## CLAIMS

1.- A method for enhancing the reliability of data in a computer (6), the computer (6) being capable of providing an output datum (Ds) from an input datum (De), and including at least two data processing modules (12A, 12B), and a computing member (14) connected to each processing module (12A, 12B),

the method comprising a step (64) for computing, with each processing module (12A, 12B), an intermediate datum ($D_{IA}$, $D_{IB}$) from the input datum (De), said computation consisting in the application of a computing function ($\sigma$) to the input datum (De), the computing function ($\sigma$) being identical for all the processing modules (12A, 12B),

the method being characterized in that it comprises the following steps:

- computing (74) with each processing module (12A, 12B), an intermediate security code ($C_{SIA}$, $C_{SIB}$) from the corresponding intermediate datum ($D_{IA}$, $D_{IB}$),

- transmitting (76) to the computing member (14), with each processing module (12A, 12B), the intermediate security code ($C_{SIA}$, $C_{SIB}$) and the intermediate datum ($D_{IA}$, $D_{IB}$),

- computing (78), with the computing member (14), a security code ($C_S$) from the intermediate security codes ($C_{SIA}$, $C_{SIB}$),

- selecting (80), with the computing member (14), an intermediate datum from the received intermediate data ($D_{IA}$, $D_{IB}$), the output datum (Ds) of the computer (6) comprising the selected intermediate datum, and

- transmitting (82) to a receiving device (8), with the computing member (14), the security code ($C_S$) and the output datum (Ds).

2.- The method according to claim 1, characterized in that each processing module (12A, 12B) includes first means (20A, 20B) for storing in memory at least one encryption variable ($V_{CA}$, $V_{CB}$) and an encryption function (Fc), the encryption function (Fc) being identical for all of the processing modules (12A, 12B), and in that during step (74) for computing an intermediate security code ($C_{SIA}$, $C_{SIB}$) from the corresponding intermediate datum ($D_{IA}$, $D_{IB}$), said computation consists of applying, with each processing module (12A, 12B), the encryption function (Fc) to at least the intermediate datum ($D_{IA}$, $D_{IB}$) and to the encryption variable ($V_{CA}$, $V_{CB}$).

3.- The method according to claim 1 or 2, characterized in that the computing member (14) includes second means (42) for storing in memory at least one decryption constant ($K_D$) and a consolidation function ($F_{conso}$), and that during step (78) for computing a security code ($C_S$) from intermediate security codes ($C_{SIA}$, $C_{SIB}$), said computation consists of applying, with the computing member (14), the consolidation function ($F_{conso}$) to each received intermediate security code ($C_{SIA}$, $C_{SIB}$) and to the decryption constant ($K_D$).

4.- The method according to claim 2 or 3, characterized in that it further includes, between the step (64) for computing an intermediate datum and the step (74) for computing an intermediate security code, a step (66) for transmitting, with each processing module (12A, 12B), the value of its intermediate datum ($D_{IA}$, $D_{IB}$) to the other processing modules (12A,. 12B) and a step (68) for testing, with each processing module (12A, 12B), the existence of a majority value from the whole of the values of the intermediate data ($D_{IA}$, $D_{IB}$), the majority value being the most frequent value among the values of intermediate data ($D_{IA}$, $D_{IB}$), if this value exists.

5.- The method according to claim 4, characterized in that, if the test for existence of a majority value is negative during the corresponding testing step (68), the method includes a step (70) for suppressing with one of the processing modules (12A, 12B), its encryption variable ($V_{CA}$, $V_{CB}$).

6.- The method according to one of claims 2 to 5, characterized in that it further includes before the step (74) for computing an intermediate security code, a step (72) for resetting, with each processing module (12A, 12B), its encryption variable ($V_{CA}$, $V_{CB}$), said reset step (72) being carried out in a synchronized way among all the processing modules (12A, 12B).

7.- The method according to any of the preceding claims, characterized in that the output datum (Ds) is the intermediate datum selected by the computing member (14) during the selection step (80).

8.- The method according to any of the preceding claims, characterized in that it further includes a step (83) for receiving, with the receiving device (8), the security code ($C_S$) and the output datum (Ds) and a step (84) for checking, with the receiving device (8), the consistency between the security code ($C_S$) and the output datum (Ds).

9.- The method according to any of the preceding claims, characterized in that the computer includes three data processing modules, the three processing modules being distributed in three pairs of modules, each module belonging to two distinct pairs, in that each processing module computes two intermediate security codes from the corresponding intermediate datum, each intermediate security code being associated with one of the two pairs to which belongs the module, in that each processing module transmits to the computing member (14) the intermediate datum and the two associated intermediate security codes, in that the computing member (14) computes the security code (Cs) from a first intermediate security code transmitted with one of the processing modules and associated with a first pair of modules, and from a second intermediate security code transmitted by another module, said second intermediate security code being associated with the first pair

of modules, and in that the intermediate datum selected by the computing member (14) is one of the intermediate data associated with the modules of the first pair of modules.

10.- A computer (6) capable of providing an output datum (Ds) from an input datum (De), including:

- at least two data processing modules (12A, 12B), each processing module (12A, 12B) including first means (22A, 22B) for computing an intermediate datum ($D_{IA}$, $D_{IB}$) from the input datum (De), said first computing means being able to apply a computing function ($\sigma$) to the input datum (De), the computing function ($\sigma$) being identical for all the processing modules (12A, 12B),

- a computing member (14) connected to each processing module (12A, 12B),

characterized in that the first computing means (22A, 22B) are further capable of computing an intermediate security code ($C_{SIA}$, $C_{SIB}$) from the corresponding intermediate datum ($D_{IA}$, $D_{IB}$), each processing module (12A, 12B) being capable of transmitting to the computing member (14) the intermediate security code ($C_{SIA}$, $C_{SIB}$) and the corresponding intermediate datum ($D_{IA}$, $D_{IB}$), and in that the computing member (14) includes second means (44) for computing a security code (Cs) from intermediate security codes ($C_{SIA}$, $C_{SIB}$), the computing member (14) being capable of selecting an intermediate datum among the received intermediate data ($D_{IA}$, $D_{IB}$) and of transmitting the security code ($C_S$) and the output datum (Ds) to a receiving device (8), the output datum (Ds) comprising the selected intermediate datum.

11.- A communication unit (2) including a computer (6) and a data receiving device (8), the computer (6) being capable of providing a security code ($C_S$) and a datum (Ds), the receiving device (8) including means for storing in memory a control algorithm, the receiving device (8) being capable of receiving the security code ($C_S$) and the output datum (Ds), and of checking, by applying the control algorithm, the consistency between the security code ($C_S$) and the output datum (Ds), characterized in that the computer (6) in accordance with claim 10.

12.- A railway management system (1) characterized in that it comprises at least one unit (2) according to claim 11.

## CLAIMS

1.- A method for enhancing the reliability of data in a computer (6), the computer (6) being capable of providing an output datum (Ds) from an input datum (De), and including at least two data processing modules (12A, 12B), and a computing member (14) connected to each processing module (12A, 12B),

the method comprising a step (64) for computing, with each processing module (12A, 12B), an intermediate datum ($D_{IA}$, $D_{IB}$) from the input datum (De), said computation consisting in the application of a computing function ($\sigma$) to the input datum (De), the computing function ($\sigma$) being identical for all the processing modules (12A, 12B),

the method being characterized in that it comprises the following steps:

- computing (74) with each processing module (12A, 12B), an intermediate security code ($C_{SIA}$, $C_{SIB}$) from the corresponding intermediate datum ($D_{IA}$, $D_{IB}$),

- transmitting (76) to the computing member (14), with each processing module (12A, 12B), the intermediate security code ($C_{SIA}$, $C_{SIB}$) and the intermediate datum ($D_{IA}$, $D_{IB}$),

- computing (78), with the computing member (14), a security code ($C_S$) from the intermediate security codes ($C_{SIA}$, $C_{SIB}$),

- selecting (80), with the computing member (14), an intermediate datum from the received intermediate data ($D_{IA}$, $D_{IB}$), the output datum (Ds) of the computer (6) comprising the selected intermediate datum, and

- transmitting (82) to a receiving device (8), with the computing member (14), the security code ($C_S$) and the output datum (Ds);

and in that the computer includes three data processing modules, the three processing modules being distributed in three pairs of modules, each module belonging to two distinct pairs, in that each processing module computes two intermediate security codes from the corresponding intermediate datum, each intermediate security code being associated with one of the two pairs to which belongs the module, in that each processing module transmits to the computing member (14) the intermediate datum and the two associated intermediate security codes, in that the computing member (14) computes the security code (Cs) from a first intermediate security code transmitted with one of the processing modules and associated with a first pair of modules, and from a second intermediate security code transmitted by another module, said second intermediate security code being associated with the first pair of modules, and in that the intermediate datum selected by the computing member (14) is one of the intermediate data associated with the modules of the first pair of modules.

2.- The method according to claim 1, characterized in that each processing module (12A, 12B) includes first means (20A, 20B) for storing in memory at least one encryption

variable ($V_{CA}$, $V_{CB}$) and an encryption function (Fc), the encryption function (Fc) being identical for all of the processing modules (12A, 12B), and in that during step (74) for computing an intermediate security code ($C_{SIA}$, $C_{SIB}$) from the corresponding intermediate datum ($D_{IA}$, $D_{IB}$), said computation consists of applying, with each processing module (12A, 12B), the encryption function (Fc) to at least the intermediate datum ($D_{IA}$, $D_{IB}$) and to the encryption variable ($V_{CA}$, $V_{CB}$).

3.- The method according to claim 1 or 2, characterized in that the computing member (14) includes second means (42) for storing in memory at least one decryption constant ($K_D$) and a consolidation function ($F_{conso}$), and that during step (78) for computing a security code ($C_S$) from intermediate security codes ($C_{SIA}$, $C_{SIB}$), said computation consists of applying, with the computing member (14), the consolidation function ($F_{conso}$) to each received intermediate security code ($C_{SIA}$, $C_{SIB}$) and to the decryption constant ($K_D$).

4.- The method according to claim 2 or 3, characterized in that it further includes, between the step (64) for computing an intermediate datum and the step (74) for computing an intermediate security code, a step (66) for transmitting, with each processing module (12A, 12B), the value of its intermediate datum ($D_{IA}$, $D_{IB}$) to the other processing modules (12A,. 12B) and a step (68) for testing, with each processing module (12A, 12B), the existence of a majority value from the whole of the values of the intermediate data ($D_{IA}$, $D_{IB}$), the majority value being the most frequent value among the values of intermediate data ($D_{IA}$, $D_{IB}$), if this value exists.

5.- The method according to claim 4, characterized in that, if the test for existence of a majority value is negative during the corresponding testing step (68), the method includes a step (70) for suppressing with one of the processing modules (12A, 12B), its encryption variable ($V_{CA}$, $V_{CB}$).

6.- The method according to one of claims 2 to 5, characterized in that it further includes before the step (74) for computing an intermediate security code, a step (72) for resetting, with each processing module (12A, 12B), its encryption variable ($V_{CA}$, $V_{CB}$), said reset step (72) being carried out in a synchronized way among all the processing modules (12A, 12B).

7.- The method according to any of the preceding claims, characterized in that the output datum (Ds) is the intermediate datum selected by the computing member (14) during the selection step (80).

8.- The method according to any of the preceding claims, characterized in that it further includes a step (83) for receiving, with the receiving device (8), the security code ($C_S$) and the output datum (Ds) and a step (84) for checking, with the receiving device (8), the consistency between the security code ($C_S$) and the output datum (Ds).

9.- A computer (6) capable of providing an output datum (Ds) from an input datum (De), including:

- at least two data processing modules (12A, 12B), each processing module (12A, 12B) including first means (22A, 22B) for computing an intermediate datum ($D_{IA}$, $D_{IB}$) from the input datum (De), said first computing means being able to apply a computing function ($\sigma$) to the input datum (De), the computing function ($\sigma$) being identical for all the processing modules (12A, 12B),

- a computing member (14) connected to each processing module (12A, 12B),

characterized in that the first computing means (22A, 22B) are further capable of computing an intermediate security code ($C_{SIA}$, $C_{SIB}$) from the corresponding intermediate datum ($D_{IA}$, $D_{IB}$), each processing module (12A, 12B) being capable of transmitting to the computing member (14) the intermediate security code ($C_{SIA}$, $C_{SIB}$) and the corresponding intermediate datum ($D_{IA}$, $D_{IB}$), and in that the computing member (14) includes second means (44) for computing a security code (Cs) from intermediate security codes ($C_{SIA}$, $C_{SIB}$), the computing member (14) being capable of selecting an intermediate datum among the received intermediate data ($D_{IA}$, $D_{IB}$) and of transmitting the security code ($C_S$) and the output datum (Ds) to a receiving device (8), the output datum (Ds) comprising the selected intermediate datum;

and in that the computer includes three data processing modules, the three processing modules being distributed in three pairs of modules, each module belonging to two distinct pairs, in that each processing module computes two intermediate security codes from the corresponding intermediate datum, each intermediate security code being associated with one of the two pairs to which belongs the module, in that each processing module transmits to the computing member (14) the intermediate datum and the two associated intermediate security codes, in that the computing member (14) computes the security code (Cs) from a first intermediate security code transmitted with one of the processing modules and associated with a first pair of modules, and from a second intermediate security code transmitted by another module, said second intermediate security code being associated with the first pair of modules, and in that the intermediate datum selected by the computing member (14) is one of the intermediate data associated with the modules of the first pair of modules.

10.- A communication unit (2) including a computer (6) and a data receiving device (8), the computer (6) being capable of providing a security code ($C_S$) and a datum (Ds), the receiving device (8) including means for storing in memory a control algorithm, the receiving device (8) being capable of receiving the security code ($C_S$) and the output datum (Ds), and

of checking, by applying the control algorithm, the consistency between the security code ($C_S$) and the output datum (Ds), characterized in that the computer (6) in accordance with claim 9.

11.- A railway management system (1) characterized in that it comprises at least one unit (2) according to claim 10.