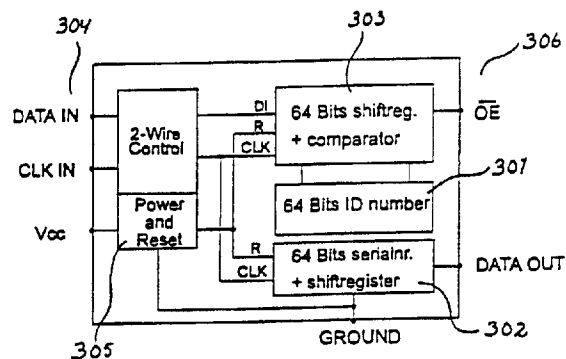




(72) JOHANSSON, Christer, SE
(72) TÖRNGREN, Bengt, SE
(71) ALINGSAS INFORMATION SYSTEM AB, SE
(51) Int.Cl.⁶ G06F 1/16
(30) 1996/05/31 (9602186-0) SE
(54) **DISPOSITIF ANTIVOL**
(54) **ANTI-THEFT DEVICE**



(57) La présente invention concerne un dispositif électronique antivol destiné à des ordinateurs et autres composants électroniques assistés par un processeur, tels que des mémoires, disques durs, des cartes enfichables et des processeurs. Ce dispositif antivol comprend un circuit de blocage intégré dans le composant à protéger, ce circuit comportant une mémoire destinée à stocker un code d'identité spécifique (code ID) servant pour chaque circuit de blocage. En outre, ce circuit présente une entrée servant à entrer un code d'identification dans le circuit, ainsi qu'un comparateur servant à comparer le code d'identification introduit avec le code d'identité spécifique du circuit, et il est conçu pour bloquer le composant et empêcher l'utilisation de celui-ci, en cas d'entrée d'un code d'identification incorrect.

(57) The present invention relates to an electronic anti-theft device for computers and other processor-assisted electronics, such as memory components, hard disks, plug-in boards and processors. The anti-theft device comprises a blocking-circuit which is integrated with the component to be protected, said circuit comprising a memory for storing a specific identity code (ID-code) for each blocking circuit. In addition, the circuit comprises an input for inputting a key code into the circuit, and a comparator for comparing the introduced key code with the ID-code of the circuit, the circuit being adapted to block the component from further use in case of an incorrect key code.

**PCT**WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification⁶ : G06F	A2	(11) International Publication Number: WO 97/45780 (43) International Publication Date: 4 December 1997 (04.12.97)
(21) International Application Number: PCT/SE97/00923 (22) International Filing Date: 29 May 1997 (29.05.97) (30) Priority Data: 9602186-0 31 May 1996 (31.05.96) SE (71) Applicant (for all designated States except US): ALINGSÅS INFORMATION SYSTEM AB [SE/SE]; Metallgatan 3-4, S-441 32 Alingsås (SE). (72) Inventors; and (75) Inventors/Applicants (for US only): JOHANSSON, Chris- ter [SE/SE]; Odengatan 16, S-441 51 Alingsås (SE). TÖRNGREN, Bengt [SE/SE]; Pl 3047, S-466 93 Solle- brunn (SE). (74) Agent: AWAPATENT AB; P.O. Box 11394, S-404 28 Göteborg (SE).		(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, GH, HU, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ARIPO patent (GH, KE, LS, MW, SD, SZ, UG), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG). Published <i>In English translation (filed in Swedish). Without international search report and to be republished upon receipt of that report.</i>
(54) Title: ANTI-THEFT DEVICE (57) Abstract The present invention relates to an electronic anti-theft device for computers and other processor-assisted electronics, such as memory components, hard disks, plug-in boards and processors. The anti-theft device comprises a blocking-circuit which is integrated with the component to be protected, said circuit comprising a memory for storing a specific identity code (ID-code) for each blocking circuit. In addition, the circuit comprises an input for inputting a key code into the circuit, and a comparator for comparing the introduced key code with the ID-code of the circuit, the circuit being adapted to block the component from further use in case of an incorrect key code.		

ANTI-THEFT DEVICETechnical Field

The present invention relates to an anti-theft device for e.g. computers and/or computer components, such as memory modules, plug-in boards, hard disks etc.

5

Background

Within the computer business the number of thefts of particularly the internal components of the computers, such as the memory modules, processors, hard disks etc. has risen considerably lately, which naturally poses serious problems for those affected.

10

It is already known from EP-A2-687 968 to use a circuit in a computer which in connection with start-ups of the computer automatically displays information on personal ownership. The identity data are stored in a non-volatile memory and the identity is checked at each start-up of the system. However, the circuit does not prevent an unauthorised person from direct use of the computer, nor does it prevent computer components from being stolen.

15

20

In order to remedy this problem the inventors provide a system making unauthorised use of stolen computer equipment impossible.

25 Object of the Invention

Consequently one object of the present invention is to provide an anti-theft device which makes unauthorised use of stolen computers or computer parts substantially more difficult.

30

This object is obtained by means of a device as defined in claim 1.

Brief Description of the Drawings

For exemplifying purposes the invention will be described in the following in more detail with reference

35

to an embodiment and to the accompanying drawings, wherein:

Fig. 1 shows the basic idea of the invention;

Fig. 2 shows the ID-check generally in accordance
5 with the invention;

Fig. 3 is a block diagram of the structure of the
check circuit;

Fig. 4 is a flow chart of the blocking-circuit function, and

10 Fig. 5 is a flow chart of the start-up process in
accordance with one application.

Description of Preferred Embodiments

As schematically illustrated in Fig. 1 the anti-
15 theft device in accordance with the invention concerns
protection of e.g. different components in a computer.
The components are checked at computer start-ups. This
is effected by providing each protected component with a
specially made identifying circuit (blocking circuit) by
20 means of which the data flow to the component is checked.
Each blocking-circuit of each component has a specific
identity code (ID-code). The code is also entered into
the host computer and may be checked automatically at
each start-up as illustrated in Fig. 2. Alternatively,
25 the code could instead be stored in the computer hard
disk or the like. In the event the computer detects a
component having a code that is unacceptable to the computer the system stops. Additionally, the very module
which requires the correct code in order to operate is
30 also blocked. This circuit is unique owing to its one-way
communication, which means that it is possible to enter
direct information into the circuit but not to retrieve
ID-information therefrom, which guarantees full security.

If the blocking-circuit has a performance of 64 bits
35 about 18.4×10^{18} possible ID-code combinations are obtainable. It may be added that the ID-code preferably is
stored permanently.

Owing to this arrangement uncontrolled transfer of modules (memories, boards etc) between computers becomes impossible. This means that the computer and its modules can function together only provided that the codes of the computer and of the modules match.

One embodiment of the blocking-circuit is illustrated in Fig. 3. This circuit comprises two permanent memory units 301, 302, such as EEPROM, one memory 301 being intended for storage of an ID-code and one memory 302 for storage of a serial number. The serial number is accessible from outside the circuit whereas the ID-number is not. In addition, the circuit comprises a supply voltage input 305 and one data input 304 and a comparator for comparing the data entered via the input 304 with the ID-code stored in memory 302. Additionally, the circuit comprises an output 306 by means of which the circuit can block the component on which it is located. This output 306 is connected to the comparator in such a manner that the circuit activates the blocking function when a key code entered via the input 304 does not match the stored ID-code.

Several components fitted with a blocking-circuit could partly have the same ID-codes and thus be called in the same manner. This could be done by so-called masking, according to which only certain of the ID-code elements are compared with the key code. This is advantageous e.g. for business enterprises to whom problem-free exchange of components between the company computers is a desirable feature. The possible number of such groups depends on the number of positions that may be masked.

The function of the blocking-circuit will be described in more detail in the following with reference to the flow chart of Fig. 4.

1. The circuit is initially supplied with voltage, Vcc (of e.g. +5V DC), which activates the reset function.

2. The start-up code ("RunIN-code") is entered on the blocking-circuit data input 304. Thereafter, the blocking-circuit is ready to receive a control word.
 3. A control word is then entered to control the circuit.
 4. The blocking circuit checks whether or not the control word is accurate. If not, the blocking circuit is disabled, which blocks the component.
 5. A control word may for instance involve transfer of the blocking-circuit serial number to a data output of the circuit.
 6. A second control word could instead involve a demand for masking (6a).
 7. A third control word provides crediting of the incorrect register (7a).
 8. Family and type numbers are then entered into the blocking-circuit data input 304.
 9. The remaining bits (55-0) are then entered in the blocking-circuit data input 304.
 10. The blocking-circuit compares the bit pattern including the mask in case the control word relating to masking is present. In case of pattern match (10a), the blocking circuit sets the control output to an active level (10b). The blocking circuit is then disabled and the exit remains low until the blocking circuit is restarted.
 11. Decrement of error register by one.
 12. If error register is set to zero the blocking circuit is disabled.
 13. Otherwise, the blocking circuit is restored to a position of reception of fresh key code and returns to point 8.
 14. Disabling routine of blocking circuit. Control output remains in previous status (10b).
- In the following, a start-up process for a system having components that are protected by blocking circuits

will be described with reference to the flow chart of Fig. 5.

1. The system is started or "resetted"
2. System boot is effected.
- 5 3. The system goes to blocking-circuit control program.
4. The control program reads set-up system parameters for the blocking-circuit module.
5. The control program transmits RunIN-code which activates the blocking circuit, placing it in reception
- 10 position.
6. The control program transmits a control word to the blocking circuit, which emits instructions to the blocking-circuit regarding how to handle input data.
7. The control program adds masking information (7a), should this be requested in set-up.
- 15 8. The control program adds credit value (8a), should this be required in set-up.
9. Any information under point 7 and/or 8 is transferred (9a) to the blocking circuit.
- 20 10. The control program reads set-up information for ID-codes.
11. Transmits information to blocking circuit.
12. Transmits ID-code to blocking circuit.
13. The control program checks for arrival of additional
- 25 key codes. When masking has been demanded the control program disregards this. Otherwise a new ID is read (13a).
14. The control program is completed and returns to the main program.
- 30 15. The system reads the parameters in the memory and initiates.
16. The system performs self-test.
17. Self-test OK produces normal start-up (18). If no, show error message (17a).
- 35 18. Start-up.
19. System is locked in endless loop.

Because of the above-mentioned error register the blocking-circuit may allow a number of error ID-code input attempts. The number of allowable attempts of this kind depends on the indicated credit value. The error register is decreased by 1 for each input attempt and when it reaches 0 the circuit is blocked against reception of additional input attempts. This function is desirable in cases when the ID-code input operation is done for instance manually and consequently clerical errors and the like may occur. In addition, the function is desirable when several components are arranged in sequence and transmitted data must reach all components. In this case, all ID-codes may be transmitted to all components and each component will regard the ID-codes of the other components as erroneous attempts.

The blocking-circuit in accordance with the invention makes uncontrolled exchanges of modules (memories, boards, processors etc.) impossible between computers or groups of computers, since a computer and its modules can function together only on condition that the computer and the module codes match. This efficiently obstructs the fencing business, which in turn reduces the attractiveness of the articles that are especially liable to be stolen.

It is likewise possible to provide for a data register of the serial numbers, ID-codes, and ownership of different blocking circuits. It is also possible to add other information to a register of this nature. However, this register should be protected to ensure that only the police authorities and other authorised persons or institutions have access thereto. The register may be used passively in order to simplify the investigations in case of theft or the like or to allow the lawful owner to retrieve lost codes. It could also be used actively to provide component manufacturers, retailers and the like access to the correct ID-code based on a specific serial number when the circuit is to be initiated.

The blocking-circuit in accordance with the invention is integrated in the circuit layout of each module and blocks it owing to its configuration until the correct key is used. The code in the blocking-circuit is not in any way accessible from the outside otherwise than through identification via the register that is connected to the blocking circuit. In addition, the blocking-circuit is sufficiently small to allow it to be bonded to any electronic module.

10 Preferably, the blocking-circuit is also encapsulated, making it completely inaccessible to influences from the outside.

 In the manufacture of computer components or electronic components which are provided with blocking circuits in accordance with the invention it is possible to store the ID-code in the circuit memory already during the manufacturing. However, this requires that the components are accompanied by a list of the ID-codes applicable to each component, allowing the codes to be entered into the control program when the system is assembled.

20 An alternative method is to provide the anti-theft device with a so-called time-out function. A delay function of this kind could mean for instance that the locking circuit is not activated, with the result that the component is kept accessible for a predetermined time period which typically amounts to a few minutes. During this time period the component and the blocking-circuit is serviceable to the user and consequently, when the system is assembled, the user himself may enter the ID-codes desired for the components. However, these ID-codes could still be decided upon centrally by the component manufacturer and delivered to the user when the system is completed.

35 The invention has been described above with reference to one embodiment. However, several varieties of the invention are possible. For instance the anti-theft device in accordance with the invention may be used in

other contexts than in computers, such as in mobile telephones, electronic boxes in cars and boats and the like wherein control is carried out with the aid of processors of some kind. Naturally it is likewise possible to use
5 key codes having a different division between the ID part, the control word and so on, just as it is also possible to use key codes of different length. Further, it is also possible to activate the blocking-circuit and transfer key codes in a different manner, for instance
10 via radio signals or other wireless signals. In this manner it could be possible to trigger the blocking function by remote control in stolen property such as vehicles, mobile telephones and similar appliances.

Such modifications of the embodiment must be considered obvious and to be encompassed by the invention as
15 the latter is defined in the appended claims.

CLAIMS

1. Electronic anti-theft device for computers and
5 other processor-assisted electronics, such as memory
components, hard disks, plug-in boards and processors,
c h a r a c t e r i s e d in that it comprises a blocking
circuit which is integrated with component to be
protected, comprising a memory for storing a specific
10 identity-code (ID-code) for each blocking circuit, and in
that the circuit comprises a communication terminal for
input of a key-code into the circuit and a comparator for
comparing this introduced key-code with the ID-code of
the circuit, the circuit being adapted to block the
15 component for further use in case of a non-correct key-
code.

2. Electronic anti-theft device as claimed in claim
1, c h a r a c t e r i s e d in that the circuit further
comprises a time-delaying unit, delaying the blocking of
20 the component during a pre-set time-period.

3. Electronic anti-theft device as claimed in claim
1 or claim 2, c h a r a c t e r i s e d in that the
components to be protected are part of a system, which
system comprises, in a memory, a register of ID-codes for
25 different components, included in the system and equipped
with anti-theft devices, and which system during start-up
automatically sends out key-codes to these components for
control thereof, whereby the system only functions when
the codes of the system and of the components match.

30 4. Electronic anti-theft device as claimed in any
one of the preceding claims, c h a r a c t e r i s e d in
that the ID-code not is available from the circuit.

5. Electronic anti-theft device as claimed in any
one of the preceding claims, c h a r a c t e r i s e d in
35 that the ID-code is stored permanently in the memory.
Electronic anti-theft device as claimed in any one of the
preceding claims, c h a r a c t e r i s e d in that every

anti-theft device also comprises a unique in the
blocking-circuit stored serial-number that is available
from the outside, whereby a dataregister can be built up
containing serial-numbers connected to corresponding ID-
5 codes for preferably all components comprising the anti-
theft device, and which possibly even connect this
information with information about e.g. the owners of the
components.

1/3

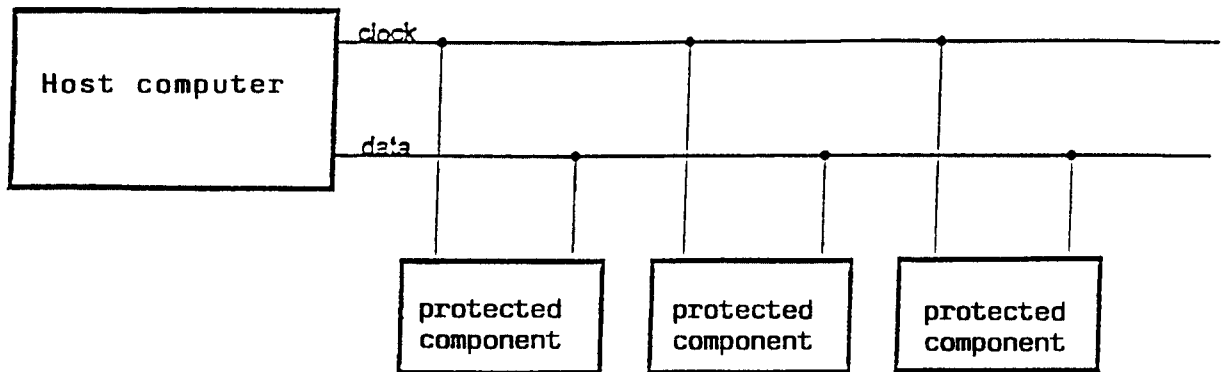


Fig. 1

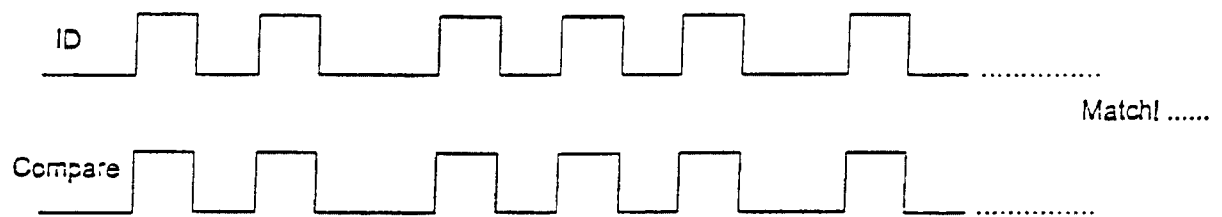


Fig. 2.

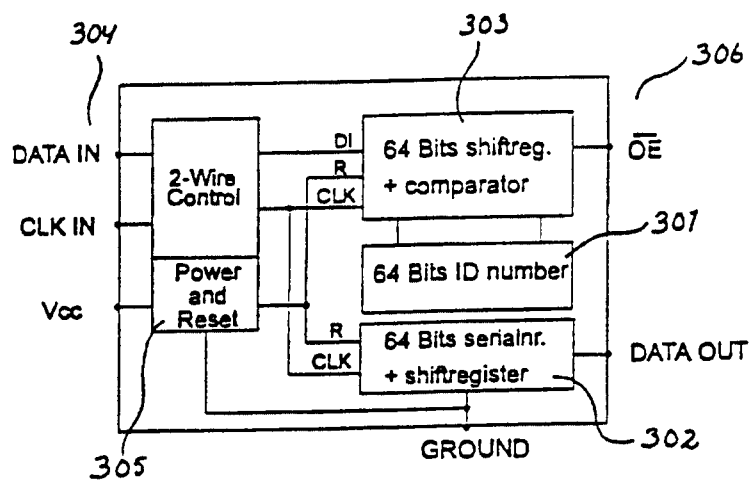


Fig. 3

2 / 3

IDrecivercircuits flowchart

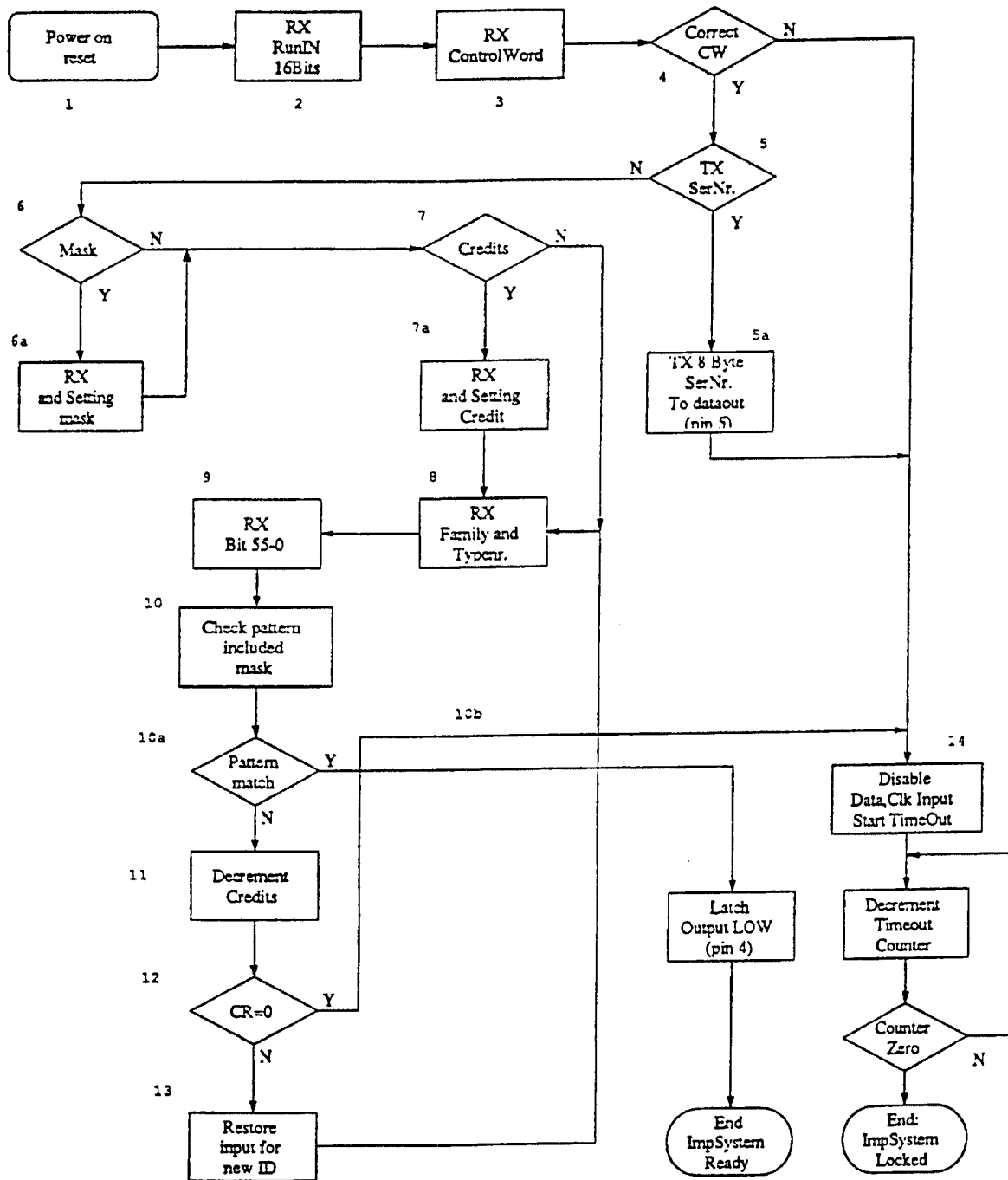


Fig 4.

3 / 3

Flowchart for Systemstartup with IMP

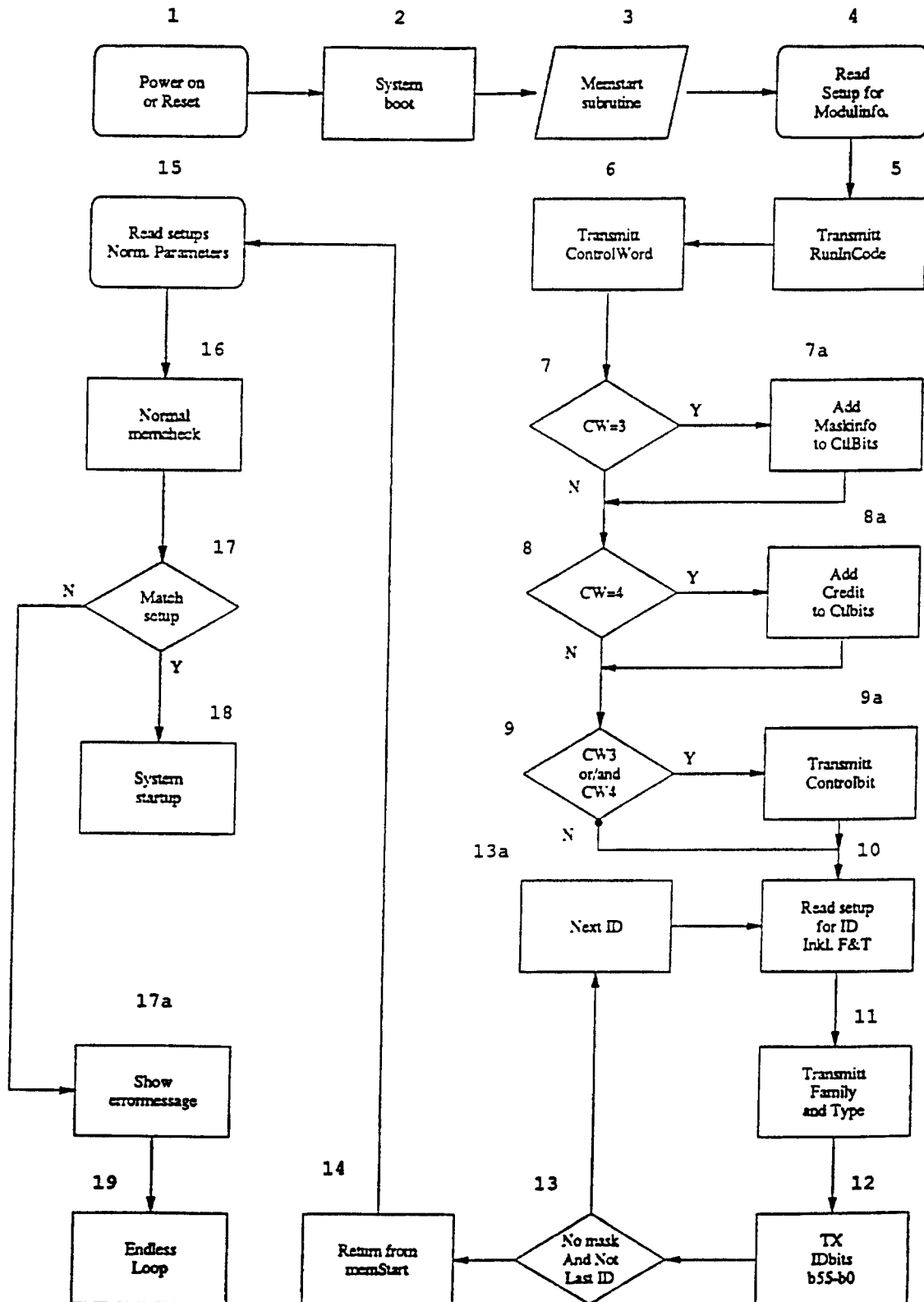


Fig. 5

