

Description

Title of the invention: Method for sharing data relating to the manufacturing of a product

[0001] Technical field

- 5 [0002] The present invention relates to a method for sharing manufacturing data on a product, to a system for sharing manufacturing data on a product, and to a computer program product comprising program instructions exploitable by said system for sharing manufacturing data on a product.

[0003] Prior art

- 10 [0004] It is known to use RFID tags (RFID standing for Radio Frequency Identification) in manufacturing processes that require a certain level of dematerialization and security and the configuration of the manufactured products of which must be guaranteed. These constraints are particularly present in high-technology fields such as production of products for aeronautical applications,
- 15 space-technology applications or the medical field. Conventionally, a manufacturing process consists in assembling, in a certain order and depending on their features, various sub-products in various manufacturing operations and manufacturing steps defined during the development and industrialization of the product. Series production involves these various manufacturing operations being faithfully repeated
- 20 by means of execution management software or any other means allowing the physical characteristics of the produced product to be subsequently compared with specifications in a file defining the product and validated. In the context of products intended for markets that are highly regulated, these products may be accompanied by a bundle of documents proving production and testing has been carried out as
- 25 required and the origins of the materials used and any other document requested by the customer. Conventionally, a manufacturing process may be generated using production execution monitoring software, such as PLM software (PLM standing for Product Lifecycle Management), ERP software (ERP standing for Enterprise Resource Planning) or MES software (MES standing for Manufacturing Execution
- 30 System). Such software is able to associate with each production step implementation of any required instructions or plan element. However, this software requires databases of large size. In addition, any change in the physical state of the

product is accompanied by a change in the information system, this inducing substantial flows of data between the various machines of the production line.

Access to low-cost communicating objects such as RFID tags is increasingly contributing to allowing, in industry, data associated with sub-products to be readily located, identified and borne. Industrial processes have been improved thereby, but use has still not been made of the full potential of these RFID tags.

[0005] There is therefore a need to improve methods for sharing manufacturing data on a product using RFID tags while avoiding, at least partially, the need to use production execution monitoring software and while improving traceability, production compliance and the security of the data shared.

[0006] Summary of the invention

[0007] The present invention aims to at least partially meet this need.

[0008] More particularly, the present invention aims to improve how manufacturing data on a product are shared.

[0009] A first subject of the invention is a method for sharing manufacturing data on a product, said product being manufactured from various sub-products in various manufacturing operations, each sub-product and/or each manufacturing operation being associated with one RFID tag, each RFID tag comprising data on the manufacturing state of the product. During manufacture of the product, the method comprises:

- a step of receiving data on the manufacturing state of the product from the at least two RFID tags;
- a step of generating new data on the manufacturing state of the product based on said received state data, said received state data being reorganized in said generating step;
- a step of transmitting the new data on the manufacturing state of the product to the at least two RFID tags.

[0010] The proposed solution is based on the existence in parallel of physical components for carrying out a production operation and of RFID tags attached to the sub-products, allowing location requests to be responded to but also data to be exchanged. Assembly results in assembly, on one site and in the same time period, of one or more sub-products, but also of the informational image of this assembly

transaction. Thus, it is the product in the process of being assembled that bears the information system. The RFID tags contain data on the manufacturing state of the product at a given time. This data on the manufacturing state of the product is updated on each manufacturing operation. The physical and digital assembly operations are in perfect one-to-one correspondence and an operation can no longer be validated if the sub-products have not actually undergone this operation.

Transactions with monitoring software are decreased to the bare minimum, this increasing resilience to potential network failures. Furthermore, data on the manufacturing state of the product are generated while limiting interactions with a wide-area network, this providing manufacturing facilities with autonomy and flexibility. Lastly, the production journey is generated iteratively by loading operations in step N+1 at the end of the validation of step N and no longer in a blanket fashion at the start of a cycle. This makes it possible to make use only of the manufacturing-state data necessary for the current step.

[0011] In one embodiment, the generating step comprises a step of aggregating the state data of the at least two RFID tags, a step of splitting said state data, and a step of merging the split data to form new data on the manufacturing state of the product.

[0012] Thus, the state data are reorganized in the course of the generating step. These data are first aggregated. By "aggregation", what is meant is the action of uniting distinct elements to form a homogeneous whole. The aggregating step thus corresponds to a concatenating step in which it is possible to identify all the aggregated elements. The aggregated state data are then split, i.e. divided to form split data. These split data are merged to form new data on the manufacturing state of the product. By "merge", what is meant is the action of uniting distinct elements to form a homogeneous whole in which it is impossible to perceive the origin of the merged data. In these steps, it is possible to perform various operations on the state data, such as operations of complete or partial duplication of the data, etc. The generated new state data are transmitted to the at least two RFID tags.

[0013] In one particular embodiment, the new data on the manufacturing state of the product are distributed between the at least two RFID tags.

[0014] These new state data are thus divided between various RFID tags, this allowing the overall security of these data to be increased while together recording

the state of progress of the manufacture of the product. The computations based on which the data on the manufacturing state of the product are distributed are carried out locally, via local machines or RFID tags, this decreasing the load on corporate servers. Preferably, the same state data are transmitted to both RFID tags. As a
 5 variant, different new state data are transmitted to each RFID tag.

[0015] In one particular embodiment, the data on the manufacturing state of the product comprise data selected from the list of the following data:

- one or more plans;
- one or more certificates of conformity;
- 10 - one or more instruction sheets;
- one or more manufacturing results.

[0016] In industry, manufacturing processes are based on execution, in production, of manufacturing operations in accordance with a specification file that is a non-exhaustive compilation of data from plans, materials, manufacturing and quality-
 15 control tolerances, various instructions, test methods, etc. Production sequences make constant reference to this specification file as production of the product progresses, and a manufacturing file is generated symmetrically, completion of the product being endorsed once these operations have been successfully completed and conformity verified.

20 [0017] In one particular embodiment, the method comprises, prior to the step of transmitting the new data, a step of encrypting said new state data.

[0018] Thus, any modification in the data on manufacturing state is reflected in a secure transaction with the RFID tags. This transaction for example uses asymmetric encryption, employing a pair of keys consisting of a private key and a public key. The
 25 overall security of the method for sharing data is thus improved.

[0019] In one particular embodiment, the method comprises a step of verifying the received state data.

[0020] Thus, on each manufacturing operation, the state data are verified. This verification takes place, for example, once state data obtained from various RFID
 30 tags have been merged. If one or more RFID tags are inadvertently replaced in the product in the process of being manufactured, the merger of the state data is not compliant and it is recommendable to stop manufacturing to verify the various RFID

tags. This state-data verification is also required to avoid any risk in the event of malicious modifications of the state data in the RFID tags during the manufacture of the product.

5 [0021] In one particular embodiment, the new state data are stored in a centralized state-data storage device.

[0022] This makes it possible to monitor the various product manufacturing operations centrally.

[0023] In one particular embodiment, the new state data are stored in a blockchain.

10 [0024] By blockchain, what is meant is a distributed database secured by cryptographic techniques. The exchanged transactions are grouped into blocks at regular time intervals, thereby forming a blockchain. After recent transactions have been recorded, a new block is generated and analyzed. If the block is valid, it may be timestamped and added to the blockchain. Each block is linked to the previous one by a hash key. Thus, once added to the blockchain, a block may no longer be
15 modified or deleted, this guaranteeing the authenticity and security of the stored data. The blocks of data of the blockchain may be readable and/or writable by entities external to the manufacturing plant. For example, the blocks of data may be consulted by a buyer of the manufactured product wanting to ensure its conformity. Such a buyer will then be able to gain access to details of the various manufacturing
20 operations via the blockchain.

[0025] Another subject of the invention is a system for sharing manufacturing data on a product, said product being manufactured from various sub-products in various manufacturing operations. Each sub-product and/or each manufacturing operation is associated with one RFID tag. Each RFID tag contains data on the manufacturing
25 state of the product. The system for sharing data comprises:

- a receiver of data on the manufacturing state of the product from the at least two RFID tags;
- a generator of new data on the manufacturing state of the product based on said received state data, said received state data being reorganized by said generator;
- 30 - a transmitter of the new data on the manufacturing state of the product to the at least two RFID tags.

[0026] In one particular embodiment, the system comprises a centralized state-data storage device for storing new state data.

[0027] In one particular embodiment, the system comprises a blockchain for storing new state data.

5 [0028] Another subject of the invention is a computer program product comprising program instructions that are exploitable by the system for sharing manufacturing data on a product according to the preceding subject, which, when they are executed or interpreted by said system, trigger implementation of the method for sharing manufacturing data on a product according to the other preceding subject.

10 [0029] The present invention will be better understood on reading the detailed description of embodiments, which are given merely by way of non-limiting example, and illustrated by the appended drawings, in which:

[0030] **[Fig 1]** figure 1 is a schematic view illustrating a system for sharing manufacturing data on a product according to the invention;

15 [0031] **[Fig 2]** figure 2 is a schematic view of a local computer of the system for sharing data of figure 1;

[0032] **[Fig 3]** figure 3 illustrates one portion of a method for sharing manufacturing data on a product according to the invention.

20 [0033] The invention is not limited to the described embodiments and variants, and other embodiments and variants will seem obvious to those skilled in the art.

[0034] In the various figures, identical or similar elements have been designated with the same references.

[0035] Figure 1 schematically shows a system 10 according to the invention for sharing manufacturing data on a product. This system here comprises:

- 25
- RFID tags A, B, C, D, E;
 - local machines 11A, 11B, 11C, 11D;
 - local computers 12A, 12B, 12C, 12D;
 - a central server 13;
 - a local network 14;

30

 - a cloud-computing system 15;
 - a gateway 16.

[0036] The RFID tags A, B, C, D, E are electronic components comprising an antenna and an electronic chip. The antenna is designed to operate in a given frequency band, and for example at a low frequency comprised between 120 kHz and 150 kHz. The electronic chip is connected to the antenna. This chip is intended to store an identifier Id_A , Id_B , Id_C , Id_D , Id_E associated with each of the RFID tags A, B, C, D, E, respectively. The electronic chip is also suitable for storing data S_A , S_B , S_C , S_D ; S'_A , S'_B ; S''_A , S''_B , S''_C ; S'''_A , S'''_B , S'''_C , S'''_D ; S_E , S''''_A , S''''_B , S''''_C , S''''_D , S''''_E on the manufacturing state of the product. These state data are modifiable in the RFID tag. It will be noted that since the product is manufactured from various sub-products in various manufacturing operations, each sub-product is associated with one RFID tag A, B, C, D. Similarly, an intangible operation, for example thermal testing or loading of software, may also be associated with an RFID tag E.

[0037] The local machines 11A, 11B, 11C, 11D are able to read the RFID tags A, B, C, D, E and to extract all or some of the data on the manufacturing state of the product. These local machines 11A, 11B, 11C, 11D are also able to write new data on the manufacturing state of the product in place of the state data initially extracted. For example, local machine 11A extracts data S_A on manufacturing state from RFID tag A and data S_B on manufacturing state from RFID tag B. These data S_A , S_B on manufacturing state are sent to local computer 12A. In return, local computer 12A provides new state data S'_A and S'_B which will be written to RFID tag A and to RFID tag B, respectively. The local machines 11A, 11B, 11C, 11D also allow various sub-products to be assembled in various manufacturing operations.

[0038] The local computers 12A, 12B, 12C, 12D are able to perform operations of aggregating data on the manufacturing state of the product obtained from various RFID tags and operations of merging split data. The merged data are next divided into new data on the manufacturing state of the product, then distributed between the various RFID tags. Figure 2 more particularly illustrates local computer 12A of figure 1. This local computer 12A comprises a receiver 121 of state data S_A , S_B from RFID tag A and from RFID tag B, respectively. The receiver 121 also receives the identifiers Id_A , Id_B of the RFID tags A, B. Local computer 12A further comprises a generator 122 of new state data S'_A , S'_B . As already specified, this generator 122 aggregates the received state data S_A , S_B then it breaks them up and merges them into new state data S'_A , S'_B . In one variant embodiment, the aggregated state data

are recombined before being broken up. This makes it possible to introduce a certain randomness into the generation of these new state data. The new state data S'_A , S'_B are associated with the identifiers Id_A , Id_B of the RFID tags A, B, respectively. Lastly, a transmitter 123 transmits the new state data S'_A , S'_B to said RFID tags A, B. The description of local computer 12A given with reference to figure 2 also applies mutatis mutandis to the other local computers 12B, 12C, 12D.

[0039] The central server 13 is able to centralize the data on the manufacturing state of the product. To this end, it comprises suitable storage means. These storage means may thus contain the entire history of the manufacturing process of the product.

[0040] The local network 14 allows communication between the local machines 11A, 11B, 11C, 11D, the local computers 12A, 12B, 12C, 12D and the central server 13.

[0041] The cloud-computing system 15 encompasses all of the accessible computing services provided from outside the manufacturing plant. These computing services are, for example, a service allowing storage on third-party servers, a networking service, a service providing software such as office software, a service providing content, and a service providing Internet access.

[0042] The gateway 16 connects the central server 11 to the cloud-computing system 12. It thus allows the local network and the Internet network of the cloud-computing system 15 to be linked. The gateway 16 mainly routes data packets. It may also perform a firewall or proxy function or monitor the quality of service of the network.

[0043] A method, according to the invention, for sharing manufacturing data on a product will now be described with reference to figure 1 and figure 3. The product manufactured here is a computer for acquiring and displaying aircraft data used to actuate the flaps of said aircraft. This acquiring computer comprises a casing, a power supply card, a CPU card (CPU standing for Central Processing Unit), and a graphics card. Each of these sub-components comprises an RFID tag. Thus, the casing is associated with RFID tag A, the power supply card is associated with RFID tag B, the CPU card is associated with RFID tag C, and the graphics card is associated with RFID tag D. RFID tag A contains identifier Id_A . RFID tag B contains identifier Id_B . RFID tag C contains identifier Id_C . RFID tag D contains identifier Id_D . An

RFID tag E is associated with a salt spray test. This test is carried out once the casing, the power supply card, the CPU card and the graphics card have been assembled. For its part, RFID tag E contains identifier Id_E .

[0044] Figure 3 illustrates steps EX1 to EX5, with X comprised between 1 and N, N representing the number of operations (assembly, processing) that the various sub-products will undergo to form the end product. In a first operation E1, the power supply card is assembled with the casing by local machine 11A. The state data S_A associated with RFID tag A and the state data S_B associated with RFID tag B are transmitted by local machine 11A. In a step E11, these state data S_A , S_B are received by local computer 12A. In a step E12, new state data S'_A , S'_B are generated. In a step E13, the new state data S'_A , S'_B are encrypted. To do this, local computer 12A comprises a private key and local machine 11A comprises a public key associated with said private key. In a step E14, these new state data S'_A , S'_B are transmitted to local machine 11A. These data are then stored in RFID tags A and B, respectively, in place of the previous state data S_A , S_B . It will be noted that the new state data S'_A , S'_B are different from the state data S_A , S_B . In one particular embodiment, the new state data S'_A are identical to the new state data S'_B . As a variant, the new state data S'_A may be different from the new state data S'_B . In parallel, in a step E15, the new state data S'_A , S'_B are stored in the centralized state-data storage device 13. These new state data S'_A , S'_B are associated, in the centralized storage device 13, with the identifiers Id_A , Id_B of the RFID tags A, B and with an identifier corresponding to the first operation E1.

[0045] The RFID tag attached to each important sub-product of the nomenclature contains, in addition to its conventional data, a set of data related to the manufacturing process, which is characterized by the fact that manufacturing is monitored in the same way as with monitoring software. The traceability and security of production data are thus drastically improved and it is possible, with each transformation of the product, whether said transformation is physical or not, to associate a transformation in the information system, and to ensure products may always be located.

[0046] In a second operation E2, the CPU card is assembled with an assembly comprising the power supply card and the casing, by local machine 11B. The state

data S'_A associated with RFID tag A, the state data S'_B associated with RFID tag B and the state data S'_C associated with RFID tag C are transmitted by local machine 11B. In a step E21, these state data S'_A , S'_B , S'_C are received by local computer 12B. In a step E22, new state data S''_A , S''_B , S''_C are generated. In a step E23, the new state data S''_A , S''_B , S''_C are encrypted. To do this, local computer 12B comprises a private key and local machine 11B comprises a public key associated with the private key. In a step E24, these new state data S''_A , S''_B , S''_C are transmitted to local machine 11C. These data are then stored in RFID tags A, B and C, respectively, in place of the previous state data S'_A , S'_B , S'_C . It will be noted that the new state data S''_A , S''_B , S''_C are different from the state data S'_A , S'_B , S'_C . In one particular embodiment, the new state data S''_A are identical to the new state data S''_B and S''_C . As a variant, the new state data S''_A may be different from the new state data S''_B and S''_C . In parallel, in a step E25, the new state data S''_A , S''_B , S''_C are stored in the centralized state-data storage device 13. These new state data S''_A , S''_B , S''_C are associated, in the centralized storage device 13, with the identifiers Id_A , Id_B , Id_C of the RFID tags A, B, C and with an identifier associated with the second operation E2.

[0047] The procedure followed is identical in the third operation E3 and in the fourth operation E4.

[0048] Thus, the third operation E3 regards assembly of the graphics card with an assembly comprising the CPU card, the power supply card and the casing, by local machine 11C. New state data S'''_A , S'''_B , S'''_C , S'''_D are generated from the state data S''_A , S''_B , S''_C , S_D by local computer 12C in various operations E31 to E35. These new state data S'''_A , S'''_B , S'''_C , S'''_D are associated, in the centralized storage device 13, with the identifiers Id_A , Id_B , Id_C , Id_D of the RFID tags A, B, C, D and with an identifier associated with the third operation E3.

[0049] The fourth operation E4 regards a salt spray test carried out, on an assembly comprising the graphics card, the CPU card, the power supply card, and the casing, by local machine 11D. New state data S''''_A , S''''_B , S''''_C , S''''_D , S''''_E are generated from the state data S'''_A , S'''_B , S'''_C , S'''_D by local computer 12D in various operations E41 to E45. These new state data S''''_A , S''''_B , S''''_C , S''''_D , S''''_E are associated, in the centralized storage device 13, with the identifiers Id_A , Id_B , Id_C , Id_D , Id_E of the RFID tags A, B, C, D, E and with an identifier of the fourth operation E4.

[0050] The end product then comprises RFID tags A, B, C, D, E with the new state data S''''_A , S''''_B , S''''_C , S''''_D , S''''_E . An identifier Id_F is associated with this end product. This identifier Id_F is stored in the centralized storage device 13 with the operations E1, E2, E3, E4.

5 [0051] In one preferred embodiment, the state data are verified on receipt thereof by the various local computers 12B, 12C, 12D. For example, it is verified whether the received state data S'_A , S'_B are identical or compatible with one another. If this is not the case, it is deduced therefrom that one of the RFID tags A, B tags has been modified, intentionally or unintentionally, between the first operation E1 and the
10 second operation E2. Therefore, manufacture of the product must be stopped.

[0052] The state data associated with the identifiers of the RFID tags and the identifiers of the various operations may be consulted at any time internally from the centralized storage device 13. These data may also be consulted by people outside the manufacturing plant via the cloud-computing system 15, the gateway 16 and the
15 central server 13 and based on the identifier Id_F present on the end product.

[0053] In one preferred embodiment, the new state data are stored in a blockchain (not shown in figure 1) as the operations E1, E2, E3, E4 progress. This blockchain is accessible by people outside the manufacturing plant via the cloud-computing system 15, the gateway 16 and based on the identifier Id_F present on the end
20 product.

[0054] Another subject of the invention is a computer program product comprising program instructions that are exploitable by the system 121, 122, 123 for sharing manufacturing data on the end product which, when they are executed or interpreted by this system, trigger implementation of the method for sharing data E1, E2, E3, E4.

25 [0055] The computer program may be stored on a storage medium that is readable by a processor. The medium may be electronic, magnetic, optical or electromagnetic.

[0056] In particular, the invention may be implemented by a device comprising a processor and a memory. The processor may be a generic processor, a specific processor, an application-specific integrated circuit (ASIC) or a field-programmable
30 gate array (FPGA).

[0057] The device may use one or more dedicated electronic circuits or a general purpose circuit. The technique of the invention may be carried out on a reprogrammable computing machine (a processor or a microcontroller, for example) executing a program comprising a sequence of instructions, or on a dedicated computing machine (for example a set of logic gates such as an FPGA or an ASIC, or any other hardware module).

[0058] According to one embodiment, the device comprises at least one computer-readable storage medium (RAM, ROM, EEPROM, flash memory or another memory technology; CD-ROM, DVD or another optical-disc-based medium; magnetic cassette, magnetic tape; non-volatile computer-readable storage disk) encoded with a computer program (i.e. a number of executable instructions) that, when it is executed on one or more processors, performs the functions of the embodiments of the invention described above.

[0059] By way of example of a hardware architecture suitable for implementing the invention, a device according to the invention may comprise a communication bus to which are connected a central processing unit or microprocessor, a read-only memory (ROM) which may contain the programs required to implement the invention, a random-access memory (RAM) or cache memory containing registers suitable for storing variables and parameters created and modified during the execution of the aforementioned programs, and a communication or I/O interface (I/O standing for Input/Output) suitable for transmitting and receiving data.

[0060] The invention thus makes it possible, based on state data on A on an RFID tag A and on state data on B on an RFID tag B, which are initial components undergoing a production process, to aggregate, split and then merge data obtained from these state data on A and on B, and to redistribute them in an encrypted manner to the storage capacity available at this moment in the process. This storage capacity corresponds to the RFID tags A and B, and hence each tag considered independently does not allow coherent information to be recreated. The security of configuration management and management of all traceability data are improved.

[0061] The invention further has the following advantages:

- the need for informational transactions with the computer network and monitoring software is limited since the data on manufacturing state are embedded directly into

the RFID tags;

- resilience to failure of the monitoring software is improved;
- it is guaranteed that any physical modification of the product during its manufacture is simultaneously reflected in a secure transaction with the information

5 system;

- the configuration of the manufactured product is guaranteed, while data on this configuration are protected by encryption and sharing said information physically between the RFID tags;

10 - any unauthorized intervention on or repair or dismantling of a sub-product results in destruction of or an inability to recover existing information on the product analogously to a tamper-evident label;

15 - the system used to progress production is completely secure and operations that do not involve physical modification (heat treatment, testing, memory loading, etc.) are easily and reliably monitored by encoding performance of these operations in the way described above;

- the use of blockchain technologies ensures operations are uniquely linked, configuration control and improved resistance to reverse engineering.

[0062] The fact that progress through the manufacturing process is characterized by the addition, on one site, of other sub-assemblies bearing RFID tags allows the security of the associated documentary evidence to be increased by dividing this
20 documentary evidence up and encrypting it on a blockchain.

[0063] As a result, progress through the manufacturing process is possible relatively independently of a monitoring system, successful completion of an operation (assembly, testing, etc.) resulting in an unequivocal and systematic transformation of
25 the documentary evidence, and encryption and re-division thereof between the RFID tags attached to the sub-components.

[0064] The invention is not limited to the described embodiments and variants, and other embodiments and variants will seem obvious to those skilled in the art.

[0065] Thus, the invention is applicable to high-technology fields such as the
30 production of products for aeronautical applications, for space-technology applications or for the medical field, in which fields configuration and traceability are key.

[0066] Thus, the invention is applicable to manufacturing processes the supply chain of which is complex or spatially dispersed with attendant problems in locating components.

5 [0067] Thus, reading of the RFID tags in the various local machines allows various sub-products to be located in the process flow.

[0068] Thus, all or some of the RFID tags have a distributed computing capacity.

10 [0069] Thus, a merge-encrypt-divide strategy may be applied to any system of collaborative IoT objects (IoT standing for Internet of Things) in which it is sought to secure data and in which the presence of all of the objects is critical to successful completion of a mission or an operation.

[0070] Thus, the invention is applicable to any group of communicating objects having a need to operate together (share information) securely and in which it is critical not to lose a component from the chain.

Claims

[Claim 1] A method for sharing manufacturing data on a product, said product being manufactured from various sub-products in various manufacturing operations, each sub-product and/or each manufacturing operation being associated with one RFID tag (A, B, C, D, E), each RFID tag comprising data (S_A , S_B ; S'_A , S'_B , S_C ; S''_A , S''_B , S''_C , S_D ; S'''_A , S'''_B , S'''_C , S'''_D , S_E) on the manufacturing state of the product, characterized in that during the manufacture of said product, said method comprises:

- a step (EX1) of receiving data on the manufacturing state of the product from the at least two RFID tags;
- a step (EX2) of generating new data (S'_A , S'_B ; S''_A , S''_B , S''_C ; S'''_A , S'''_B , S'''_C , S'''_D ; S''''_A , S''''_B , S''''_C , S''''_D , S''''_E) on the manufacturing state of the product based on said received state data (S_A , S_B ; S'_A , S'_B , S_C ; S''_A , S''_B , S''_C , S_D ; S'''_A , S'''_B , S'''_C , S'''_D , S_E), said received state data being reorganized in said generating step;
- a step (EX4) of transmitting the new data on the manufacturing state of the product to the at least two RFID tags (A, B, C, D, E).

[Claim 2] The method as claimed in claim 1, wherein the generating step comprises a step of aggregating the state data (S_A , S_B ; S'_A , S'_B , S_C ; S''_A , S''_B , S''_C , S_D ; S'''_A , S'''_B , S'''_C , S'''_D , S_E) of the at least two RFID tags, a step of splitting said state data, and a step of merging the split data to form new data (S'_A , S'_B ; S''_A , S''_B , S''_C ; S'''_A , S'''_B , S'''_C , S'''_D ; S''''_A , S''''_B , S''''_C , S''''_D , S''''_E) on the manufacturing state of the product.

[Claim 3] The method as claimed in either one of claims 1 and 2, wherein the new data on the manufacturing state of the product are distributed between the at least two RFID tags.

[Claim 4] The method as claimed in any one of claims 1 to 3, wherein the data on the manufacturing state of the product comprise data selected from the list of the following data:

- one or more plans;
- one or more certificates of conformity;
- one or more instruction sheets;
- one or more manufacturing results.

[Claim 5] The method as claimed in any one of claims 1 to 4, wherein said method comprises, prior to the step (EX4) of transmitting the new state data, a step (EX3) of encrypting said new state data.

5 [Claim 6] The method as claimed in any of claims 1 to 5, wherein said method comprises a step of verifying the received state data.

[Claim 7] The method as claimed in any one of claims 1 to 6, wherein the new state data are stored (EX5) in a centralized state-data storage device (13).

[Claim 8] The method as claimed in any of claims 1 to 7, wherein the new state data are stored in a blockchain.

10 [Claim 9] A system for sharing manufacturing data on a product, said product being manufactured from various sub-products in various manufacturing operations, each sub-product and/or each manufacturing operation being associated with one RFID tag, each RFID tag comprising data on the manufacturing state of the product, said data-sharing system comprising:

15 - a receiver (121) of data ($S_A, S_B; S'_A, S'_B, S_C; S''_A, S''_B, S''_C, S_D; S'''_A, S'''_B, S'''_C, S'''_D, S_E$) on the manufacturing state of the product from at least two RFID tags;

- a generator (122) of new data ($S'_A, S'_B; S''_A, S''_B, S''_C; S'''_A, S'''_B, S'''_C, S'''_D; S''''_A, S''''_B, S''''_C, S''''_D, S''''_E$) on the manufacturing state of the product based on said received state data, said received state data being reorganized by said generator

20 (122);

- a transmitter (123) of the new data on the manufacturing state of the product to the at least two RFID tags.

[Claim 10] The system as claimed in claim 9, wherein said system comprises a centralized state-data storage device (13) for storing new state data.

25 [Claim 11] The system as claimed in either one of claims 9 and 10, wherein said system comprises a blockchain for storing the new state data.

[Claim 12] A computer program product comprising program instructions that are exploitable by the system for sharing manufacturing data on a product as claimed in claims 9 to 11, which, when they are executed or interpreted by said system,

30 trigger implementation of the method for sharing manufacturing data on a product as claimed in any one of claims 1 to 8.