"Vasile Alecsandri" University of Bacău
Faculty of Sciences
Scientific Studies and Research
Series Mathematics and Informatics
Vol. 19 (2009), No. 2, 21 - 36

CONTROLS FOR RFID IN SUPPLY CHAIN PROCESSES AUDIT

CRISTIAN AMANCEI and BOGDAN AMANCEI

Abstract. The increasing use Radio Frequency Identification (RFID) systems to provide real-time visibility of inventory from the point of manufacture to the point of sale expand the capabilities of organizations by enabling companies to achieve a greater visibility and flexibility in their supply chain processes. This environment requires the auditor to identify the associated risks and the controls that mitigate those risks, in order to help the organization to provide certified services in collaboration with their partners. In addition, this paper presents aspects of the audit mission for RFID systems in supply chain processes.

1. CHARACTERISTICS OF RFID SYSTEMS

RFID is emerging as a premier technology for automating the identification and tracking of commodities and collecting valuable information on their contents, physical state and more. Organizations in Supply Chain, Retail, Transportation, Healthcare and other industries are increasingly employing RFID technology to bring new efficiencies to supply chains, track assets, ensure product quality and consumer safety, protect the integrity of their brands, promote security and more[7].

RFID has proven to be an effective technology for allowing companies to track inventory in the supply chain from the point of receipt back to suppliers. Supply chain RFID provides real-time, highly accurate inventory visibility enabling the following improvements in sales and operations:

- Shorter more accurate cycle-counts
- Reduced out-of-stocks
- Improved merchandising effectiveness

Keywords and phrases: RFID, supply chain, logistics, audit, controls Characteristics of RFID Systems
(2000) Mathematics Subject Classification: 68M15

- Improved service level attainment
- Higher inventory turns
- Reduced product loss
- Improved route optimization
- Expired product removal
- Shorter invoice-to-cash cycles

RFID is evolving enabling innovative functionality in a variety of environments and applications [9]:

- Law firms and courts are using RFID tags to track the movement and increase the security of critical and / or private Intellectual Property (IP)
- Retailers are equipping shopping carts with mobile RFID tag readers, to help shoppers navigate through stores more quickly and to deliver real-time promotions linked to shopper preferences
- Businesses are increasingly tagging IT assets such as laptops and server blades with RFID technology to improve business continuity, disaster recovery, IP security, and regulatory compliance

A RFID system has several components including chips, tags, readers and antennas. In its simplest form, a small silicon chip is attached to a small flexible antenna to create a tag. The chip is used to record and store information. When a tag is to be read, the reader (which also uses an antenna) sends it a radio signal. The tag absorbs some of the RF energy from the reader signal and reflects it back as a return signal delivering information from the tag's memory [6].

RFID systems communicate using frequencies around 900MHz with a maximum read range of 10 meters under ideal conditions. This makes RFID a promising solution for reading pallets and cartons off of conveyors or in portals from a distance. But this capability does not in any way preclude RFID from near field and near contact applications as RFID systems can be easily tailored to meet lower range requirements. This can be accomplished by reducing power at the reader, reducing the size of the reader antenna, and/or reducing the size of the tag antenna [10].

RFID tags are designed and produced in a variety of shapes and sizes, dependent on application requirements. As RFID has a large maximum read range to begin with, using extremely small tags for such applications as near field item level tracking (where tags may reside under bottles caps or behind product labels, for example) is promising. Applications such as pallet or case level tracking of commodities on conveyors or passing through portals, and read from a distance typically require larger tags [10].

RFID readers are generally composed of a computer and a radio. The computer manages communications with the network, allowing tag data to be communicated to enterprise software applications such as ERP systems. The radio controls communication with the tag, typically using a language dictated by a published protocol such as the EPC Class 1 specification. This particular protocol, one of several in use, is the most common language used by tags in supply chain applications [10].

RFID helps organizations to address the changeless of managing inventory through supply chain. For the changeless that are addressed through this technology refer to the table below:

TABLE I. CHALLENGES OF MANAGING INVENTORY THROUGH THE SUPPLY CHAIN

Challenge	Business Impacts
Manual Cycle-counts	- Increased labor expense - Less time spent selling to / servicing accounts - Less accurate counts / invoicing - Less accurate forecasting - Longer invoice-to-cash cycles
Out-of-Stocks	- Lost revenue - Brand dilution - Lower customer satisfaction / service level attainment - High delivery expenses
Shrinkage	- Higher product costs - Billing inaccuracies
Low Inventory Turns	- Higher working capital requirements - Higher carrying costs - More write-downs/write-offs - Lower return on assets
Product Expiration / Recalls	- Higher safety risks - Increased legal liability - High warranty costs - Negative customer experience

2. IMPLEMENTATION ON SMALL MEDIUM ENTERPRISES (SME)

New developments tend to significantly lower SME entry costs for RFID technology, through developing and providing a lightweight, royalty-free, innovative, programmable, privacy friendly, middleware platform that will facilitate low-cost development and deployment of innovative RFID solutions. This platform will act as a main vehicle for realizing the proposed swift in the current RFID deployment paradigm.

Portions (for example specific libraries) of the middleware application will be hosted and run on low-cost RFID-enabled microelectronic systems, in order to further lower the total cost ownership (TCO) in mobility scenarios (for example mobile warehouses, trucks)[5].

A. *Privacy Protection and Privacy Friendliness*

The principles of privacy protection and privacy-friendliness will be incorporated in the logic of the middleware. The specific principles are:

- Removing data unnecessary for the business (for example tags identities after the object has been sold).
- Separation of personal data and object data (for example different databases and/or different transactions).
- Establishment of certification programs to verify compliance for example through independent auditing of the RFID infrastructure and middleware.
- Establishment of guidelines for adopters, with special focus on SMEs. These guidelines will cover not only technical aspects associated with consumer privacy, but also recommended business procedures to maximize privacy-friendliness.
- Creation of a "seal" to provide adopters with a marketing tool to promote the advantages of their privacy-friendliness.

B. *Ubiquitous Added-Value Sensing and Low-Cost Readers*

A primary focus of the added-value sensing activities will be the new generation of battery-assisted RFID-tags that incorporate physical sensors, such as temperature, humidity, pressure and acceleration meters [11].

These sensors have been proven extremely beneficial in a variety of business cases, for example, where the position of tagged merchandise and its physical conditions are of extreme important.

Nevertheless, these sensors are up-to-date voluminous and expensive to facilitate common business cases, involving large amounts of low-cost tagged items.

C. *Applications and Scenarios*

The ease of development and cost-effectiveness enabled by the platform will be manifested across different application domains, such as [12]:

- Cold Chain Management for food and diary products.
- Asset Management for Pharmaceuticals.
- Product Packaging, Tracking and Traceability.
- Health care.
- Pharmaceutical.

The developments of the new systems will be validated in the scope of Pilot Trials involving European SMEs. Innovative RFID scenarios showcase and pilots will be built around the following axes:

- Fully automated reading and processing functionality. Applications will run without human intervention.
- Mobility scenarios involving several mobile warehouses in the scope of the supply chain.
- Measurement of added-value parameters such as temperature, humidity or pressure.

D. *Pilots objectives*

In relation to the overall objectives of the project, the objectives of the pilots will in general be the following [12]:

1) To verify that the developed middleware is programmable to be used by SMEs (e.g., health, food, industry...).

2) To verify ease of deployment of Middleware software on SMEs IT infrastructure, on low-cost hardware (i.e. to validate the lightweight nature of the middleware).

3) To verify that the middleware software is able to work with 500 RFID tag detections but also with 500 000 tag detections (Scalability).

4) To verify the middleware software is easy to use (based on feed back from the SMEs regarding the programmability and the difficulties to use the middleware).

5) To verify that the use of RFID and middleware software results in true really cost savings for SMEs.

6) To verify that the middleware software can be effectively adapted for mobility RFID solutions with low-cost (significant lower than the cost required today).

3. AUDIT MISSION FOR RFID IN SUPPLY CHAIN PROCESSES

The goal of the audit mission is to obtain a reasonable assurance concerning the deployment and the operating of the RFID systems, in accordance with the appropriate rules and settlements (regulations), and with specific security standards [1].

The following steps are essential to be performed for the audit process itself:

7) Define the physical scope of the audit: The audit team should define the security perimeter within which the audit will take place. The perimeter may be physically organized around logical asset groups such as a datacenter specific or around business processes such as sales operations. The physical scope of the audit allows the auditors to focus on assets, processes, and policies in a manageable fashion.

8) Define the process scope of the audit: This document describes how to effectively scope the supply chain processes or areas that should be included in an audit. It is critical that any business, regardless of size, put limits on the supply chain processes or areas that will be the focus of the audit.

9) Conduct historical due diligence: An oft-forgotten step in the audit process is pre-audit due diligence. This due diligence should focus on historical events such as known vulnerabilities, damage-causing security incidents, as well as recent changes to IT infrastructure and business processes. It should include an assessment of past audits, paying attention to the results of penetration test if any. Furthermore, auditors should compile a complete inventory of the assets located within the physical scope of the audit and a complete list of specified controls relevant to those assets.

10) Develop the audit plan: An effective audit is almost always guided by a detailed audit plan that provides a specific project plan for conducting the audit. This should include a specific description of the scope of the audit, critical dates/milestones, participants, and dependencies.

11) Perform security risk assessment: Once the audit team has an effective plan in place, they can begin the core of the audit – the risk assessment. The risk assessment should cover the following [3]:

- Identify and locate the exact assets that are used by the RFID in supply chain and prioritize those assets according to value to the business. For example, a cluster of web servers supporting the sales order entry application is more important than a web server supporting the IT department’s incident list.
- Identify potential threats against the assets covered by the audit. The definition of a threat is something that has the potential to exploit vulnerability in an asset.

- Catalog vulnerabilities or deficiencies for each asset class or application layer. Vulnerabilities exist for specific types of assets and present opportunities for threats to create risk.
- Identify the controls currently in place for each asset class or application layer. These controls must exist and be used on a regular basis. Anything short of this should be noted and not counted towards existing controls. Controls include technologies such as IDS, processes such as data backup procedures, and personnel such as the systems administrator that manages the relevant assets.
- Determine probabilities of specific risks. Audit teams must make a qualitative assessment of how likely it is that each threat/vulnerability will occur for a specific asset class or application layer. The probability calculation should account for the ability of existing controls to mitigate risk and it will be evaluated on a numerical scale.
- Determine the potential harm or impact of a threat. Auditors must again make a qualitative assessment of the likely extent of the harm for a specific asset class or application layer and it will be represented on a numerical scale.
- Perform the risk calculation. These calculations should be performed on an asset class / application layer basis and will yield a priority list for risk mitigation efforts and specific controls that need to be implemented.

12) Document the results of the audit in detail and proactively presented to decision makers for review. The document should include an executive summary, audit determinations, required updates/corrections, and supporting data in the form of exhibits.

13) Specify and implement new/updated controls: The ultimate benefit of an audit is that it should yield specific recommendations for improving business processes that involves RFID in supply chain. These recommendations should take the form of controls that the business can adopt, the deadline for adoption, and the party responsible for adoption [4].

4. RISKS FOR RFID SYSTEMS

RFID technology enables an organization to significantly change its business processes to [13]:

- Increase its efficiency, which results in lower costs,
- Increase its effectiveness, which improves mission performance and makes the implementing organization more resilient and better able to assign accountability, and

- Respond to customer requirements to use RFID technology to support supply chains and other applications.

The RFID technology itself is complex, combining a number of different computing and communications technologies to achieve the desired objectives. Unfortunately, both change and complexity generate risk. For RFID implementations to be successful, organizations need to effectively manage that risk, which requires an understanding of its sources and its potential characteristics.

We have extracted from current methodologies for risk and control identification [2] the most important risk areas:

- **Process Risk** - Attacks on RFID system components could affect business processes the RFID system was designed to enable.
- **Business Risk** - Competition could gain unauthorized access to RFID generated information and use it to gain competitive advantage over the organization implementing the RFID system.
- **Privacy Risk** - Personal privacy rights may be compromised if an RFID system uses what is considered personally identifiable information for a purpose other than originally intended.
- **External Risk** - RFID technology potentially could represent a threat to non-RFID systems, assets, and people.

E. *Process Risk*

RFID systems typically are implemented to replace or enhance a paper or partially automated process. Organizations implementing RFID systems could become reliant on those systems, which if not implemented properly with business continuity planning might be less resilient to disruptions than the systems they replace. Considering the following example, the situation in which the organization replaces its paper-based inventory management system from the warehouse with an RFID-enabled system. The paper system involves storing completed forms at the warehouse and sending form duplicates to a central office, while the new RFID system locates its database servers at a single computing center. In this environment, the paper system might be more resilient to a local disaster than the RFID system, despite the increased efficiency, accuracy, or effectiveness of the RFID-enabled business process.

Failure of any component or subsystem of the RFID system could result in system wide failure. In the above example, system wide failure might result from many causes, such as loss of the network connection between the warehouse and the computing center, a software virus that disables critical functionalities, or a new source of radio interference that prevents readers from accurately reading tags. Due to these situations the RFID system may become unavailable, and then the potential impacts can range from slowing the business process to the loss of critical operational records. If the system is mission critical, then the system should appropriately classify and the inclusion in the business continuity plan is mandatory.

By having the system included in the business continuity plan appropriate risks will be addressed by developing measures that will reduce the impact or will create alternative solutions that mitigate the risk.

F. *Business Risk*

RFID is a powerful technology, in part, because it supports wireless remote access to information about assets that either previously did not exist or was difficult to create or dynamically maintain. While this access is a significant benefit, it also creates a risk that unauthorized parties could also have similar access to that information if proper controls are not in place.

A competitor can gain information from the RFID system in a number of ways, including eavesdropping on RF links between readers and tags, performing independent queries on tags to obtain relevant data, and obtaining unauthorized access to the database server that stores the information about tagged items. Supply chain applications may be particularly vulnerable to this risk because a variety of external entities may have read access to the tags or related databases.

In some cases, the information may trigger an immediate response. For example, someone might use a reader to determine whether a shipping container holds expensive electronic equipment, and plans a theft on that container after receiving the information.

In other cases, data might also be aggregated over time to provide a complete image over the organization’s operations, business strategy, or proprietary methods. For instance, monitoring activities could be performed on the number of tags entering a facility to provide information of its business growth or operating practices. In this case, if someone determined that a warehouse recently received a number of very large orders, then it could determine that the operator might manipulate the market and take action in order to profit from this situation by requesting large discounts.

G. *Privacy Risk*

RFID technology raises several important privacy concerns. One concern is that organizations may collect personal information for a particular purpose, such as to complete a financial transaction or grant an individual access to a facility, and then later use that information for a different purpose that the individual finds undesirable, such as to conduct a direct marketing campaign, or the potential unintentional disclosure of personal information to unauthorized third parties.

There are privacy risks from the perspective of the individual and from the perspective of the organization implementing RFID technology. The privacy risk from the perspective of the individual is the unauthorized revelation of personal information and the personal consequences of that breach. The privacy risk from the perspective of the implementing organization might include:

- Penalties if the organization does not comply with privacy laws and regulations,
- Customer avoidance because of real or perceived privacy concerns about RFID technology,
- Being held legally liable for any consequences of the weak privacy protections.

Business objectives often conflict with privacy objectives. Organizations can benefit from the analysis and sharing of personal information obtained with RFID technology. For example, consumers may want tags to be disabled at point-of-sale so that they cannot be used for tracking purposes afterwards. However, if it is easy to disable a tag at point-of-sale, then it may also be easier for adversaries to disable tags prior to point-of-sale, altering the business process and allowing theft. Moreover, organizations may want to use tags after point-of-sale for reverse logistics operations (post-sale support, recalls, and other purposes).

H. *External Risk*

RFID systems typically are not isolated from other systems and assets in the enterprise. Every connection point between the RFID system and something outside the RFID system represents a potential vulnerability for the entity on the other side of the connection, whether that is an application process, a valued asset, or a person. External risks are present for both the RF and enterprise subsystems of an RFID system. The main external risks for the RF subsystem are hazards resulting from electromagnetic radiation, which could possibly range from adverse human health effects to ignition of combustible material, such as fuel or ordnance. The main external risk for the enterprise subsystem is successful computer network attacks on networked devices and applications. The impact of computer network attacks can range from performance degradation to complete compromise of a mission-critical application.

These risk areas have a great impact on the organization operations and the organization image. Not being able to appropriately manage these risks could involve large range of impaction for the company: starting from theft and loss of products, to large system failure (2-3 business days) and loss of market share due to reputation being affected.

5. CONTROLS FOR RFID SYSTEMS

The RFID security controls are divided into three groups:

- **Management** - A management control involves oversight of the security of the RFID system. For example, the management of an organization might need to update existing policies to address RFID implementations, such as security controls needed for an RF subsystem.
- **Operational** - An operational control involves the actions performed on a daily basis by the system's administrators and users. For example, RFID systems need operational controls that ensure the physical security of the systems and their correct use.
- **Technical** - A technical control uses technology to monitor or restrict the actions that can be performed within the system. RFID systems need technical controls for several reasons such as protecting data on tags, errors processing procedures, causing tags to self-destruct, and protecting wireless communications.

I. Management Controls

Management controls are typically involved in risk assessment, system planning, and system acquisition, as well as security certifications, accreditations, and assessments, according to best practices politics. Example of controls according to RFID security best practices and control methodologies [8],[2]:

- **RFID usage policy** that describes the authorized and unauthorized uses of RFID technology in an organization and the personnel roles assigned to particular RFID system tasks;
- **IT security policies** for RFID systems should address:

- Access control to RFID information, especially records contained in the databases server;
- Perimeter protection, including port and protocol restrictions for network traffic between the RF and enterprise subsystems and between the enterprise subsystem and a public network or extranet;
- Password management, particularly with respect to the generation, distribution, and storage of tags' access, *lock*, and *kill* passwords;
- Management system security for readers and middleware, including the use and protection of SNMP read and write community strings;
- RFID security training for system administrators and operators;

- Development of policies and procedures that addresses the appropriate use of information and systems;
- Management of associated cryptographic systems, including certification authorities and key management.

- **Minimizing Sensitive Data Stored on Tags - i**nstead of placing sensitive data on tags, the data could be stored in a secure enterprise subsystem and retrieved using the tag's unique identifier.

J. *Operational Controls*

Types of operational controls:

- Physical access controls restrict access to authorized personnel where the RFID systems are deployed.
- Proper placement of RF equipment helps avoid interference and reduce hazards from electromagnetic radiation.
- Organizations can destroy tags after they are no longer useful to prevent competition from gaining access to their data.
- Operator training can help ensure that personnel using the system follow appropriate guidelines and policies.
- Information labels and notice can inform users of the intended purposes of the RFID system and simple methods users can employ to mitigate risk.
- Periodic manual sample sized review of the information received through the RFID system is necessary in order to identify potential errors.

K. *Technical Controls*

The general types of controls include:

- Provide authentication and integrity services to RFID components and transactions,

While a wide variety of authentication methods exists for IT systems, the most common techniques for the RF subsystem of RFID systems are passwords, keyed-hash message authentication codes (HMAC), and digital signatures. In some cases, the primary objective of the authentication technology is to prevent unauthorized reading from or writing to tags. In other cases, the objective is to detect cloning of tags and passing of false information.

- Protect RF communication between reader and tag,

Several types of technical controls focus on the RF interface to tags, including: cover-coding to obscure the content of messages from readers to tags; data encryption before transmission; selection of operation radio frequency to avoid interferences from other sources; shielding to limit eavesdropping; interfaces for tags can be temporarily shut off to prevent unauthorized access.

- Protect the data stored on tags.

Technical controls currently available for protecting tag data include: tag memory access control, which can restrict use of tag commands and protect data stored in a tag's memory; encrypting the data on tags; kill features which can prevent subsequent unauthorized use of a tag.

6. METRICS FOR THE WAREHOUSE ACTIVITY

Implementation of a RFID system without the development of an appropriate system of metrics for monitoring the performance of the system is useless.

We propose the following 3 metrics to be measured before and after the implementation of the RFID system:

i. *Quantitative precision of the supplier* – the percent of products delivered by the supplier that is not according with the quantity order, compared with the total order. This metric is used to monitor the delivery performance of the supplier, from the quantity point of view. This metric should be computed monthly for each supplier. The price is being used in the formula in order to compare the results between the suppliers.

$$QPS_k = \frac{\sum_{i=1}^{N}(QO_{ik} - QR_{ik}) * P_{ik}}{\sum_{i=1}^{N} QO_{ik} * P_{ik}} * 100\%$$

where:

QPS_k – quantitative precision of the k supplier.
QR_{ik} – quantity received of i product from the k supplier.
QO_{ik} – quantity ordered of i product from the k supplier.
P_{ik} – price of i product for the k supplier.
N – total number of products.

The target value of this indicator is around 2% before the implementation of the RFID system. By using RFID tags the target value should decrease to the level of 1%.

ii. *Quality of order preparation in the warehouse* – the percent of products picked incorrect during order preparation from total orders. This metric is used to monitor the quality of the warehouse work. This metric should be computed weekly and monthly. The price is being used in the formula in order to compare the results during time.

$$QOP = \frac{\sum_{j=1}^{M} Q_j * P_j}{\sum_{i=1}^{N} Q_i * P_i} * 100\%$$

where:

QOP – quality of order preparation.
Q_i – quantity picked for delivery.
Q_j – quantity incorrect picked for delivery.
P – product price.
N – total number of orders picked in one week/month.
M – total number of orders incorrect picked in one week/month.

The target value of this indicator is around 3% before the implementation of the RFID system. By using RFID tags the target value should decrease to the level of 1%.

iii. *Total stock duration* – number of sales days covered by the current stock, without taking into consideration products with stock 0 from the last X days. The metric is usually computed Monday or in the first day of the month, by taking into consideration all the products.

$$TSD = \sum_{k=1}^{N} \frac{(\sum_{j=0}^{-X} EODS_{jk}) / X}{(\sum_{i=0}^{-Nd} Sd_{ik}) / Nd}$$

where:

TSD – total stock duration.
$EODS_{jk}$ – stock at the end of the day for k product.
Sd_{ik} – sales from one day for k product (current and previous days).
Nd – number of days during the week when the store is open.
X – number of days taken into consideration in order to compute the average stock from warehouse. Values: 0 –

taking into consideration the current day, Nd – taking into consideration the open days, 30 – for all the month.

N – total number of products taken into consideration.

The target value of this indicator is around 5 days before the implementation of the RFID system. By using RFID tags the target value should decrease to the level of 3 days due to better operation at the central warehouse level.

7. CONCLUSION

The impact of RFID systems in supply chain activities is increasing very fast. At the same time also the risks that come with the new technologies are increasing. In this environment the companies need to recognize the risks of RFID systems and to commit resources that will take decisive actions to control their vulnerabilities and to evaluate which countermeasures directly and cost-effectively reduce their highest risks.

Through this article we have extracted some important areas risks and suggested some controls to be implemented in order to mitigate the risks. A complete list of control is difficult to develop without having the specified the products type (low value, high value), the business type (production, distribution etc.) that will implement the system and the costs that the organization is willing to accept for additional controls.

An audit of the system implementation and operation is necessary to be performed in order to receive assurance that appropriate risks management care has been taken into consideration by the management.

The proposed metrics for the warehouse activity offer a base for monitoring the results obtained at the warehouse level after implementing the RFID system. At this moment we do not have results obtained from the implementation of such system in Romania. The market is waiting for results from other organizations in order to decide to invest in such implementation. The target values for the metrics have been obtained from the business plan constraints of implementing a RFID system.

References

[1] I. Ivan, G. Noşca and S. Capisizu, **Auditul sistemelor informatice**, ASE Printing House, Bucharest, 2005

[2] IT Governance Institute, *COBIT 4.1*, 2007

[3] M. Popa, F. Alecu and C. Amancei, **Characteristics of the Audit Process for Information Systems**, in *The Proceedings of the International Conference Competitiveness and European Integration – Business*

Information Systems & Collaborative Support Systems in Business, Cluj-Napoca, October 26 – 27, 2007, Risoprint Printing House, Cluj-Napoca, pp. 295 – 299

[4] T. Surcel and C. Amancei, **ERP System Audit a Control Support for Knowledge Management**, in *Economic Informatics Journal* , vol XII, No. 4(48), 2008, Inforec Publishing House, Bucharest

[5] **RFID and IT infrastructures: Maximizing Business Value**, Aberdeen Group, 2008

[6] J. M. Myerson, **RFID in the Supply Chain**, Auerbach Publications, 2006

[7] D. Blanchard, **Supply Chain Management – Best Practices**, John Wiley & Sons, 2007

[8] F. Thornton, B. Haines, A.M. Das, H. Barhava, A. Campbell, **RFID Security – Protect the Supply Chain**, Syngress Publishing

[9] download.microsoft.com/.../4205-RA-RFIDSolutionSelectionGuide2008-MED-11-spf.pdf

[10] http://www.imsrfid.com/faq.html

[11] ftp://ftp.cordis.europa.eu/.../futint-3-internet-of-things_en.pdf

[12] ftp://ftp.cordis.europa.eu/pub/fp7/ict/docs/futint-3-internet-of-things_en.pdf

[13] http://www.scielo.cl/pdf/jtaer/v3n2/art07.pdf

Cristian Amancei
Department of Computer Science in Economics
The Bucharest Academy of Economic Studies
Piata Romana 6, Bucharest, ROMANIA,
cristian.amancei@ie.ase.ro

Bogdan Amancei
The Bucharest Academy of Economic Studies
Piata Romana 6, Bucharest, ROMANIA,
b.amancei@yahoo.com