

The invention relates to integrated circuits for microchip cards and more particularly to cards of which the integrated circuit microchip comprises not only a microprocessor and a read only program memory (intangible) but also an electrically programmable memory capable of storing not only the data but also the code executable by the microprocessor.

These memory cards are of particular interest in applications comprising a hierarchy of a number of possible functionalities: for example, the manufacturer of microchips for integrated circuits prepares operation programs for the microprocessor at a first functionality level; in particular, he establishes all the programs of the read only memory which are definitely fixed; the microchip manufacturer who incorporates the integrated circuit in his board will establish a second functionality; the institutional client of the card (bank, supplier of services etc.) will establish a third functionality, and the final user (client of the supplier of the service) will be able to use a fourth functionality. This theoretical hierarchy is quoted purely by way of example.

The invention has been found to provide a particularly simple method of making available a number of different functionalities accessible at different utilization levels.

According to the invention the integrated circuit is to comprise not only a microprocessor and a read only memory but also an electrically programmable memory capable of containing code executable by the microprocessor, as well as the following:

- in the read only memory, a number of instructions known as filtering instructions, executable by the microprocessor, in order to read the contents placed at a first specified address of the electrically programmable memory, this address being termed the "filter address",

- means for verifying whether the contents placed at the filter address represent an address belonging to the

electrically programmable memory and situated within predetermined limits, this address being termed the "sub-program address",

- means for causing the microprocessor to execute a sub-program of instructions, which is contained in the electrically programmable memory, from this sub-program address on condition that this address is situated within the prescribed limits, and means for continuing the program of the read only memory if that is not the case, this latter program containing a number of successive filtering instructions each corresponding to a different respective filter address in the electrically programmable memory and to different sub-program address limits for each filtering instruction.

The invention thus offers a general organization of the memories of the microchip, enabling the placing of a number of applications at different levels to be controlled as desired and in a very simple manner.

Further characteristics and advantages of the invention will emerge from a study of the following detailed description, given by reference to the attached drawings, wherein:

Figure 1 shows on highly schematic lines the general organization of an integrated circuit microchip of a microchip board with microprocessor;

Figure 2 illustrates the organization of the memory in an integrated circuit microchip according to the invention.

A conventional integrated circuit microchip of a microprocessor memory board is illustrated in Figure 1. It comprises in the first place a central processing unit 10 (CPU, in English "Central Processing Unit"), in addition to all associated peripheral resources:

- a read only memory 12 (ROM) containing instructions executable by the microprocessor, particularly the programs for the control of the memories and of security of access to the board;

- a live working memory 14 (RAM);

- an electrically programmable EPROM memory (erasable by ultra-violet) or, better still (FLASH EPROM or EEPROM electrically erasable); this memory may comprise not only data but also executable code (instructions executable by the microprocessor);

- input-output gates 18 enabling exchanges to be effected with the exterior of the card, in principle through a very small number of input-output studs E/S.

The invention is particularly applicable to cases in which hierarchized application programs are required to be executable by the microprocessor: a program of a higher hierarchical level must be executed before a program of the subsequent level.

The invention provides that the integrated circuit and its ROM and EPROM or EEPROM memories are organized as follows: first of all it is the read only memory that controls the authorization of access to the EEPROM memory, both at the reading and at the writing stage; subsequently zones of the EEPROM memory, at addresses which will be termed "filtering addresses", are reserved for the purpose of accommodating other addresses, which will be termed "sub-program addresses". Finally, the EEPROM memory contains, starting from a sub-program address, a sub-program executable by the microprocessor. It is the use of this sub-program that is controlled according to the invention.

This organization is illustrated in Figure 2. The memory ROM contains code executable sequentially under the control of a counter (not shown), i.e. the instructions are executed in succession in the same order as the successive addresses of the memory (except for various "branchings" and "jumps"). A zone ZOA of the ROM memory contains, for example, a program for initializing the board (various tests, security verifications, zeroing of registers, etc.) executed when commencing the use of the system.

Following the zone ZOA, a zone Z1A contains a filtering instruction by means of which the presence (and the possibility of using) a first sub-program in the EEPROM

memory can be verified. The filtering instruction is a small sub-program executable by the microprocessor and defining means for:

- reading, in the EEPROM memory, a content at a specified address (address of a zone Z1B of the EEPROM memory); this address is fixed, since it is by the read only memory that it is defined;

- verifying that the content at the address Z1B is an address of the EEPROM memory, this address being contained within the specified limits which, in particular, cover a zone Z1C of the EEPROM memory;

- if this is the case, passing on to the address specified; if it is not the case, proceeding to the subsequent address Z2A of the ROM memory. At the specified address it is the sub-program present in the zone Z1C of the EEPROM memory that will be executed.

A number of successive filtering instructions are thus contained in successive zone of the memory ROM. Each of them corresponds to a respective application sub-program of the EEPROM memory.

In the example shown, for instance, there are three successive filtering instructions in the ROM memory, in successive zones Z1A, Z2A, Z3A of this memory.

The instruction of the zone Z1A refers to a filtering address Z1B of the EEPROM memory, and this instruction contains those limits which are fixed a priori (in the read only memory) between which the contents of the zone Z1B must be situated in order to ensure that the sub-program corresponding to this filtering instruction will be executed. This sub-program is contained in the zone Z1C.

Similarly, the filtering instruction Z2A corresponding to the program of the subsequent hierarchic level (which will not be executed until after the execution of the sub-program of the Z1C zone or after the result of the first filtering) controls the reading of a zone Z2B which is different from the zone Z1B. The sub-program corresponding to this instruction is stored in the zone Z2C; the

microprocessor, however, will only execute the program if the zone Z2C of the contents of the address Z2B is an address situated within the predetermined limits fixed in the memory ROM. These limits are not the same as for the filtering instruction of the zone Z1A, so that blocks are reserved in the memory EEPROM, thanks to the data fixed in the ROM memory, each block corresponding to a certain hierarchic filtering level (in the same order as that in which the filtering instructions of the ROM memory are executed).

Finally, the filtering instruction of the zone Z3A defines further limit values, and thus another block, in which the sub-program of the third level must be situated, i.e. in a zone Z3C of the EEPROM memory. Here again, the test will be positive or negative according to the contents which have been stored in the EEPROM memory at the address Z3B.

When a microchip board is being prepared with a view to a number of possible applications the corresponding programs will be stored in the zones Z1C, Z2C, Z3C of the EEPROM memory.

When the decision has been taken to permit the use of such a sub-program, all that is then required is to store in the EEPROM memory, in the zones Z1B, Z2B, Z3B, address values corresponding to the commencement of the zones containing the application sub-programs which are actually to be put into operation. For those which are not to be utilized, zero or invalid values, i.e. values which will in no case correspond to possible "branchings" towards the "unauthorized" sub-programs, will be stored in the address zones of sub-programs Z1B, Z2B or Z3B.

Access to the zones Z1B, Z2B, Z3B can be reserved (access security control by the ROM memory) according to a certain access hierarchy, particularly by means of confidential codes. This ensures that these zones will in principle no longer be modifiable by users of a lower level in the access hierarchy.

A description has thus been given of an integrated

circuit organization enabling steps to be taken in advance to ensure that successive supplementary functionalities, which are hierarchized, can be added to the functionalities defined by the read only memory, the control of the activation of these supplementary functionalities being very simple, as it is effected by merely writing a valid address into the EEPROM memory at an address which has itself been specified.

**CLAIM**

Integrator circuit comprising a microprocessor (10), a dead program memory (12) and an electrically programmable memory (16) capable of containing instructions executable by the microprocessor, characterized in that it comprises in addition:

- in the read only memory, a number of instructions termed filtering instructions executable by the microprocessor to read the contents placed at a first specified address (Z1B, Z2B, Z3B) of the electrically programmable memory, the address known as "filter address",

- means for verifying whether the contents placed at the filter address represents an address of the electrically programmable memory situated within predetermined limits fixed in the read only memory, this address being termed "sub-program address",

- means for causing the microprocessor to execute a sub-program of instructions, which is contained in the electrically programmable memory, from this sub-program address, on condition that this address is situated within the prescribed limits and means for continuing the program of the dead memory if that is not the case, this latter program containing a number of successive filtering instructions each corresponding to a different respective filter address in the electrically programmable memory and to different sub-program address limits for each filtering instruction.