

An RFID-Based Anti-Counterfeiting Track and Trace Solution

Ioan Ungurean, Cornel Turcu, Vasile Gaitan and Valentin Popa
*Stefan cel Mare University of Suceava
Romania*

1. Introduction

As markets become more global and competition intensifies, firms are beginning to realize that competition is not exclusively a firm versus firm domain, but a supply chain against supply chain phenomenon (Wu, 2008). Under these circumstances, an increasing strategic importance to any organization independent of size or of sector is to deliver information, goods and services in full, on time and error-free to customers.

Radio Frequency Identification (RFID) technology represents one of a number of possible solutions to enhance supply chain. RFID technology permits the unique identification of each container, pallet, case and item to be manufactured, shipped and sold, thus allowing an increased visibility throughout the supply chain. Also, an RFID anti-counterfeiting mechanism could be implemented.

This chapter focuses on how RFID technology can be used to solve problems faced by supply chain, such as track and traceability, anti-counterfeiting. It proposes a track-and-trace anti-counterfeiting system using RFID technology. The submitted system (hereinafter referred to as ATPROD system) is aimed at relatively high-end consumer products, and it helps protect genuine products by maintaining the product pedigree and the supply chain integrity. Our system integrates mobile systems to extend corporate data outwards to mobile devices for viewing and querying. Also, users can use any mobile device endowed with an RFID reader for data collection. In this way, manual entry data has been eliminated. Moreover, users can read the tags wherever the items are placed, which enables a more flexible storage environment and an efficiency increase of supply chains and anti-counterfeiting.

We developed an RFID embedded system based on an eBox with an RFID reader attached. This system, named MICC (Interfacing, Command and Control Module), enables many applications to run at the same time as concurrent processes.

Each entry or/ and exit gate of the warehouse in a supply chain could be managed by a MICC module. If there are multiple gates the installed MICC modules (from warehouse or company) could be linked together into a network.

From a functional perspective, the MICC module must meet the following requirements: to read/ write data on RFID tags attached to items passing through a gate, to manage a large number of RFID tags passing through a gate at the same time, to provide data transmission via the network to a central server, to process local data and to provide the possibility of

online and offline operation, as well as a set of commands in order to adapt it to a range of applications by software configurations.

From a hardware perspective, the MICC module is an embedded device, built around Vortex86SX SoC (System on Chip) device. This device integrates an x86 processor, different input/ output interfaces (RS-232, parallel, USB, GPIO), BIOS, power management, MTBF counter, LoC (LAN on Chip), JTAG on the same chip. Two versions of MICC module have been designed and developed: MICC01 - without VGA output and MICC02 with VGA output. The RFID reader could be directly connected to the eBox using the USB or serial port. As for the operating system employed, each module runs Windows CE 6.0, which can perform real-time operations.

An OPC (OLE for process control) data server will run on a MICC module. This server is designed according to OPC specifications and can be a possible support for RFID middleware. The OPC data server ensures communication with the RFID reader/ writer and sends information to the central database.

Thus, the application from the MICC module will be developed as an OPC data server that will communicate via RS232 or USB with RFID reader/ writer. The communication between data server and RFID reader is based on a communication model that uses real-time capabilities of the operating system. This communication model allows the management of a large number of tags at the same time.

The developed system offers a good price-performance ratio. Also, it will satisfy a large number of customer requirements for fields such as industry, retail, supply chain, logistics etc.

2. Functional description of the authentication system

The MICC module is designed as a component of an RFID-based authentication and track & trace system for supply chains. This subchapter displays a short description of this system.

The main role of the system is to authenticate well-known brand products. Such authentication is carried out at various points within the supply chain (starting with the manufacturer, up to the end user). The secondary function of the system is to track and trace products.

Each product has an RFID tag (also named transponder) attached to it. An RFID tag has a factory-programmed identification code stored in a non-volatile memory. This tag also provides a limited capacity memory that is used to store required information. Thus, an RFID tag could store data concerning the trace of the product to which the tag is attached (for every point of the trace; such information will also be sent to the manufacturer's server). Operationally, product authentication and track & trace can be structured on three levels (see Fig. 1): manufacturer, distributor and retailer. At the manufacturer's level, there is a server by which product authentication is performed.

At the manufacturer's level, each manufactured product will have an attached tag that identifies the product (at the encasement phase). This tag may display initial information (manufacturer, product code, manufacturing date, warranty period, server's address where authentication of products can be performed, or any other information). If a product needs special transport and storage conditions, the RFID tag may hold a temperature sensor and memory, in order to carry out temperature logger (automatic data recorder), which will include data read from the temperature sensor. Also, at this level, products can be grouped into packages or pallets.

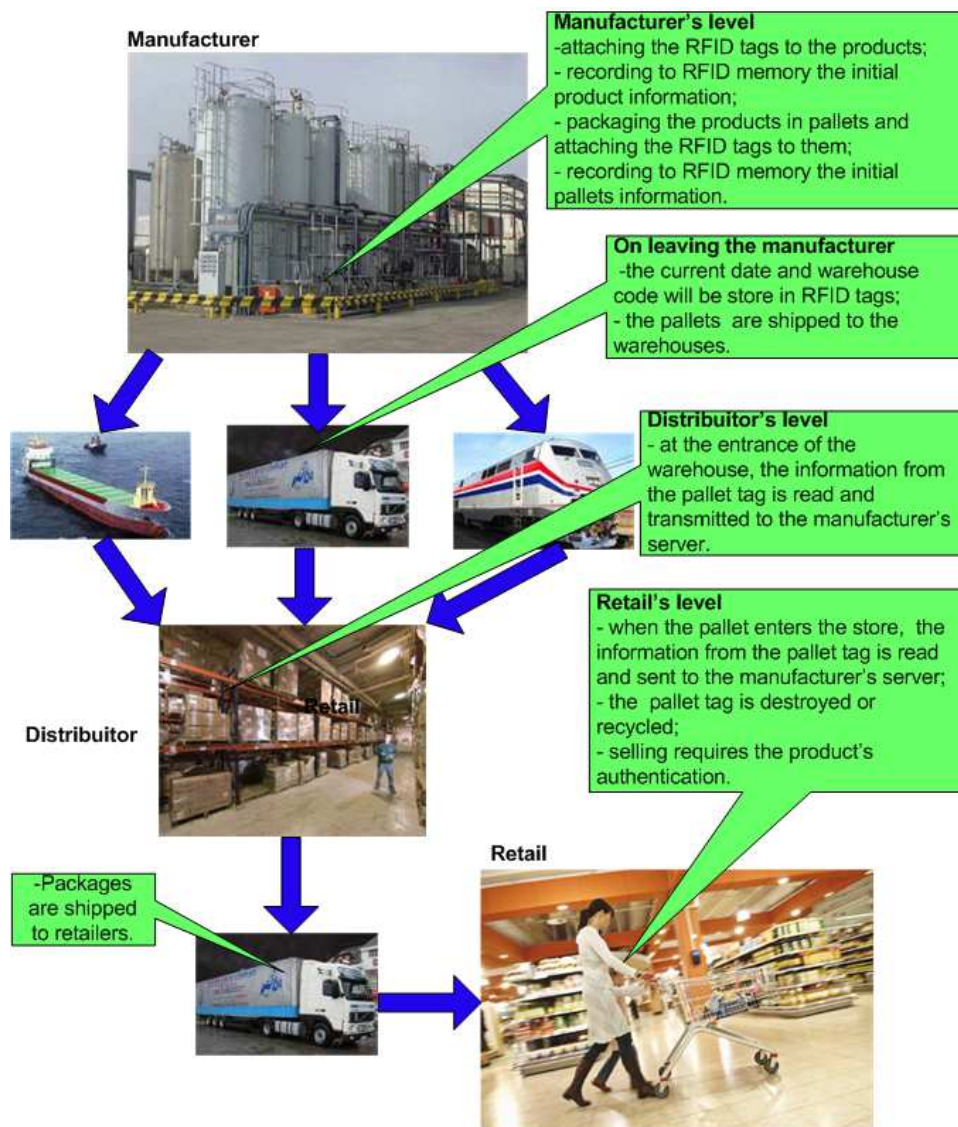


Fig. 1. Authentication and track and trace of products from manufacturer to end user customer

At the distributor's level, when a product is received into the warehouse, the information saved on the attached RFID tag will be read and sent to the manufacturer (if authentication is required). To accomplish the authentication process, a comparison is carried out between the information received from the distributor and the information from the manufacturer (stored in the manufacturer's database server). The distributor receives the results of this comparison. If the authentication process confirms the product's origin, then the data

regarding product reception into the distributor's warehouse will be automatically written to the product tag. Since distributors can be organized on three levels (international, national and regional), products or packages can be transported to any other distributor or retail dealer in the supply chain.

In retail, when products are received into the warehouse, authentication can be performed in the same manner as at the distributor's level. Afterwards, the RFID tag attached to the product can be destroyed or kept attached to the product in order to preserve product ID for future maintenance.

3. Hardware architecture of the ATPROD system

The operational model proposed in this chapter aims to authenticate, track and trace products, starting from their manufacturing phase up to their selling to end users (Fig. 1). The ATPROD system may also be developed in order to track and trace products, until they reach a recycling center. Block diagram and hardware elements are illustrated as follows:

Fig. 2 emphasizes the general hardware architecture of the operational model, at one of points in the supply chain where a pallet/ product passes: manufacturing, distribution or retail. Elements illustrated in the block diagram are the following: RFID tags attached to products and pallets, RFID readers, MICCs (Interface, Command and Control Module), PCs used in order to process information read from RFID tags and to authenticate products in accordance to this information; firewall and/ or router used to secure Internet connection, manufacturer's server – installed at the manufacturer's level for each manufacturer, PCs provided in order to read information associated to each product, MICC. The MICC module will be used in order to process information read from RFID tags, to authenticate the products according to this data, as well as to write the product tag and send information to the manufacturer's database server.

For each manufacturer, a central server is employed to store data specific to each product. This server will be connected to the Internet (and protected by a firewall), and used to perform authentication. All PCs connected to the Internet can connect to this server, through a password and security certificate, to access information about products of a specific manufacturer.

Pallets and/ or products are provided with RFID tags. Information stored on these tags is read/ written/ updated by RFID readers. Readers are connected by a serial port or USB port to PC or MICC module, which controls and processes information read from RFID tags. By means of these connections, the MICC modules should receive information read from RFID tags; the modules should also transmit new information to be written on the RFID tags. The ATPROD system should operate on 13.56 MHz and should allow multiple tag readability (reading of tags attached to products included in a pallet) enabled by its anti-collision function.

MICC modules are similar, in function, to dedicated computing systems (Barr, 2007), being connected to the Internet (and protected by means of firewalls), in order to carry out the authentication of products on manufacturer's server. Dedicated computing systems are used more often, because they center round systems designed and optimized to carry out specific tasks. In contradistinction to the general use of computing systems (personal computers), a dedicated system includes a hardware subsystem specialized and optimized to carry out the tasks for which the system was designed. Since the system is dedicated to reach specific tasks, the designers can optimize its architecture, in order to reduce its dimension and final cost.

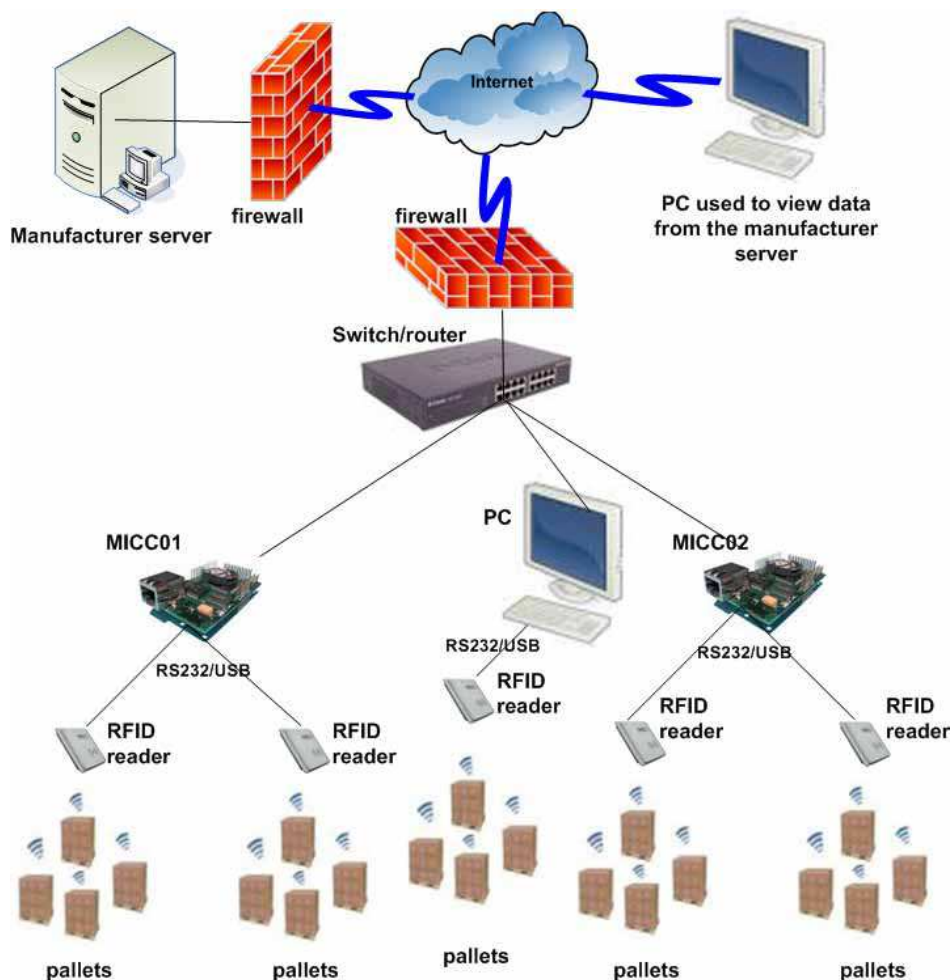


Fig. 2. Hardware architecture of the ATPROD system

The architecture illustrated in Fig. 2 is part of the class of dedicated architectures; these types of architectures face intensive network traffic better, the latter being specific to the infrastructures of a high number of RFID tags. A router or firewall equipment will isolate the network, and ensure data security. In this way, bandwidth is saved, which would have been otherwise busy with various passwords, authentications and other security information. Computing time is also saved, which otherwise would have been spent with different encryption/ decryption methods, key generators etc.

In defining hardware architecture at unit level (manufacturer, reseller or retailer), hardware resources should be taken into consideration (storing capacity, communication interfaces, computational ability), required by the software packages used on implementing the system.

In what concerns the software, the use of OPC specifications helps improve the system (Lange et al., 2010) (Gaitan et al., 2010), as a potential support to RFID middleware. These

specifications are used by many manufacturers to implement many applications of their work field. The current OPC specifications reached the maturity phase (Mahnke et al., 2009). OPC specifications allow the connection of any OPC server to any other OPC client. Several clients can be connected to the same server and a client can connect to more than one server. Thus, a server can become another server's client, or servers can connect directly with one another. A special versatility will therefore be achieved for application configuration. These characteristics may generate a configuration of servers hierarchically connected in a tree type structure.

Clients at the level of MICC modules can also be created, in the view of configuring and local tracking, for packaging of cases, pallets or charging/ discharging at docks level. If servers from other levels are clients of other servers, then servers from the last level will represent the clients of readers. The diversity and complexity of readers should be hidden by these servers. As result, they will implement a software level, often named HAL (Hardware Abstraction Level), especially to operating systems, which signifies a level of hardware abstracting. Each unit is connected to the Internet, and all units are grouped in a VPN network.

4. Block diagram of MICC module

After an analysis of hardware requirements for the MICC module, its designing in accordance with SoC Vortex86SX device was proposed. Depending on functions provided by the Vortex86SX processor (***a, 2010), carrying out a MICC module is proposed. Its architecture can be seen in Fig. 3. The Vortex86SX processor (***a, 2010) is compatible with x86 family and is of a SoC type. By using this solution, Windows XP or Linux operating systems can be set up on a MICC module, where the system operates as a desktop system of limited resources. If the aim is the executing of tasks in real time, operating systems as Linux Embedded or Windows CE can be used. As illustrated in the figure, the MICC module provides 1 port of Ethernet, 3 USB ports, 2 RS232 ports, 32 programmable digital I/ O (0-5V), 1 IDE port for HDD connection, an interface for connecting a CF flash card, one PS2 port for connecting mouse and keyboard, as well as one VGA output used for monitor connection.

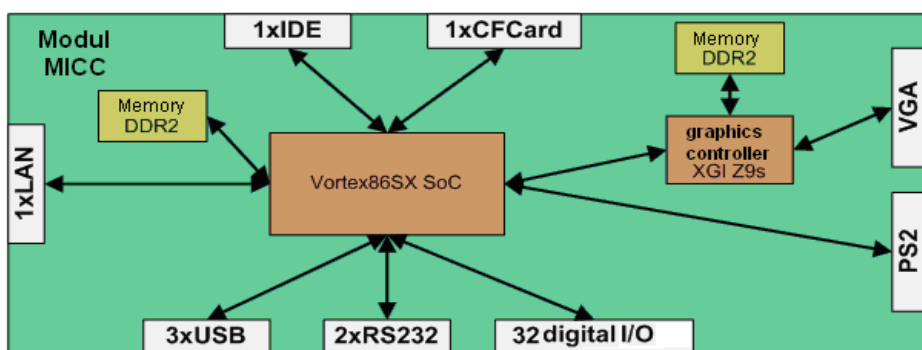


Fig. 3. Block diagram of MICC module

Most of the facilities provided by the MICC module are integrated on a SoC Vortex86SX chip (***a, 2010). Besides, this chip includes a DDR2 memory of 128 MB connected to

Vortex86SC by a DDR2 interface, and a graphical controller XGI Volari Z9s connected to Vortex86SX by a PCI interface. After defining these requirements, printed circuit board (PCB) design can be started. Electrical circuitries can be performed for MICC02 version (with VGA port), and the MICC01 (without VGA) can be obtained by using the same PCB, on which the graphical controller and DDR2 memory used will not be mounted.

The MICC module is designed according to Vortex86SX (***a, 2010) produced by DMP company (***b, 2010). Vortex86SX is a SoC x86, manufactured by using 0.13 microns technology and a model of very low power consumption (less than 1 Watt). This intelligent SoC displays important features, such as: various interfaces of input/ output (RS-232, parallel, USB or GPIO), BIOS, WatchDog type timer, management of power consumption, MTFB counter, LoC (LAN on chip), JTAG, etc., features that are not integrated on a single chip of 27x27mm (BGA-581). Vortex86SX is compatible with Windows CE, Linux and DOS operating systems. It integrates, on the same chip SoC 32KB a cache memory L1, ISA bus on 16bits, PCI bus Rev. 2.1 of 33MHz on 32 bits, SDRAM, DDR2, ROM controller, IPC (peripheral internal controllers with DMA and timer/ counter of interruption included), SPI (serial peripheral interface), Fast Ethernet MAC, FIFO UART, USB 2.0 main and IDE controller.

5. Designing PCB circuit board for MICC module

The next step in designing the MICC module is the PCB circuit board design. We aimed to obtain a board of 11x11cm, resulting in an ergonomic MICC module of low sizes. The PCB circuit board is structured on 3 layers (Top, Middle and Bottom) of minimal width of a running wire of 10 mil (use of three layers is preferred, due to the high number of pins for Vortex86SX SoC chip). Fig. 4 illustrates the PCB circuit board for designing the MICC device.

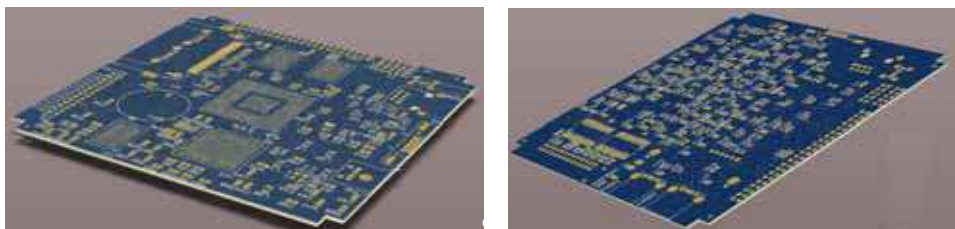


Fig. 4. Front and back images of the PCB

6. Software architecture of the ATPROD system

The general architecture of the ATPROD system is illustrated in Fig. 5. It is obvious that several manufacturers may co-exist in this architecture. Each of them could have more production lines, geographically distributed in more locations. The warehouses and retailers are also geographically distributed in some more locations, provided with Internet connection, in order to have access to the manufacturers' servers and to be able to authenticate products and send information related to their traceability.

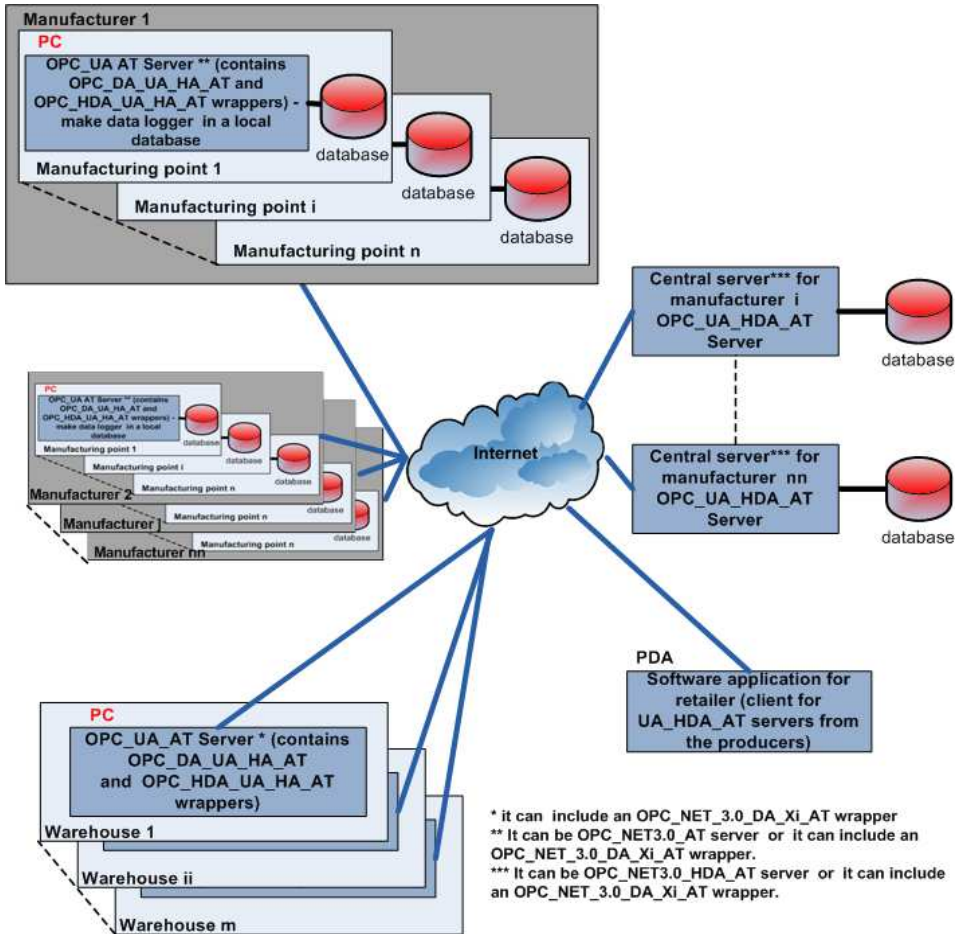


Fig. 5. Software architecture of the ATPROD system

Each manufacturer has a central server, on which an OPC_UA_HDA_AT server runs. This server will store information regarding the products that exit the production line and are sent to the resellers' warehouses. At the level of each distribution point, there is a PC that runs an OPC_UA_AT server. This server is able to send requests for information about the manufacturing process, as well as to save relevant information within a local database historian.

It is important to remember that this server should not be in the same location as the manufacturing points, where the only condition to be met is the existence of an Internet connection. In this way, OPC_UA_AT servers from the manufacturing points are in fact clients of the OPC_UA_HDA_AT server. Fig. 5 also illustrates the way in which the shared database is developed: for each reseller, the database is shared to all distribution points and central server.

Each warehouse is provided with a server, on which an OPC_UA_AT server runs; this server also represents a client of OPC_UA_HDA_AT associated to each producer, in order

to require necessary data for authentication. The manufacturer's server will also receive information about input of products, storing conditions or exit of products from warehouses. In what concerns the retail dealers, a PDA with an RFID reader can be used, on which a client of OPC_UA_HDA_AT servers runs. These servers are clients for OPC_UA_AT manufacturers' servers and can be used in order to authenticate products.

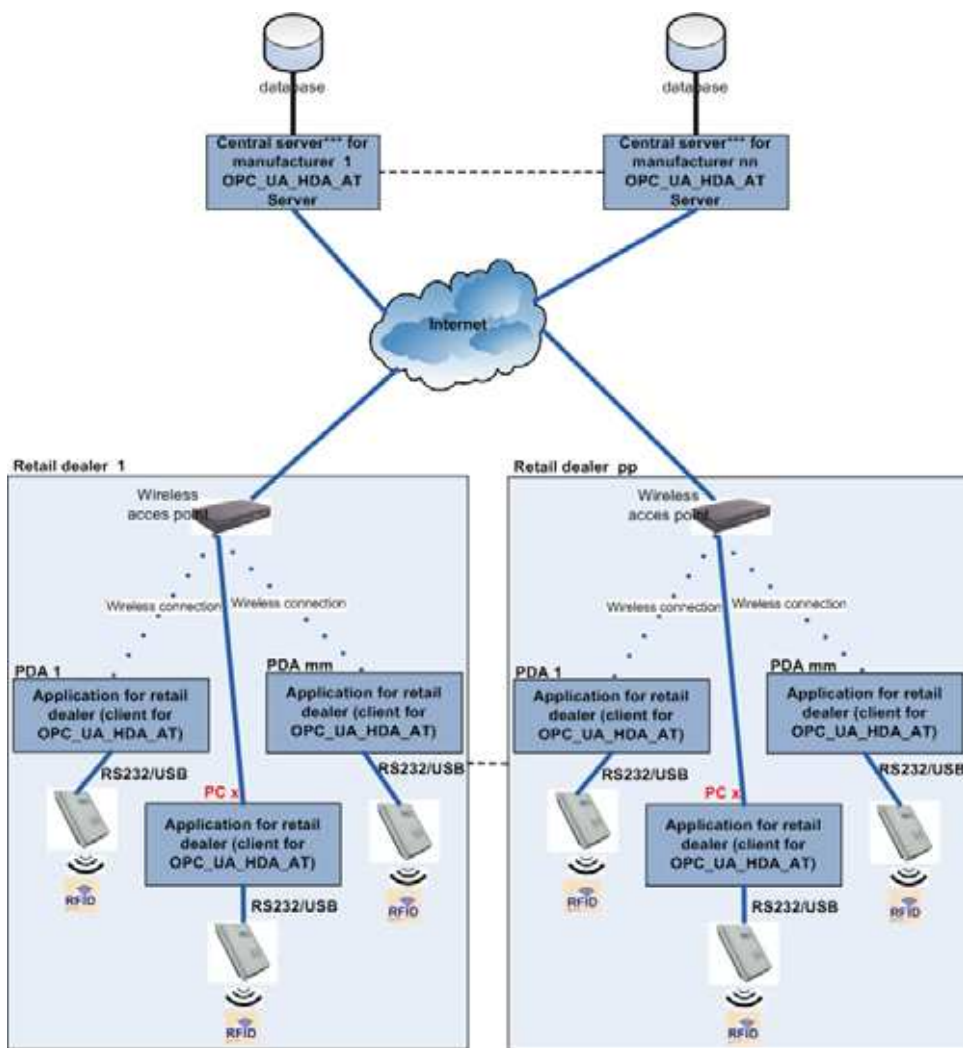


Fig. 6. ATPROD system seen from the perspective of a retail dealer

A client from a warehouse or retail dealer can send an authentication request to the manufacturer's servers (central or local). If the needed information cannot be found within the central database server associated to the manufacturer, this will require data from a server existing in the manufacturing point. After information is achieved, it is sent to the client which has required it, in order for the client to identify products. Using such mechanism, information existing within the shared database related to the tagged products can be freely accessed.

As can be seen in Fig. 5, the shared database between manufacturers' local servers and the central servers is illustrated in red color. For each point, a SQL database server is set up. OPC_UA_AT and OPC_UA_HDA_AT servers can access the local database by means of SQL commands.

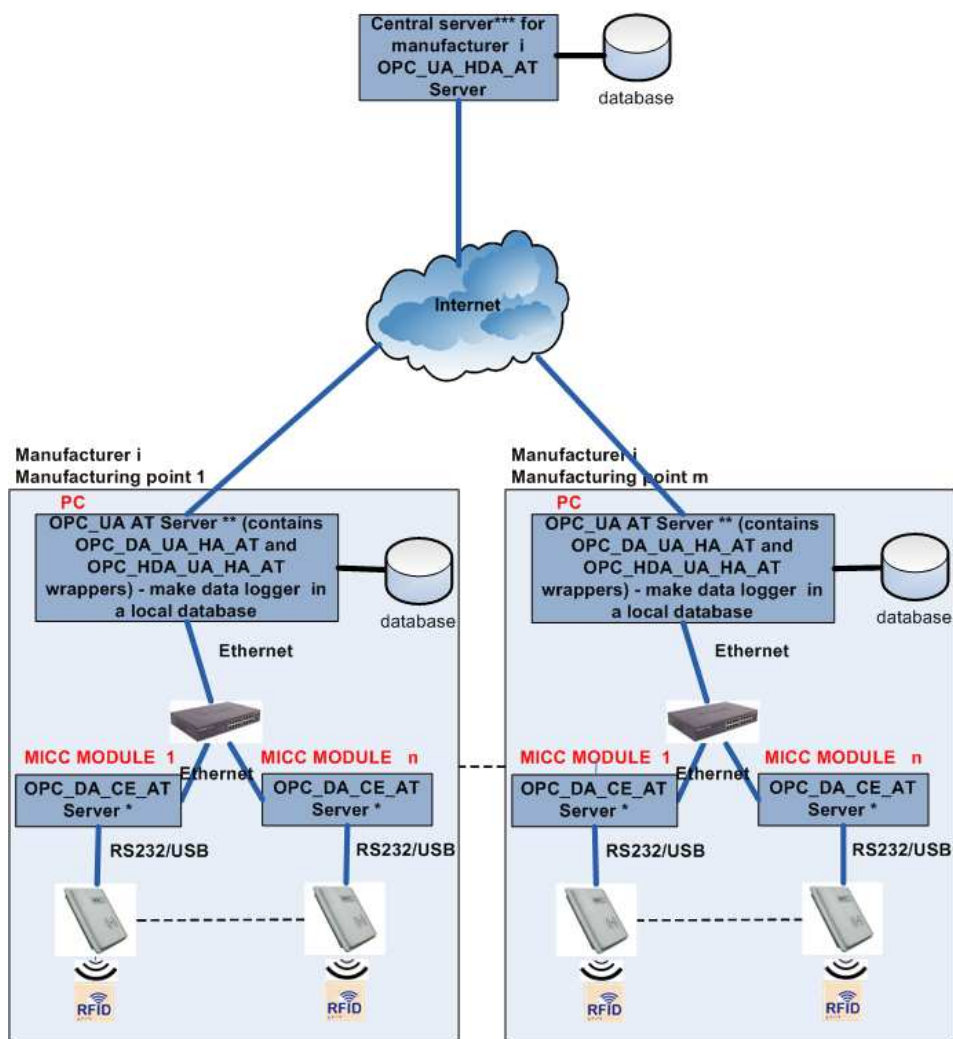
Fig. 6 emphasizes the way a shared database can be accessed by dealers. Therefore, one or several PDA or tag-reading PCs can be provided for each dealer. It is very important that PDA devices and PCs used for authentication should be connected to the Internet, so as to make possible the access to the manufacturers' servers. If the Internet connection of a manufacturer associated server does not work properly, the authentication of products will not be accomplished. On such computing systems, an OPC client application runs for OPC_UA_HDA_AT servers associated to each manufacturer. When a product is sold, the client application requires information from the manufacturer's server in relation to the authentication of that product.

The requested information is sent to client application, and the authentication of product is carried out. After authentication, information concerning the selling of product is sent back to the manufacturer's server.

Information concerning the selling of products is not erased from the database. By means of client application, the database administrator will be able to carry out erasing operations related to products sold or to create an archive with this information (for each manufacturer) that users can use at a later time.

Operationally, servers within ATPROD system are placed in two different locations: at manufacturers and in warehouses. Fig. 7 illustrates the structure of servers, as seen from the manufacturer's perspective.

There are several RFID tagging points at each manufacturing point, and several MICC modules connected to RFID readers. The OPC servers running at these points are assigned as OPC_DA_CE_AT and their presence is justified by the necessity to label all products that exit the production line. Since MICC module should work both online and offline, a historian OPC server can also run on it; therefore, a historian will be carried out for data that should have been sent on network, but cannot be transmitted when the connection with the server is no longer active at the level of manufacturing points. OPC_UA_AT server existing at the manufacturing point level includes OPC_DA_UA_AT and OPC_HDA_UA_AT wrapper, so as to connect to OPC_DA_AT and OPC_HDA_AT servers on MICC modules. This server stores a historian with all operations performed at the manufacturing point. The central server OPC_UA_HDA_AT from the manufacturer's level should also be a client of the OPC_UA_AT servers, at the level of manufacturing points, so as to require the necessary data. However, such data is not stored within the central server database, but within the database of manufacturing points. OPC_UA_AT servers can be replaced with OPC_NET3.0_AT servers that use WCF (Windows Communication Foundation) technology.



* It can include an OPC_HDA_CE server
 ** It can be OPC_NET3.0_AT server or it can include an OPC_NET_3.0_DA_XI_AT wrapper
 *** It can be PC_NET3.0_HDA_AT server or it can include an OPC_NET_3.0_DA_XI_AT wrapper.

Fig. 7. Placing of servers to the manufacturer site

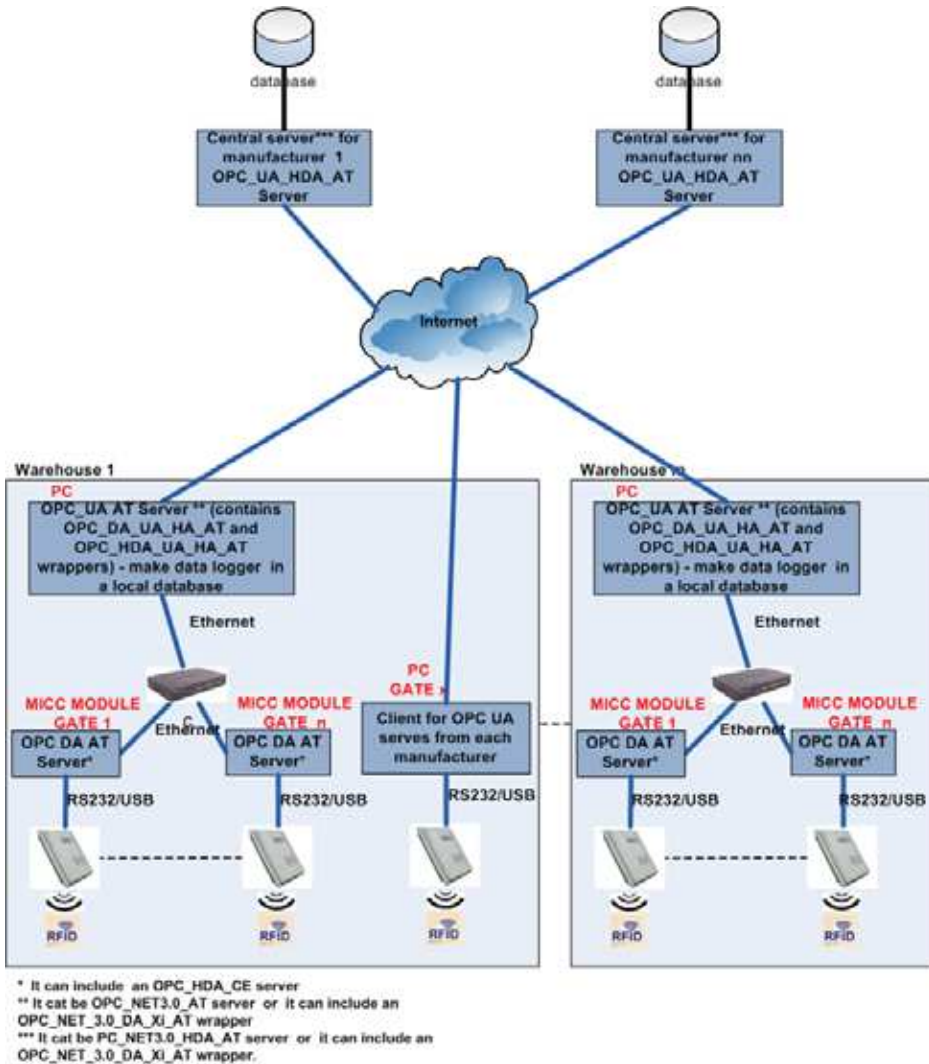


Fig. 8. Placing of servers to warehouses' site

Fig. 8 emphasizes the architecture of servers as regards the warehouses. One might see that here, at the level of each system's gate, there is a MICC module. Such a module is provided with an RFID reader, connected by RS232 serial port or USB port, in order to read/ write information from RFID labels. This module runs OPC-DA-CE-AT and OPC-HDA-CE-AT servers. An OPC-UA-AT server runs on a server at the warehouse level. This server is a client of OPC-DA-CE-AT and OPC-HDA-CE-AT from MICC modules. This fact is accomplished by including the OPC-DA-UA-AT and OPC-HDA-UA-AT wrappers. In order to achieve the information necessary to product authentication, this server signifies a client of the servers existing at manufacturers' level. Any input or output of products from

the warehouse will be sent to manufacturers' servers. In case of small distribution chains, OPC-UA servers can be replaced with OPC_NET3.0_AT servers that use the WCF (Windows Communication Foundation) technology.

Up to the present, six types of servers have been identified: OPC_DA_CE_AT, OPC_HDA_CE_AT, OPC-UA_AT, OPC_DA-UA_AT, OPC-UA_HDA_AT, OPC_NET3.0_AT.

OPC_DA_CE_AT runs on MICC modules, specific to manufactures and warehouses. This server includes a driver for the communication with RFID reader. Such a server should run on WINDOWS CE 6.0 operating system. OPC_HDA_CE_AT runs on MICC modules, specific to manufacturers and warehouses. This server is a client of OPC_DA_CE_AT server and will carry out a history if the local connection is interrupted. The server should run on WINDOWS CE 6.0 operating system. OPC-UA_AT runs at the level of manufacturing points and warehouses. It is a client of OPC_DA_CE_AT and OPC_HDA_CE_AT servers, including the OPC_DA-UA_AT and OPC_HDA-UA_AT wrappers. This is also a client of OPC-UA_HDA_AT servers, at the level of manufacturers. OPC-UA_HDA_AT runs at the level of manufacturing points and centralizes all data corresponding to products circulating within the distribution chain. OPC_NET3.0_AT- emphasizes an alternative of OPC-UA_AT and OPC-UA_HDA_AT servers.

7. Software architecture of the MICC module

MICC module is connected by means of RS232 or USB ports to a RFID reader/ writer, using 13.56 MHz frequency band and ISO 15693 standard. This module should allow the reading or writing of information on RFID tags.

One should mention that products can use two types of RFID tags: standard self-adhesive RFID tags, 13.56 frequency band, ISO 15693, variable memory (I code SLI – 896 bits, Tag-it TM HF-I - 2048 bits) and RFID tags of types: flexible card, self-adhesive, active, 13.56 MHz frequency band, ISO 15693, provided with integrated temperature sensor and temperature values history, Variosens model made by KSW Microtec, 8kbits EEPROM, which can store 1 720 values of 10 bits temperature values. All products have tags attached to them, mostly of them of first class mentioned above; those products that need special conditions of warehousing and transport can also have attached RFID tags of the second type.

Operationally, the MICC device should meet the following requirements: reading of information from RFID tags; setting up the tags so as to establish the sampling rate; if necessary, reading the temperature and storing its value into RFID tag's memory; storing of information read from RFID tag into its own memory; sending data to central server by means of Ethernet; possibility of both on-line and off-line operations.

Fig. 9 illustrates the position of MICC module within ATPROD system. Therefore, it is placed at the input or exit of a warehouse. In what concerns the input, the MICC device reads the RFID tags attached to products that enter warehouses, sends the information read to the central server, accomplishes the authentication of products (by comparing information from tags to information existing within manufacturer's server), and writes the information related to the input on RFID tag. When products have attached RFID tags provided with temperature sensors, the MICC module reads the history of temperatures and deletes this history from RFID tag.

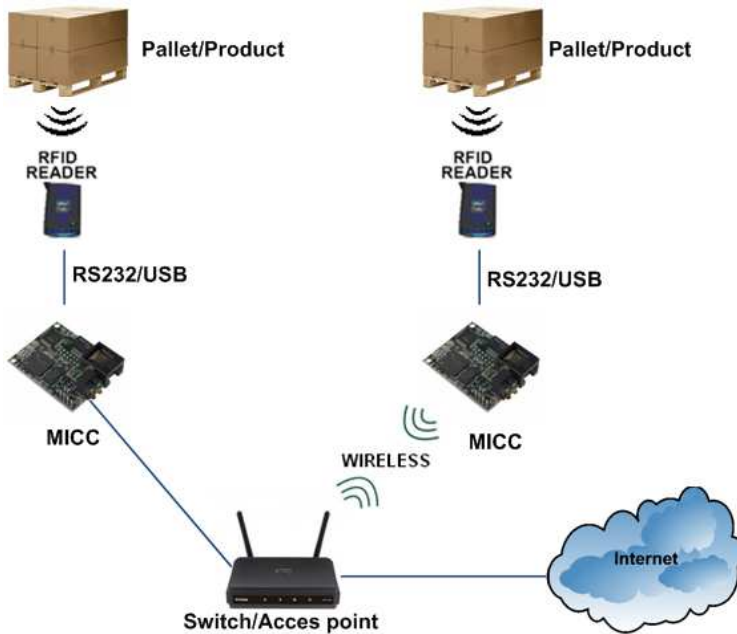


Fig. 9. MICC module operating mode

Fig. 10 also shows the UML diagram with a view to using the MICC module. From this diagram, the main two operations carried out in this module can be identified, as follows: reading of information from RFID tag, as well as writing of information on this RFID tag.

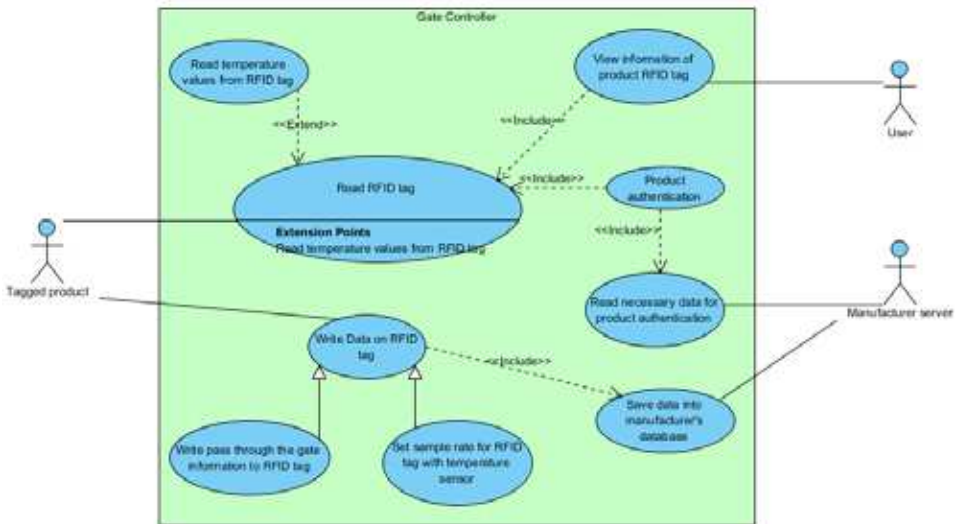


Fig. 10. UML diagram of using MICC module

Reading of information from RFID tag is done depending upon RFID tag's type (with or without temperature sensor). The operation of product authentication is carried out after reading information from RFID tag, and includes the connection to the manufacturer's server, the reading of information from this server about products, and finally a comparison between this information and that provided on RFID tags. Due to this procedure, authentication of products can be performed only if the module is provided with direct connection to manufacturers' servers.

As previously stated, data writing is performed depending upon the RFID tag under use. If an RFID tag provided with temperature sensor is used, then the sampling rate can be set up in order to save temperature values, and to empty the memory after reading the information included on RFID tag. If a classical tag is used, that is, without temperature sensor, then the tag will be written with information concerning the input or exit in or from warehouse, input/ exit date, warehouse code, etc.

The application running on MICC device will be further developed in C++, under an OPC server type, able to communicate with the RFID by means of RS232 or USB. The application will be developed by using SDK package, performed after creating an image on Windows CE 6.0 (Samuel, 2008).

8. Conclusion

RFID will have significant impacts on the economy as well as on the operational and financial performance of companies in the focus areas: productivity, employment, markets, goods and services, and innovations and new products. RFID will especially generate significant impacts in applications with a unique selling proposition, e.g. anti-counterfeiting, secure supply chains, and cold chain and quality monitoring, as well as better information for decision makers.

This chapter proposes an RFID-based system to track, at the item level, material flows among partners until they reach the consumer, while maintaining data accuracy. The presented system helps small, medium companies and enterprise organizations to improve productivity and provide better service to their customers. Thus, our system has the potential of helping retailers provide the right product at the right place at the right time, allowing maximizing sales and profits.

The system is still under construction and in the near future some security aspects will also be taken into consideration.

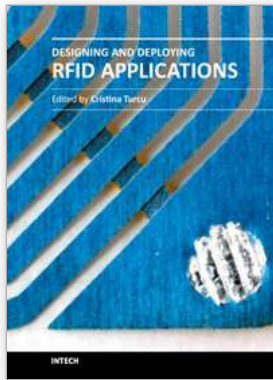
9. Acknowledgment

This work was supported by the project "Computer system for controlling and checking the authenticity of products - ATPROD" - Contract no. 12082/ 2008, project co-funded by 2007-2013 PNCDI Program.

10. References

- Barr, M., (2007). *Embedded Systems Glossary*, Available at <http://www.netrino.com/Embedded-Systems/Glossary>
- Chalasanani, S.; Boppana, R.V.; Sounderpandian, J (2005). RFID Tag Reader Designs for Retail Store Applications, *AMCIS 2005 Proceedings*, Paper 149, Available at <http://aisel.aisnet.org/amcis2005/149>

- Gaitan, N. C.; Gaitan, V. G.; Pentiu, S. G.; Ungurean, I.; Dodi, E. (2010). Middleware based model of heterogeneous systems for scada distributed applications, *Advances in Electrical and Computer Engineering*. Vol.10, No.2, pp. 121-124, ISSN: 1582-7445
- Lange, J.; Iwanitz F.; Burke, T.J (2010). *OPC - From Data Access to Unified Architecture*, fourth edition, revised and extended, 431 pages, ISBN 978-3-8007-3242-5
- Mahnke, W.; Leitner, S.H.; Damm, M. (2009). *OPC Unified Architecture*, Springer; 1 edition (May 4, 2009), ISBN: 978-3-540-68898-3
- Preradovic, S.; Karmakar, N.C.; Balbin I. (2008). RFID Transponders, *IEEE MICROWAVE MAGAZINE*, Vol. 9, No. 5, pp. 90-103, ISSN: 1527-3342
- Samuel P.(2008). *Professional Microsoft Windows Embedded CE 6.0*, Wrox; New edition (November 3, 2008), ISBN: 978-0470377338 **a (2008). *A Summary of RFID Standards, RFID Journal*, Available at: <http://www.rfidjournal.com/article/view/1335/1/129> **a (2010). *Vortex86 System-On-Chip (SoC)*, Available at <http://www.vortex86sx.com/> **b (2010). *DMP Electronics INC.*, Available at <http://www.dmp.com.tw/>



Designing and Deploying RFID Applications

Edited by Dr. Cristina Turcu

ISBN 978-953-307-265-4

Hard cover, 384 pages

Publisher InTech

Published online 15, June, 2011

Published in print edition June, 2011

Radio Frequency Identification (RFID), a method of remotely storing and receiving data using devices called RFID tags, brings many real business benefits to today world's organizations. Over the years, RFID research has resulted in many concrete achievements and also contributed to the creation of communities that bring scientists and engineers together with users. This book includes valuable research studies of the experienced scientists in the field of RFID, including most recent developments. The book offers new insights, solutions and ideas for the design of efficient RFID architectures and applications. While not pretending to be comprehensive, its wide coverage may be appropriate not only for RFID novices, but also for engineers, researchers, industry personnel, and all possible candidates to produce new and valuable results in RFID domain.

How to reference

In order to correctly reference this scholarly work, feel free to copy and paste the following:

Ioan Ungurean, Cornel Turcu, Vasile Gaitan and Valentin Popa (2011). An RFID-Based Anti-Counterfeiting Track and Trace Solution, *Designing and Deploying RFID Applications*, Dr. Cristina Turcu (Ed.), ISBN: 978-953-307-265-4, InTech, Available from: <http://www.intechopen.com/books/designing-and-deploying-rfid-applications/an-rfid-based-anti-counterfeiting-track-and-trace-solution>

INTECH

open science | open minds

InTech Europe

University Campus STeP Ri
Slavka Krautzeka 83/A
51000 Rijeka, Croatia
Phone: +385 (51) 770 447
Fax: +385 (51) 686 166
www.intechopen.com

InTech China

Unit 405, Office Block, Hotel Equatorial Shanghai
No.65, Yan An Road (West), Shanghai, 200040, China
中国上海市延安西路65号上海国际贵都大饭店办公楼405单元
Phone: +86-21-62489820
Fax: +86-21-62489821

© 2011 The Author(s). Licensee IntechOpen. This chapter is distributed under the terms of the [Creative Commons Attribution-NonCommercial-ShareAlike-3.0 License](#), which permits use, distribution and reproduction for non-commercial purposes, provided the original is properly cited and derivative works building on this content are distributed under the same license.