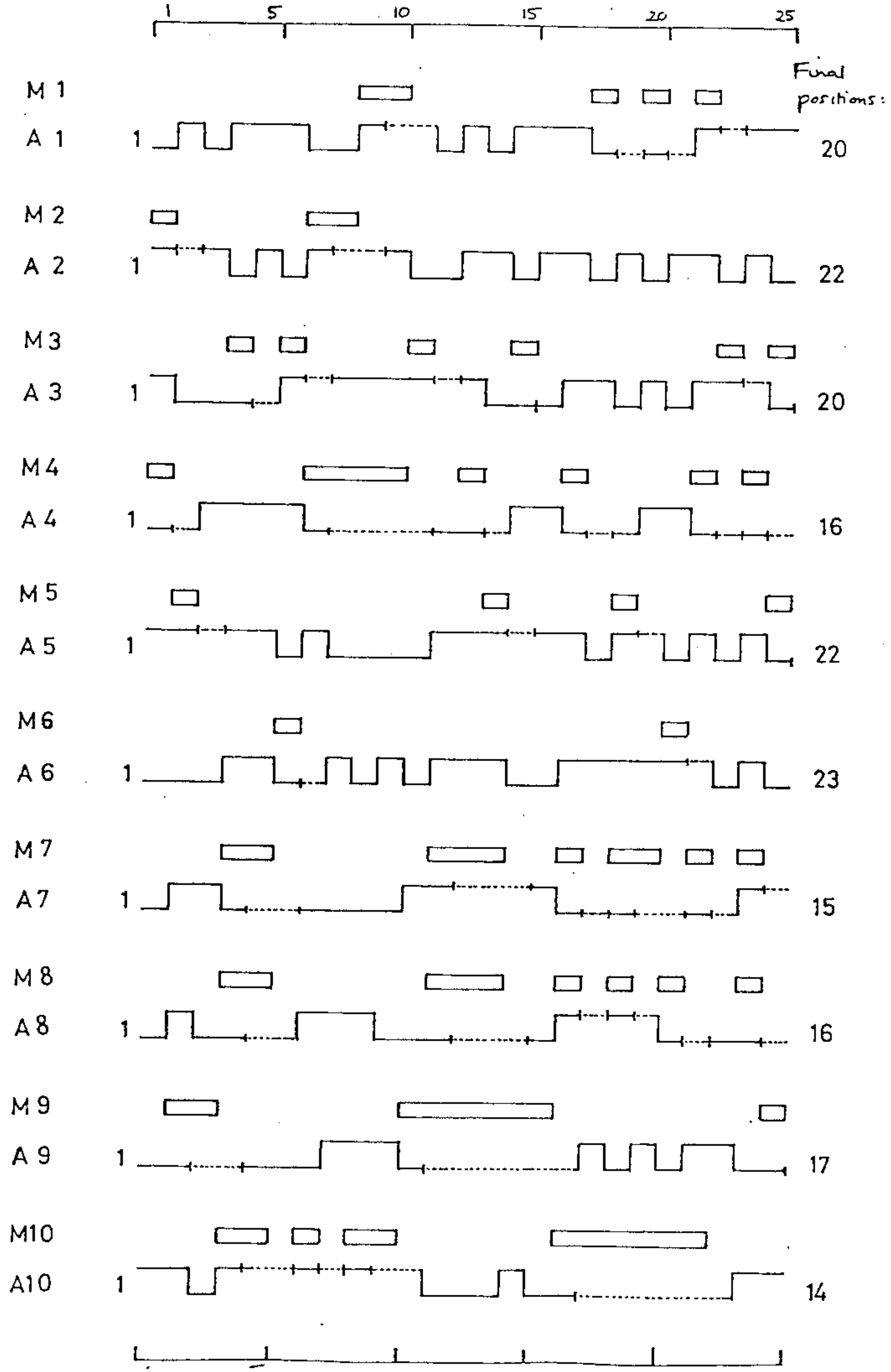
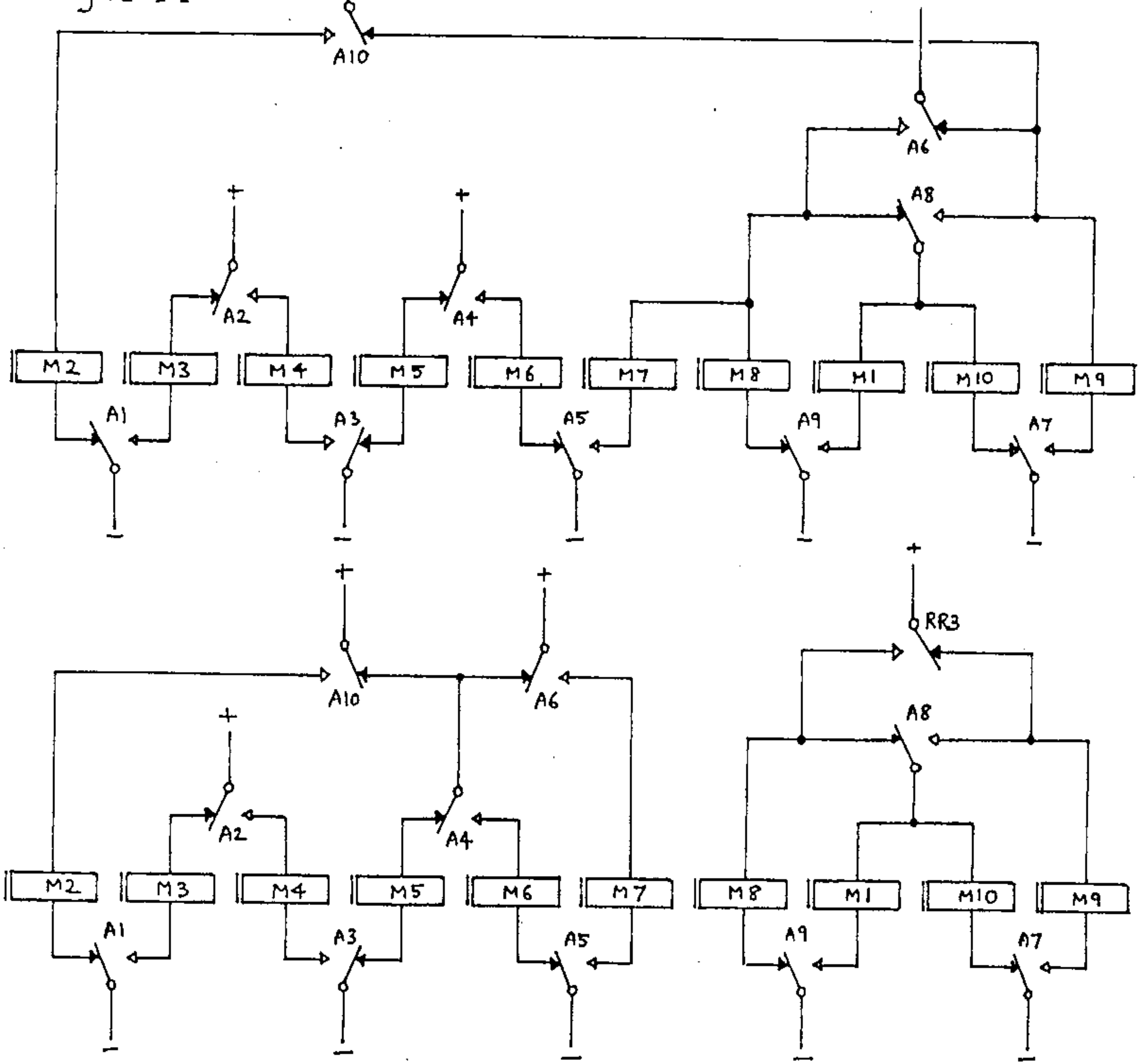


Figure 11



Without

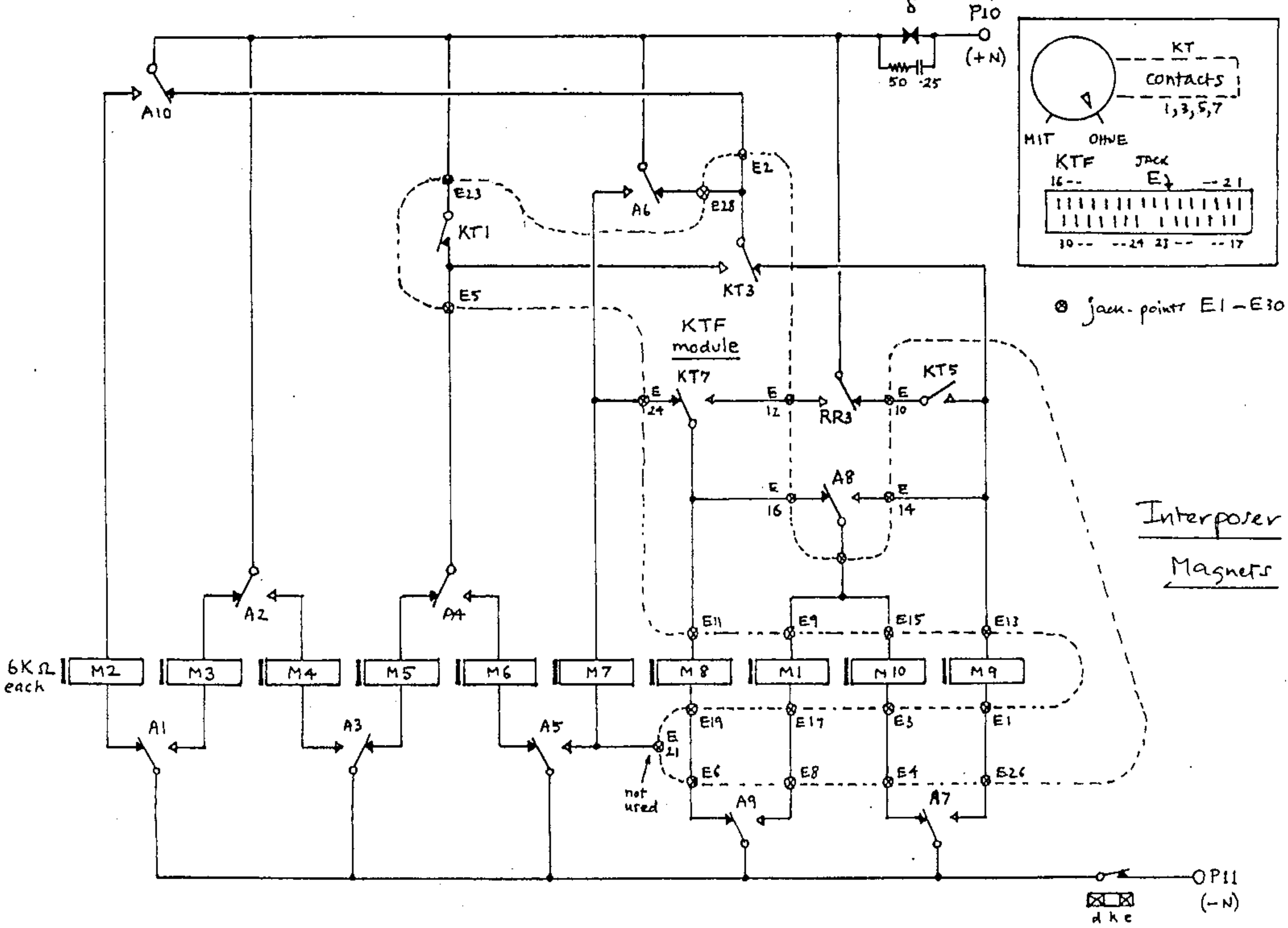
KTF

With

KTF

Schematic of interposer Logic

Figure 10



Interposer

Magnets

Figure 9

signal elements

SR1	SR2	SR3	SR4	SR5	1	2	3	4	5
0	0	0	0	0	1	3	4	5	2
1	0	0	0	0	2	3	4	5	1
0	1	0	0	0	5	3	4	1	2
1	1	0	0	0	2	3	4	1	5
0	0	1	0	0	4	3	1	5	2
1	0	1	0	0	2	3	1	5	4
0	1	1	0	0	5	3	1	4	2
1	1	1	0	0	2	3	1	4	5
0	0	0	1	0	3	1	4	5	2
1	0	0	1	0	2	1	4	5	3
0	1	0	1	0	5	1	4	3	2
1	1	0	1	0	2	1	4	3	5
0	0	1	1	0	4	1	3	5	2
1	0	1	1	0	2	1	3	5	4
0	1	1	1	0	5	1	3	4	2
1	1	1	1	0	2	1	3	4	5

plain

cipher ↓

permutation of signal elements by SR1 – SR5

Transposition:

signal elements

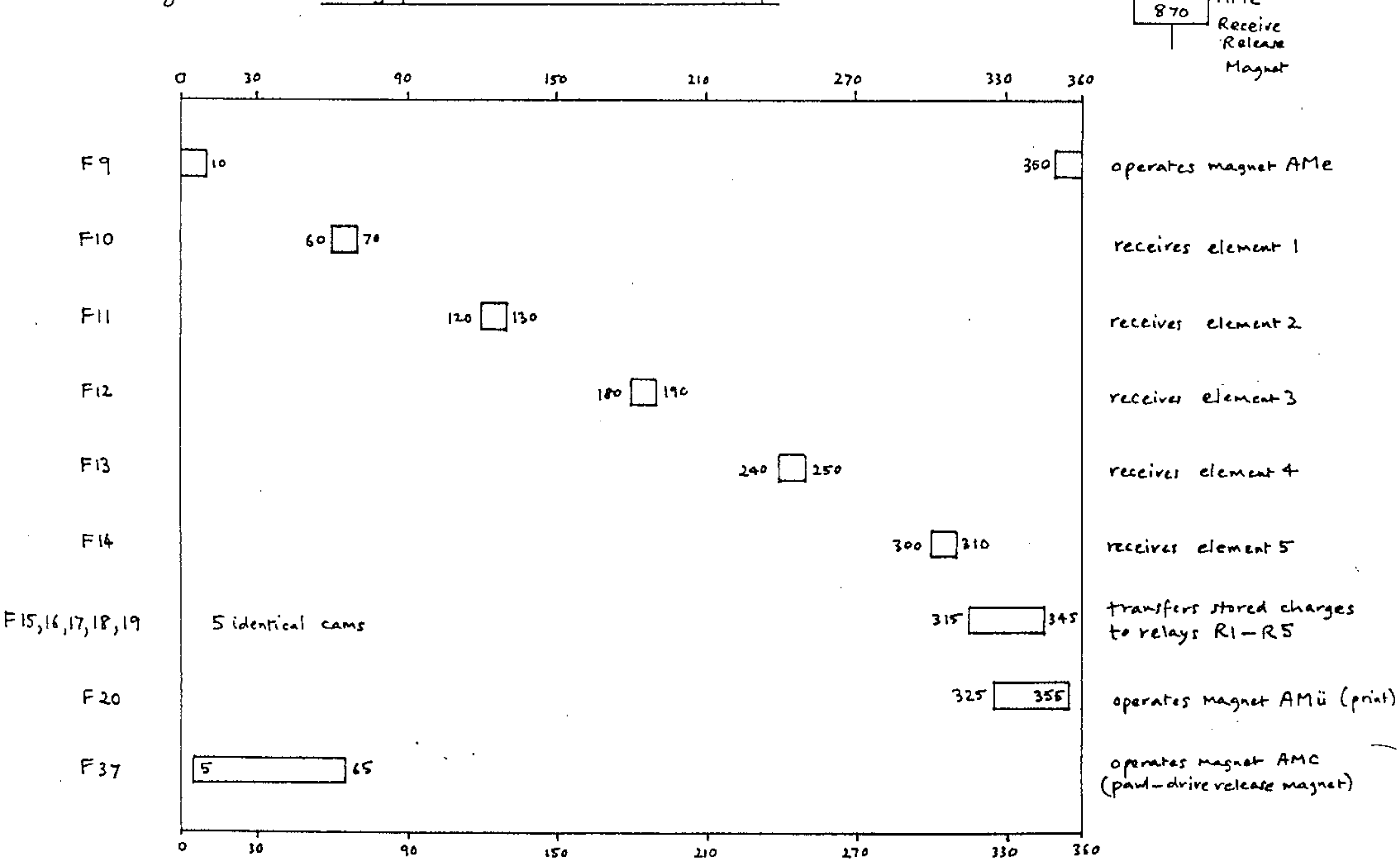
SR1	SR2	SR3	SR4	SR5	1	2	3	4	5
0	0	0	0	1	2	3	4	5	1
1	0	0	0	1	1	3	4	5	2
0	1	0	0	1	5	3	4	2	1
1	1	0	0	1	1	3	4	2	5
0	0	1	0	1	4	3	2	5	1
1	0	1	0	1	1	3	2	5	4
0	1	1	0	1	5	3	2	4	1
1	1	1	0	1	1	3	2	4	5
0	0	0	1	1	3	2	4	5	1
1	0	0	1	1	1	2	4	5	3
0	1	0	1	1	5	2	4	3	1
1	1	0	1	1	1	2	4	3	5
0	0	1	1	1	4	2	3	5	1
1	0	1	1	1	1	2	3	5	4
0	1	1	1	1	5	2	3	4	1
1	1	1	1	1	1	2	3	4	5

plain

cipher ↓

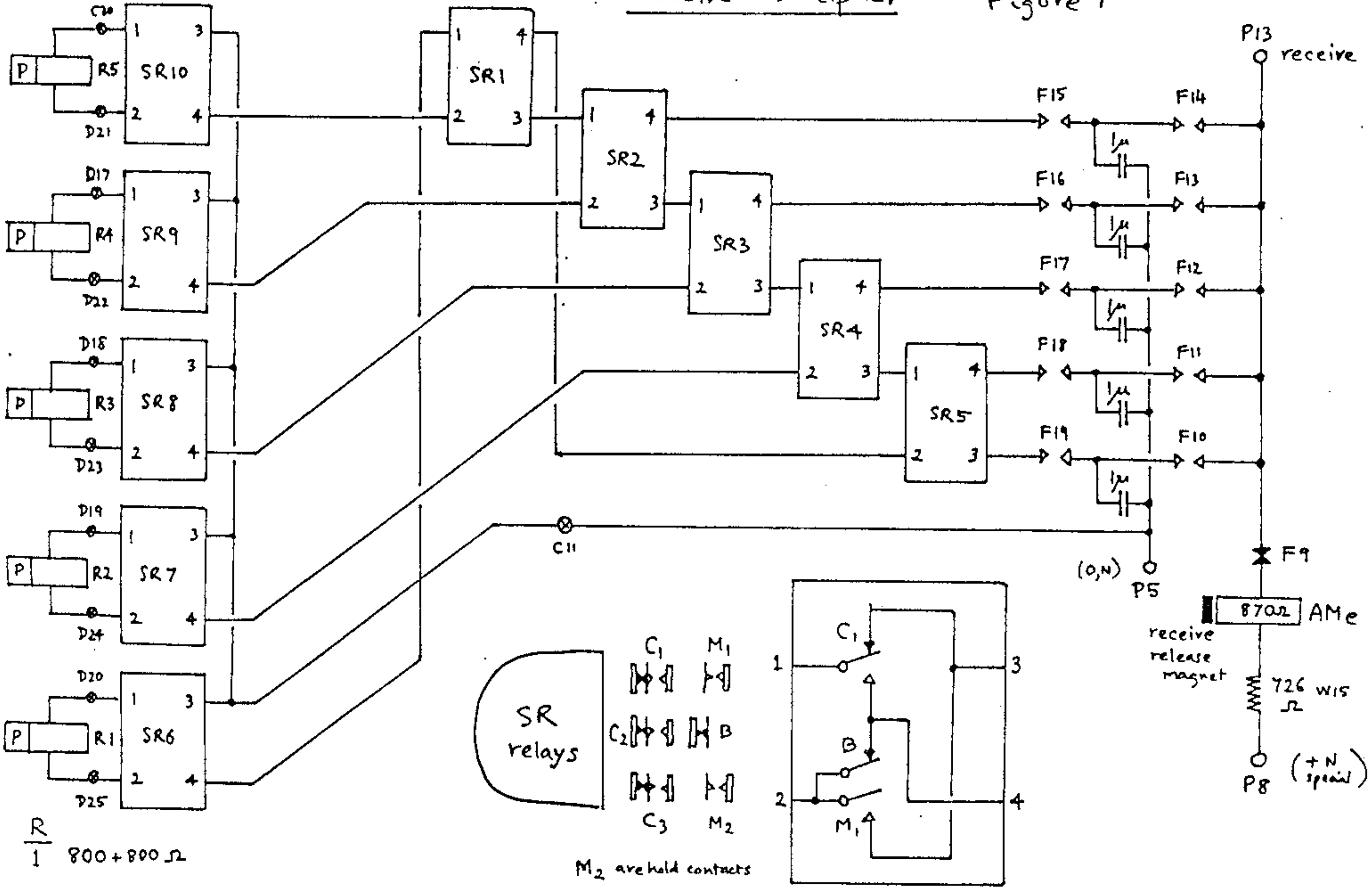
← clear

Figure 8 Timing of cams on the receive camshaft



Receive – Decipher

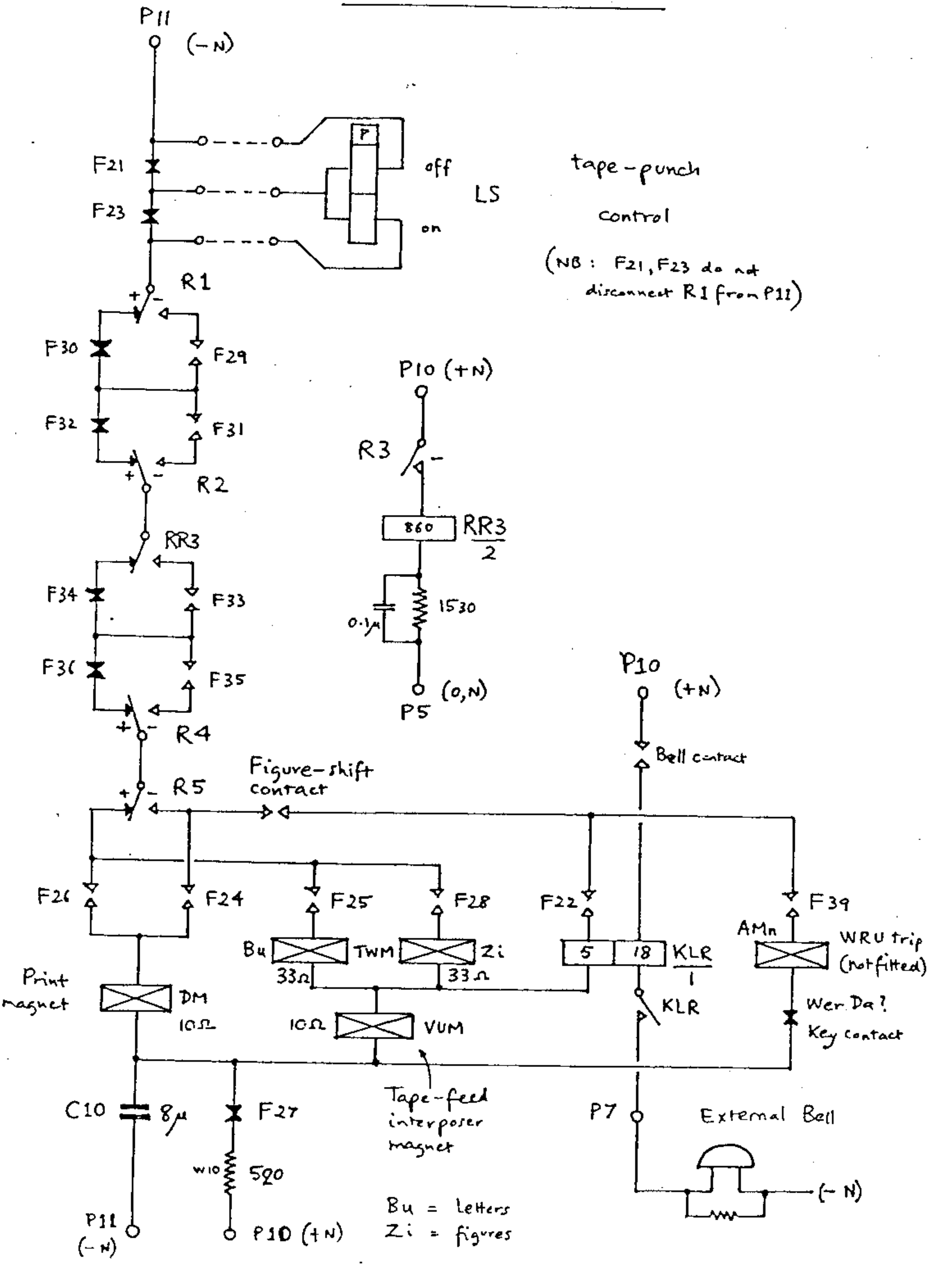
Figure 7



R/1 800+800 Ω

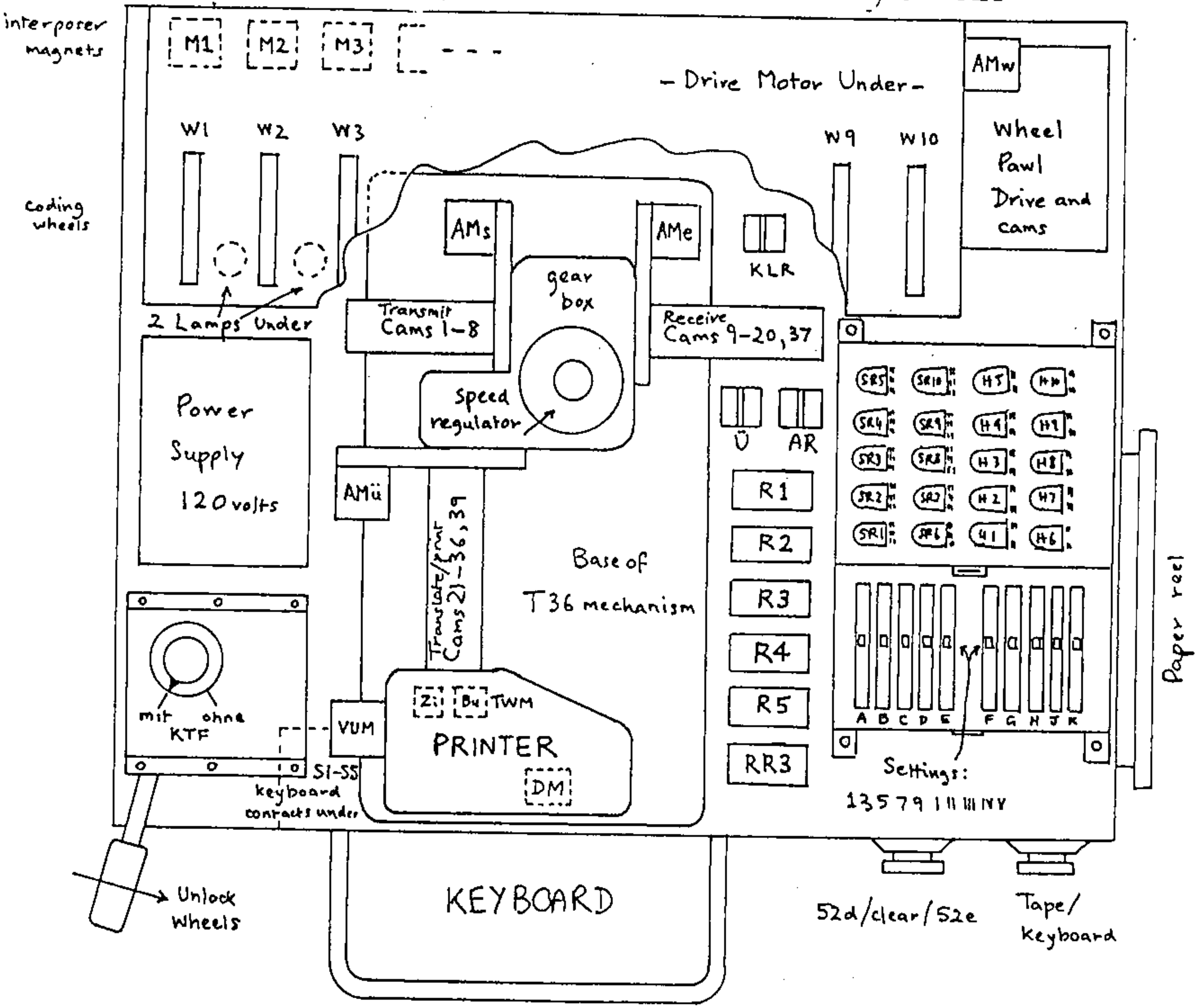
Figure 17

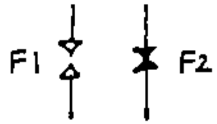
Translator — Printer



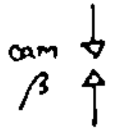
Bu = letters
Zi = figures

Figure 1 — Plan view of the T52e

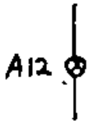




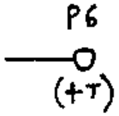
cam-operated contacts
- send cams F 1–8
- receive cams F 9–20,37
- print cams F. 21–36, 39



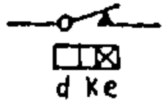
cam-contacts on pawl drive shaft $\alpha / \beta\ \gamma\ \delta$, $\left.\begin{matrix}\mu\\ \lambda\end{matrix}\right\}$ 9 each



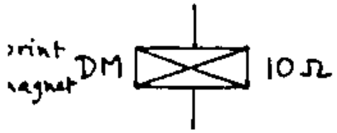
jack-points on relay / key setting box and KTF unit only , units A B C D E



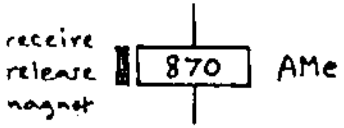
pin of the 13-point connection plug
function of the circuit



52d / Klar / 52e switch
this contact makes in position '52e'
contacts shown in 'e' setting



miscellaneous drive magnets
DM VUM TWM (BuRZL) WRU

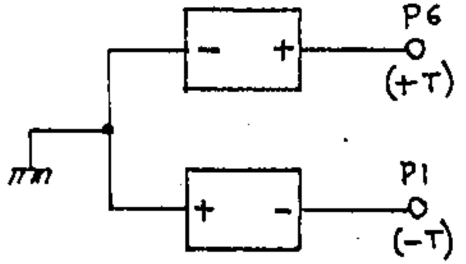


magnet to release clutch of a camshaft or pawl drive shaft

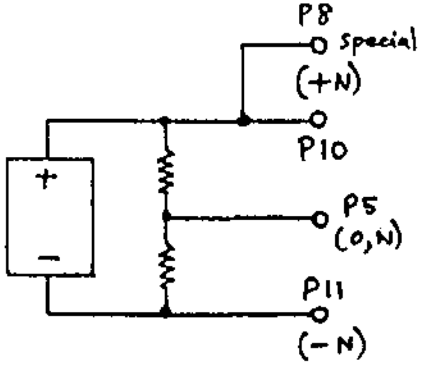
P-connections

1	–T
2	AC
3	AC
4	frame
5	0,N
6	+T '
7	bell
8	+N
9	transmit
10	+N
11	–N
12	U relay
13	receive

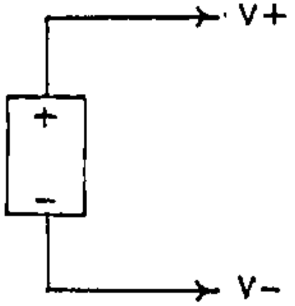
D.C. Supplies



external +60/–60v supply used to generate the transmitted telegraph signal



external +60/–60v supply used in T52 generally including interposer magnets



internal 120v supply used for B contacts and relay SR1–10 and H1–10

Figure 19 Release Magnets Etc.

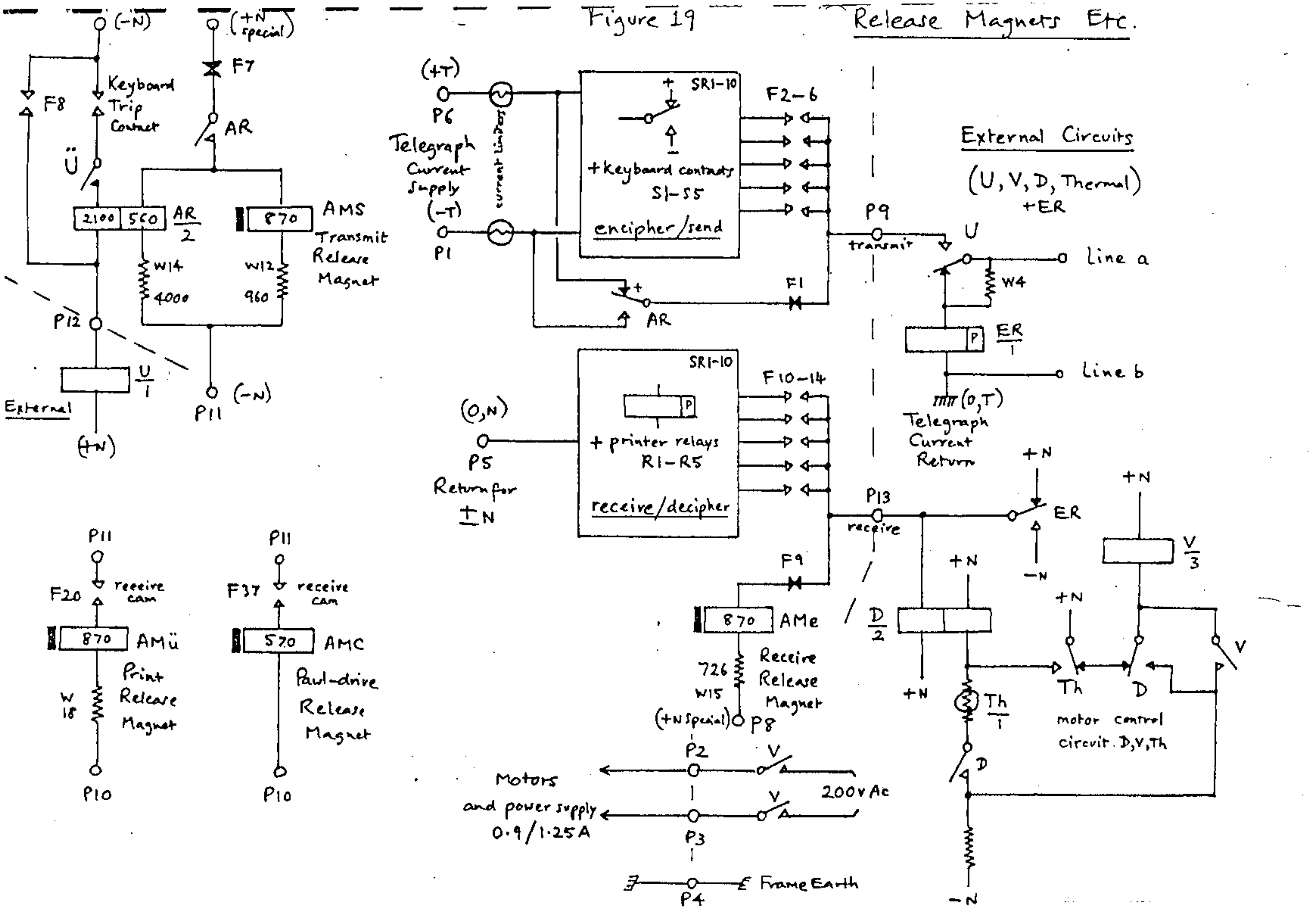
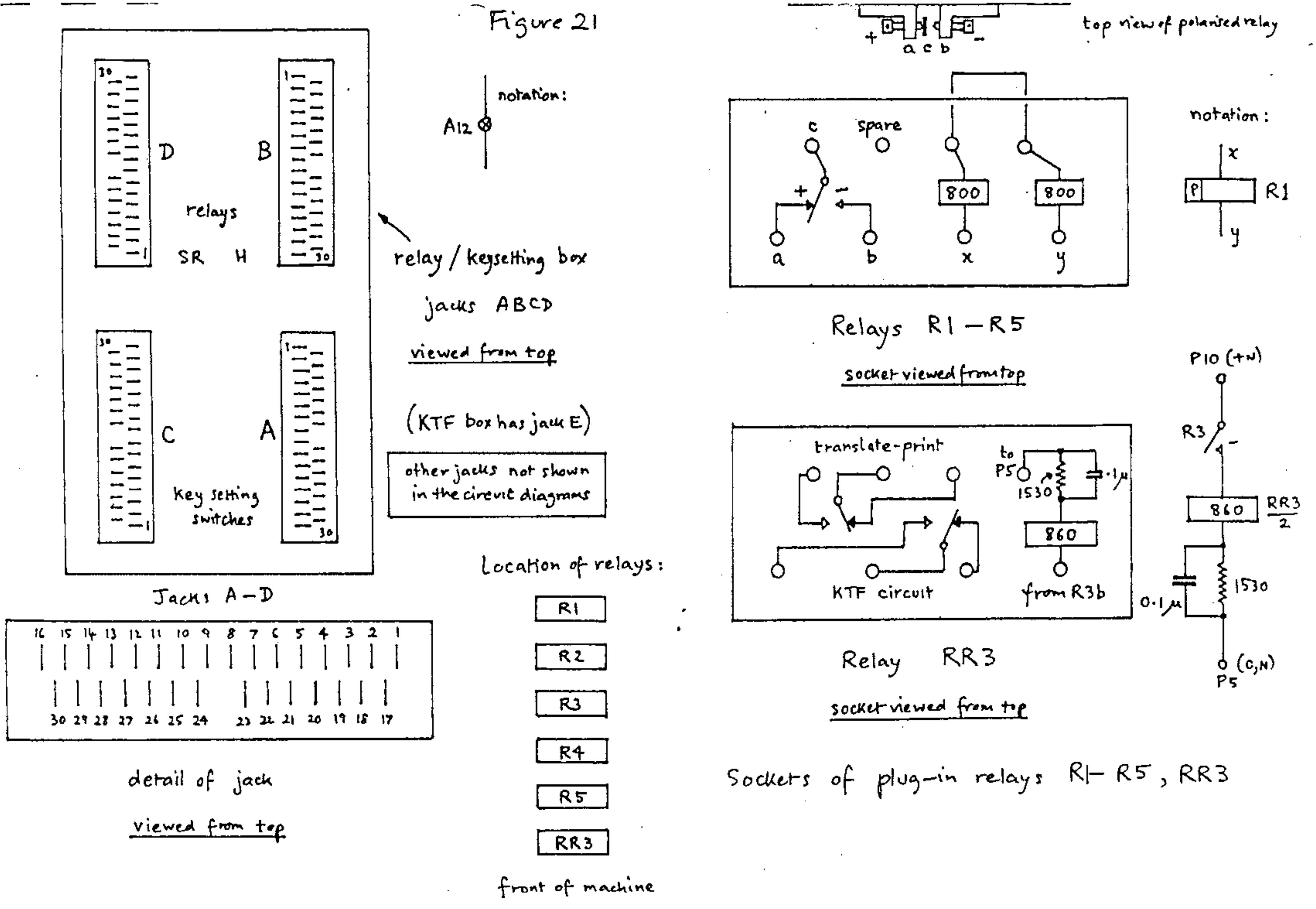


Figure 21



Jacks A – D

Sockets of plug-in relays R1 – R5, RR3