RFID FOR AUTOMATING ACCOUNTING PROCESSES IN LOG CABIN CONSTRUCTION

Valdis Pornieks [(a)], Egils Ginters[(b)], Gunārs Grundštoks[(c)]

[(a; b)] Sociotechnical Systems Engineering Institute
Vidzeme University College
4 Cesu Street, Valmiera LV-4200
LATVIA
[(c)] IT House, Ltd.
7/28 Rigas Street, Valmiera LV-4201
LATVIA

[(a)]valdis.pornieks@va.lv, [(b)]egils.ginters@va.lv, [(c)]gunars.grundstoks@ithouse.lv

ABSTRACT
RFID has the potential to significantly improve the accounting processes in log cabin construction, but before introduction a new technology to existing business processes it is necessary to analyse the risks and gains that are connected to it. A downside of RFID is the weak data protection capabilities that current solutions on the market offer; therefore a new accounting process model is provided that features non-standard security solutions.

Keywords: Radio Frequency Identification, RFID, Logistics, Data security, Log Cabins, Inventory.

1. INTRODUCTION

The accounting and management of log cabin building processes in Latvia is mostly handled manually. By reaching certain levels of building capacities the manual handling of material flow becomes too complex and time consuming. Especially as all materials (Logs) undergo multiple processing operations, which often is done by external companies. Thus there is the need for process automation to increase productivity and manageability of production.

It would be possible to use bar-codes for this purpose, but these have several limitations. Barcodes need to be scanned each separately which slows down the process of registering material movement. The fastest way would be to scan all logs simultaneously while moving through a gate. Another downside is that barcodes can not be rewritten which can be useful if data about each log needs to be changed because it has been processed and it is necessary to store data like measurements directly on the tag for quick access.

RFID is a promising technology that allows organizing accounting and material flow tracking in a fast and effective way, but it is necessary to determine if an RFID system is feasible in terms of economics and process organization.

Several companies like *Cambium-Forstbetriebe, (Germany*) are already using RFID for controlling timber freight movement which has allowed minimizing theft and material losses by up to 90% (Progress software 2007). In the U.S. RFID has found other application. It is used to fight smuggling of wood legally cut materials are marked with RFID tags so they can be uniquely identified, thus it is made difficult for smugglers to sell illegally cut materials as certified (Cooper 2007).

2. BUILDING LOG CABINS

The log cabin building process is similar in almost all companies. Generally there are four steps (See Figure 1): (i) acquiring materials, logs can be bought or cut by the company itself; (ii) processing of materials, before using logs for construction they have to be dried and shaved (often these are outsourced processes); (iii) assembling of the log cabin, the house is pre-built so the joints of the logs can be shaped to match each other; (iv) building at customers site, finally all the necessary materials are transported to the customers site and the log cabin is built. Logs with different lengths and widths are necessary for the building of log cabins, so it is necessary to have up-to-date information about the inventory. For this it is necessary to track (i) what materials have been acquired and what processing do they need (drying, shaving); (ii) what materials are being processed and when will they be ready; (iii) and of course what materials have been used for construction, for knowing what materials are left in the inventory and how economically have materials been used in construction.

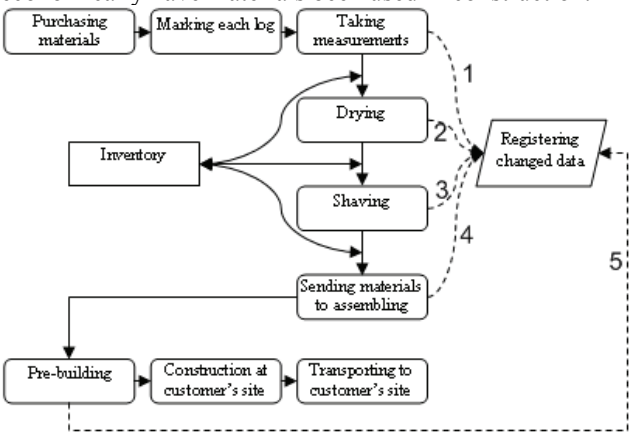

Figure 1: Log cabin building process

Depending on the predicted requirement for log cabins a truck load of materials is ordered after variable period of time. When acquired, logs usually are marked either by writing a number directly on the log or by attaching a plastic number tag, thus at every processing stage of logs their numbers are written down and subsequently entered in the accounting software. This process is time consuming and often it is difficult to supply up-to-date inventory information. The introduction of an RFID based material tracking system can reduce time required for data entry and processing up to 20 times at each material processing step. Data about material processing and flow has to be entered at multiple points marked with numbers 1 through 5 in the log cabin building process diagram (See Figure 1). If RFID would be used for marking the logs, then the information gathering at every next material processing step could be partly or completely automated. When taking log measurements (step marked 1), RFID can be used to store a logs measurements or to associate a log with its measurements stored into a database. This way it is possible to quickly access inventory state data. In combination with electronic measuring instruments the time necessary for this process can be reduced to a minimum and the accuracy of measurements increased.

3. DATA SECURITY ISSUES AND SOLUTIONS

The wireless communication abilities of RFID devices not only introduce benefits in process improvement, but also potential data misuse. As with RFID data is communicated over the air anyone can listen to the communications or unnoticed read and write data to RFID tags, thus it is important to use secure communication channels, to prevent unauthorized persons to gain access to data.

There are several malicious purposes, for what RFID can be misused: (i) *Unauthorized data altering* – the identification number of a tag is typically read-only data, but if other information like log measures are written on tags, then someone might alter it to gain financial benefit; (ii) *Counterfeit* – The U.S. example mentioned previously shows that even construction materials like wood are being counterfeited; (iii) *Sabotage*; (iv) *Competitive intelligence*. Other goals like person tracing and profiling, identity theft and financial fraud are possible to achieve using RFID, but these are not likely to occur in the case of log cabin inventory management (Pornieks, Ginters and Neumann 2007).

To protect an RFID system from these attacks it is necessary to ensure that only authorized persons have controlled access to the RFID tags. In current solutions on the market this issue is weakly supported, but several scientists have offered their data security solutions. In the following a list of criteria (**K**) is described that allows comparing these solutions. For the eligibility to criteria a solution can receive up to five points, depending on how well this solution satisfies the requirements. And for each criterion a weight (**W**) is assigned that shows how important it is to satisfy this criteria for the use in logistics. Thus a protocol can achieve a score (**S**) of maximum 100 points, that are calculated as follows:

$$S = \sum_{i=1}^{6} K_i \times W_i$$

The criteria taken in to account are: (i) *Tag cost* is an essential factor in the decision to use this technology or not, as it can have significant influence on the overall costs of business processes. If a protocol requires less on-tag resources the tag can be produced cheaper, therefore this criteria receives the weight=5; (ii) *Usability* receives w=3, because it is important to create an simple and cheap to setup RFID system, that can be easily aligned to required business processes, but this must only be done once; (iii) *Data protection* has w=2, as sensitive data rarely have to be stored on the tag itself, typically such data is stored in centralized databases, that are easier to control and protect. In this case the tag is only used to hold reference data; (iv) *Anti-counterfeit* receives w=5, because one must be able to correctly identify the producer of the material/product so the supplier is ensured that counterfeiters are not able illegally benefit from his effort in building customer relations or to damage his reputation with low quality goods. But the recipient can be sure to receive the expected quality and services; (v) *Privacy* is required to prohibit unauthorised analysis material movement. This feature is more important for tags identifying end-user products, but also businesses are not protected from privacy attacks, so it receives w=4; (vi) *Additional features* that protect data security are welcome, but not essentially important in the decision to use this protocol or not, therefore w=1.

The solution overview diagram (see Figure 2) displays the total performance of each protocol and the performance in each of the selected areas. The protocols are displayed as follows: 1-LMAP (Peris-Lopez 2006), 2-Supply Chain (Li and Ding 2007), 3-Tree Search (Molnar 2005), 4-PUF (Batina, Guajardo, Kerins, Mentens, Tuyls and Verbauwhede 2007), 5-ECC (Batina, Guajardo, Kerins, Mentens, Tuyls and Verbauwhede 2007), 6-AES (Aigner and Feldhofer 2005), 7-OHLCAP (Choi, Lee and Lee D.H., 2005), 8-TI PKI (Pearson 2006) and 9-Distance Bound (Reid 2007). For reference a column (Max) with the maximum possible scores in each area is added.

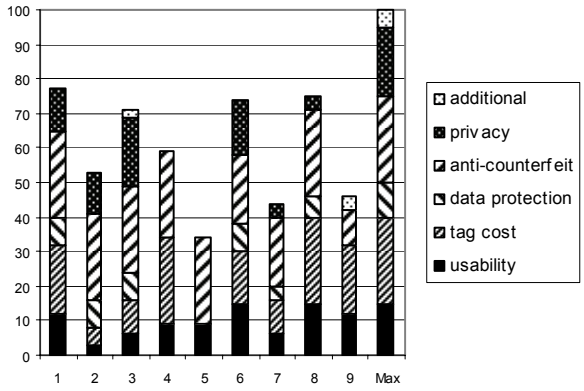

Figure 2: Solution performance overview diagram

The most promising protocol appears to be LMAP that requires quite low amounts of resources and offers protection against most attacks. It uses few simple binary calculation operations for cryptographic needs, but requires more space for the storage of secrets than most other protocols, but this solution also requires permanent online access to the database which is difficult or expensive to support in log cabin building processes, thus a solution with offline working capabilities like AES might be more feasible.

4. SIMULATION FOR EFFICIENCY

The LMAP protocol requires always an online connection with the database, this also means that the data gathered, with RFID devices is always up-to-date, but more initial investment is required to connect remote locations and the necessary RFID devices to the companies internal network. In some cases it is very difficult to supply a permanent and stable internet connection to guarantee the necessary data flow.

On the contrary the AES protocol is less secure, but allows working with the RFID devices, while not having a connection to the database, unfortunately this way data is sent to the database with a delay typically this would be on the end of the shift, when the responsible employee would setup a connection to the database and transfer new data to the database in a batch. In this case data that is required for planning further processes arrives hours later than with the LMAP protocol. Therefore it is necessary to understand how much the delay in data flow influences the production process.

To clarify which solution is better suited for the log cabin accounting processes two EXTEND models are created where one covering the LMAP solution, but the second – AES. And with both models simulations with identical input data are performed so that the efficiency of each security solution and data processing model can be compared.

The initial data can be divided in 3 groups. First of all the incoming material flow is determined by material purchase. In the current case the materials are supplied by two partners with each in average delivering one truck load every month. The dimensions and moisture of logs differs slightly in each load. The material processing time generally depends on the quantity of materials and the time needed to process one unit, which varies little. And finally the incoming orders for building new log cabins and availability of workers and working area determines the material usage in the current case up to 3 log cabins houses can be built simultaneously.

After each material processing step, data about the state of the materials is gathered (See Figure 3).

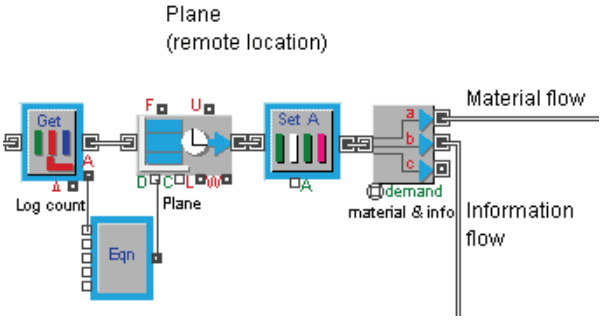

Figure 3: Information and material flow

And the use of the two different RFID protocols is simulated. In case of LMAP data like, the inventory state, is updated as soon as the information is available, but with AES information is updated with delay, at the end of shift (See Figure 4).

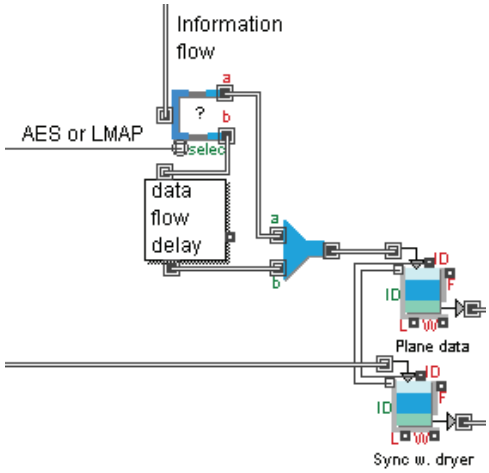

Figure 4: Information flow and synchronisation

The models have been verified and validated in a workshop together with industry experts. The models structure complies with the existing business processes. Process execution time corresponds to the measured real-world values. Statistical validation of the models has been conducted, by comparing the simulation results with mathematically calculated results. Data sets were evaluated using Kolmogorov-Smirnov test.

The analysis of both models shows that the LMAP solution overall would be more effective in data gathering and more secure, but it requires more initial investments to ensure uninterrupted reader connection to the database which becomes even more difficult when remote data gathering locations must be considered. Differences of both protocols do not show much influence on the

process in the current case, but it would be important where data is more often generated and processed.

5. CONCLUSIONS

While prices for RFID devices are falling the RFID technology becomes a more important part of logistics and supply chain. However the use of a wireless solution causes data security problems, but the solving of these must not reduce the usage efficiency of RFID systems. The proposed two level evaluations of information security techniques is a useful approach not only for log cabin builders, but as well for other RFID technology users.

When selecting a passive RFID communication protocol it's security capabilities, time the protocols requires for processing data and the cost of implementation and maintenance must be considered. The first evaluation level allows selecting an appropriate protocol for the necessary information security level taking in account also the cost of tags, but the second level (modeling) shows the influence of a protocol on business processes and data processing speed. With this information the feasibility of implementing a passive RFID system can be calculated.

REFERENCES

Aigner M., Feldhofer M., 2005, *Secure Symmetric Authentication for RFID Tags*, http://tcmc.tugraz.at/tcmc2005/PDF/20050228-IAIK-SecureAuthentication.pdf, [accessed 2007.09.11]

Batina L., Guajardo J., Kerins T., Mentens N., Tuyls P., Verbauwhede I., 2007, *Public-Key Cryptography for RFID-Tags*, PerCom Workshops, IEEE Computer Society, pages 217-222

Choi E. Y., Lee S.M., Lee D.H., 2005, *Efficient RFID Authentication protocol for Ubiquitous Computing Environment*, http://protocol.korea.ac.kr/~dhlee/papers/Efficient%20RFID%20Authentication%20protocol.pdf, [accessed 2007.09.11]

Cooper S., 2007, *Global Timber Smugglers-and How You Can Stop Them*, http://www.popularmechanics.com/science/earth/4215504.html, [accessed 2007.12.03]

Li Y., Ding X. , 2007, Protecting RFID communications in supply chains, ASIACCS, ACM, pages 234-241

Molnar D. et.al., 2005, *A Scalable, Delegatable Pseudonym Protocol Enabling Ownership Transfer of RFID Tags*, Selected Areas in Cryptography, Springer, pages 276-290

Pearson J., 2006, *RFID Tag Data Security Infrastructure: A Common Ground Approach for Pharmaceutical Supply Chain Safety*, http://whitepapers.zdnet.co.uk/0,1000000651,260270952p,00.htm, [accessed 2007.08.16]

Peris-Lopez P. et.al., 2006, *LMAP: A Real Lightweight Mutual Authentication Protocol for Low-cost RFID tags*, pphttp://events.iaik.tugraz.at/RFIDSec06/Program/papers/013%20-%20Lightweight%20Mutual%20Authentication.pdf, [accessed 25.11.2007]

Pornieks V., Ginters E., Neumann G., 2007, *RFID usage and data security*, ICTE in Regional Development, ISBN 9984-633-10-1.

Progress software, 2007, *Cambium-Forstbetriebe*, http://www.progress.com/openedge/customers/manufacturing/cambium/index.ssp, 2007.11.24

Reid J. et.al., 2007, *Detecting relay attacks with timing-based protocols*, ASIACCS, ACM, pages 204-213

AUTHORS BIOGRAPHY

Prof. Egils Ginters.is Director of Sociotechnical Systems Engineering Institute at the Vidzeme University College. Full time professor at the Vidzeme University College and working also for Riga Technical University. He is member of Institute of Electrical and Electronics Engineers (IEEE) and Information Systems Audit and Control Association (ISACA). Prof. Egils Ginters is member of the Board of Association of Computer Technologies of Latvia. He is an author of data processing systems designing methodology LISTechnology and more than 80 publications. Currently he is director of the master programme in Sociotechnical Systems Modeling.

Mag.Sc. Gunars Grundstoks has studied Possibilities of application of RFID technologies in the sphere of log–home manufacturing in his Master thesis. Gunars Grundstoks has professional experience with automating accounting processes for wood-processing and log cabin building industries. He is also Founder and CEO of IT House Ltd. which is one of the main software developers in Latvia for wood-processing and log cabin building industries.

Mag.Sc. Valdis Pornieks is a lecturer at Vidzeme University College and is responsible for the RFID laboratory of the Sociotechnical Systems Engineering Institute. He is also the co-founder and technical director of IT House Ltd. Valdis Pornieks is the author of 4 publications.