13

M2M in Agriculture – Business Models and Security Issues

S. Gansemer[1], J. Sell[1], U. Grossmann[1], E. Eren[1], B. Horster[2], T. Horster-Möller[2] and C. Rusch[3]

[1]University of Applied Sciences and Arts Dortmund, Dortmund, Germany
[2]VIVAI Software AG, Dortmund, Germany
[3]Claas Selbstfahrende Erntemaschinen GmbH, Harsewinkel, Germany
Corresponding author: S. Gansemer <sebastian.gansemer@fh-dortmund.de>

Abstract

Machine-to-machine communication (M2M) is one of the major innovations in the ICT sector. Especially in agricultural business with heterogeneous machinery, diverse process partners and high machine operating costs, M2M offers large potential in process optimization. Within this paper, a concept for process optimization in agricultural business using M2M technologies is presented using three application scenarios. Within that concept, standardization and communication as well as security aspects are discussed. Furthermore, corresponding business models building on the presented scenarios are discussed and results from economic analysis are presented.

Keywords: M2M, agriculture, communication, standardization, business case, process transparency, operation data acquisition, business model, security.

13.1 Introduction

Machine-to-machine communication (M2M) currently is one of the major innovations in the ICT sector. The agricultural sector is characterized by heterogeneous machinery, diverse process partners and high operational

Advances in Intelligent Robotics and Collaborative Automation, 295–312.

machinery costs. Many optimization solutions aim to optimize a single machine but not the whole process. This paper deals with improving the entire process chain within the agricultural area. In the first part of this paper, a concept for supporting process optimization in heterogeneous process chains in agricultural business using M2M communication technologies is discussed. The second part presents business cases for the proposed system and outcomes from economic analysis. In the third part last not least security aspects related to the proposed system are discussed.

13.2 Related Work

The application of M2M technology in agriculture is targeted by several other research groups. Moummadi et. al. [1] present a model for an agricultural decision support system using both multi-agent-system and constraint programming. The systems purpose is controlling and optimizing water exploitation in greenhouses.

Wu et. al. [2] present a number of models for M2M usage in different sectors such as utilities, security and public safety, tracking and tracing, telematics, payment, healthcare, remote maintenance and control and consumer devices. They discuss technological market trends and the influence of different industries on M2M applications.

An insurance system based on telematics technology is demonstrated by Daesub et. al. [3]. They investigate trends in insurance industry based on telematics and recommend a supporting framework.

A business model framework for M2M business models based on cloud computing is shown by Juliandri et. al. [4]. They identify nine basic building blocks for a business model aiming to increase value while reducing costs.

Gonçalves and Dobbelaere [5] discuss several business scenarios based on specific technical scenarios. Within the presented scenarios, the stakeholders assume different levels of control over the customer relationship and the assets determining the value proposition.

A model for software updates of mobile M2M devices is presented in [6]. They aim on low bandwidth use and avoidance of system reboot.

13.3 Communication and Standardization

The agricultural sector is characterized by heterogeneous machinery and diverse process partners. Problems arise from idle times in agricultural processes, suboptimal machine allocation and improper planning. Other problems

are generated by incompatibilities of machinery built by different manufacturers. Because of proprietary signals on machine buses not fitting on one another collaboration between machines may be inhibited [7, 8].

To support collaboration of heterogeneous machinery a standardized communication language is needed. Communication takes place either direct via machine to machine or via machine to cloud.

Sensors in machines record different parameters such as position, moving speed, mass and quality of harvested produce. These operational and machine logging data from the registered machines are synchronized between machines and finally sent via telecommunication network to a recording web portal. Data are stored within the portal´s database and are used for optimizing process chain or develop and implement business models based on that data. All data is sent through machine's ISO- and CAN-bus in proprietary syntax.

Within the concept, each machine uses a "black-box" which translates manufacturer specific bus signal data to a standardized data format. The concept is shown in Figure 13.1. Machines may be equipped with diverse numbers of sensors resulting in different numbers of signals available. The standard should cover most of those signals. However, due to the diverse machinery available, not every signal available on the machine can be supported within the proposed concept.

Within this paper, the concept of a portal (M2M-Teledesk) is presented suited for dealing with the problems mentioned above. The system's framework is shown in Figure 13.2. The black-boxes installed on each machine are interfaces between the machine's internal buses and the portal

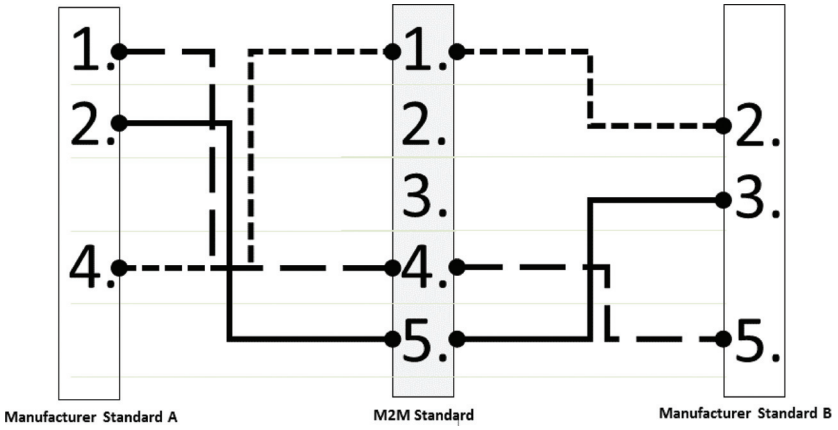

Figure 13.1 Synchronization of standards.

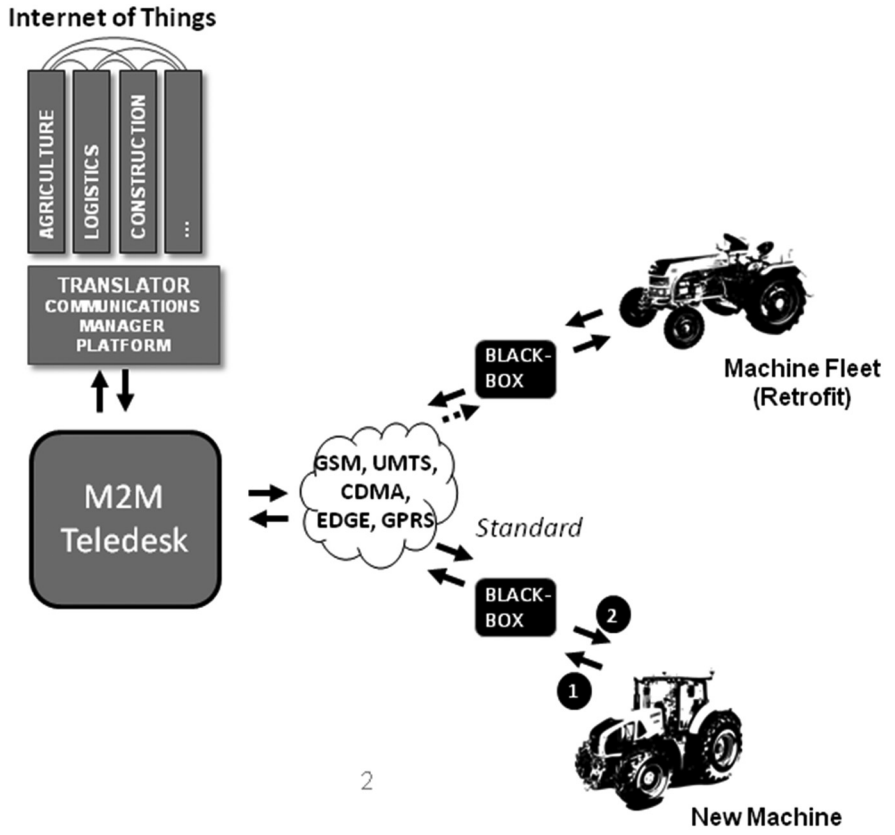

Figure 13.2 M2M teledesk framework [9].

(M2M-Teledesk). Black-boxes are equipped with mobile network communication interfaces for transferring data between machines among each other and between machines and the portal as well.

Every machine is set up with a black-box which reads internal buses and translates signals to the proposed open M2M standard, runs different applications and communicates data to and from the machine using WIFI or mobile data communication networks. The system uses a public key infrastructure for safety and trust reasons (see Section 13.7). Within the portal collected data is aggregated and provided to other analyzing and evaluating systems (e.g. farm management). Depending on the machine a full set or a subset of data specified in the standard can be used. Older machines may be retrofitted with a black-box providing only a subset of available data as a smaller number of sensors are available only.

The data is visualized within the portal and helps the farmer to optimize business processes to meet documentation requirements or to build data-based business models. Especially when it comes to complex and detailed records of many synchronized machines, the system shows its advantages.

Communication between machines takes place either directly from machine to machine or via a mobile communication network (e.g. GSM or UMTS). Within agricultural processes operating in rural areas, the availability of mobile communication networks is not always given. There are two strategies to increase the availability of network coverage:

- National roaming SIM cards;
- Femtocells.

With national roaming SIM cards being able to roam into all available networks, the availability of mobile network coverage can be increased, while with standard SIM cards only one network can be used in the home country [10]. National roaming SIM cards are operating in a country different from their home location (e.g. a spanish SIM card operating in Germany). The SIM card can roam into all available networks as long as issuing provider and network operator signed a roaming agreement. Although network coverage can be increased, a communication channel cannot be guaranteed.

With femtocells [2], dedicated base station is placed on the field where machines are operating. The concept is presented in Figure 13.3. Machines

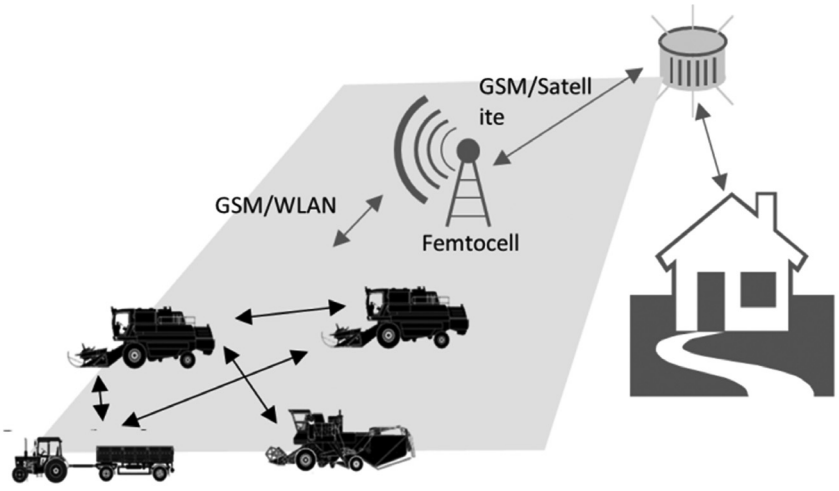

Figure 13.3 Femtocell communication in agriculture [9].

communicate to the base station e.g. via WLAN or GSM/UMTS, while base-station is connected to the portal by GSM/UMTS or satellite connection. The location of the femtocell base-station should be chosen in a way that coverage is given at every location within the corresponding area either via the femtocell or via direct connection to a mobile network. This strategy enables communication even without network coverage by the operator. However, the implementation effort is significantly higher than in case of using national roaming SIM cards.

13.4 Business Cases

The described system can be used in different manners. Three main business cases have been identified:

- Process Transparency (PT);
- Operation Data Acquisition (ODA);
- Remote Software Update (RSU).

Process transparency (PT) mainly focuses on in-time optimization of process chains, while ODA uses downstream analysis of data. Remote software update (RSU) aims to securely install applications or firmware updates on machines without the use of a service technician. These three business cases are described below in more detail.

13.4.1 Process Transparency (PT)

Processes in agricultural business are affected by several process participants. Furthermore, the used machines in many cases are operating with high costs. A visualization of an exemplary corn-harvesting process is presented in Figure 13.4. During the harvesting process, a harvester is e.g. cropping corn. Synchronously, a transport vehicle needs to drive in parallel to the harvester to transport the harvested produce. Machines involved in this sub-process need to be synchronized in real time. In case of the transport vehicle being filled up, it has to be replaced by another empty transport vehicle. Full transport vehicles make their way to e.g. a silo or a biogas power plant where the transport vehicle has to enter via a scale to measure the mass of the harvested produce. Furthermore, a quality check of the harvested produce is carried out manually.

This process may be optimized by the portal in different ways. Due to the registration of sensor data, the weighting and quality check part in the process may be skipped or reduced to spot checks if the customer deems the data within the system to be trustworthy. Furthermore, the data is visualized by the

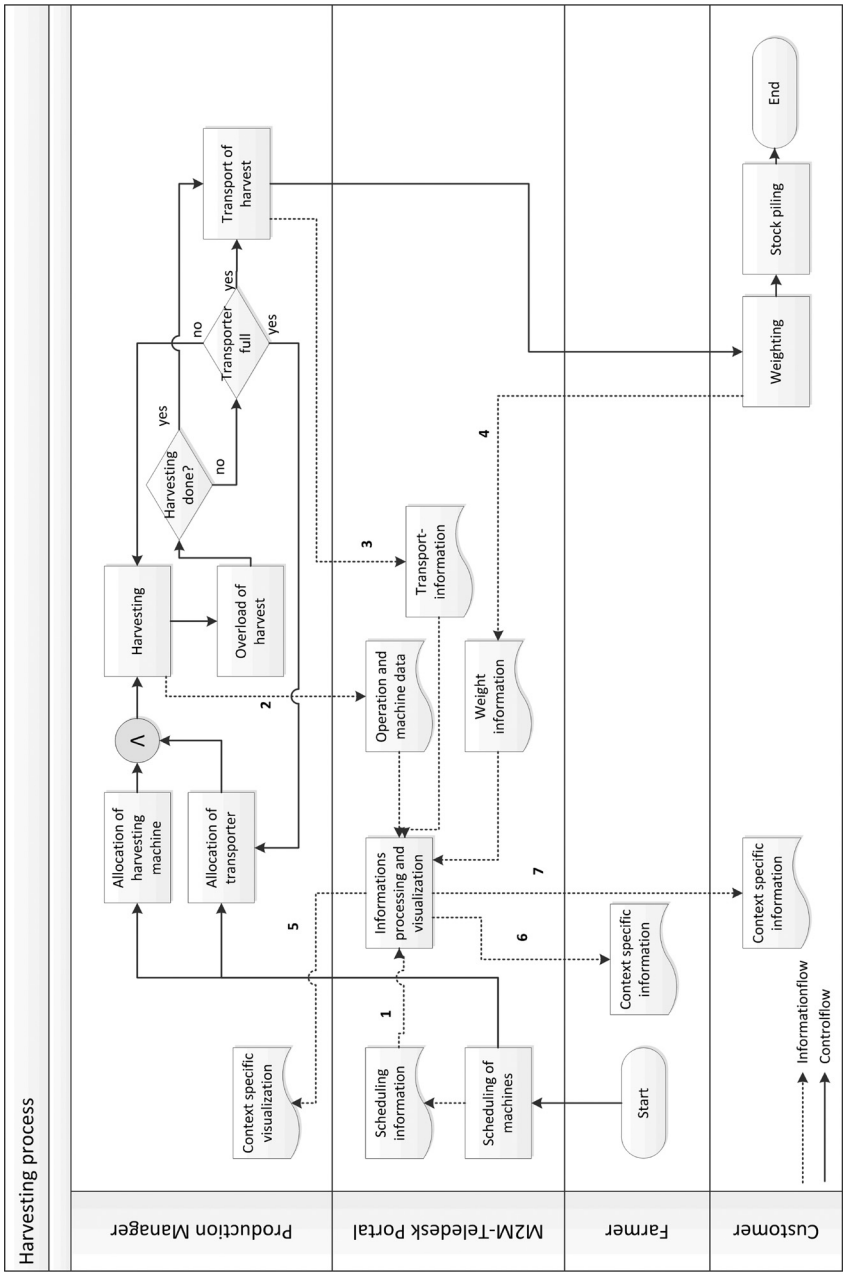

Figure 13.4 Information- and controlflow of scenario harvesting process.

portal to give the production manager the opportunity to optimize the process in near real-time. Before starting the process, a production plan is prepared by the production manager either manually with support by the system or automatically by the system. Within the plan, machines are allocated with time and position data. When the system registers a plan deviation, the plan is updated either manually or automatically. This approach allows reducing idle times saving costs and resources.

13.4.2 Operations Data Acquisition (ODA)

Within Operations Data Acquisition (ODA) scenario data gathered by the machine sensors is saved for downstream processing and analysis. While process transparency aims to synchronize process data in real-time to support process optimization, ODA data is gathered and sent to the server after the process is finished. Analysis is done e.g. to generate yield maps or to analyze machine behavior.

13.4.3 Remote Software Update (RSU)

The remote software update (RSU) process aims to remotely install software on a machine. Software update includes two sub scenarios, firmware upgrade and app-installation. App-installation means the installation of an additional piece of software from a third-party-software provider while firmware updates. The main aspect of software update is to ensure that the software is installed in a secure way, meaning that the machine proof to install software which comes from an authorized source and was not changed during network transport. Details on the security measures can be found in Section 13.7.

13.5 Business Models

Based on the scenarios and the data described above business and licensing models are developed. Figure 13.5 shows the value chain of M2M Teledesk consisting of six partners.

For all partners of the value chain business potential has been analyzed and is shown in Table 13.1. The table shows the partner's roles, the expected revenue and cost development and the resulting business potential.

Figure 13.5 Value chain of M2M-Teledesk [9].

Table 13.1 Revenue, costs and business potential for partners along M2M value chain

Partner	Role	Revenue Development (Per Unit)	Cost Development (Per Unit)	Business Potential
Module manufacturer	Manufacturer of black-box	Constant	Declining	+
Machine manufacturer	Manufacturer of machines	Progressive	Declining	++
Mobile network operator	Data transport, SIM management	Constant	Declining	+
3rd party software provider	Software developer, application provider	Constant/ progressive (depending on business model)	Depending on business model	+
Portal provider	Portal operator	Progressive	Declining	++

The module manufacturer produces the black-boxes (see Figure 13.2) built into the machines or used to retrofit older machines. Revenues for module manufacturers mostly come from black-box sales. Costs per unit are expected to decline with increasing number of sold units.

The machine manufacturer's revenues come from machine sales as well as services delivery and savings due to remote software updates. The cost of development is expected to be declining with the increasing number of sold units.

The mobile network operator's role is to deliver data through a mobile network. SIM card management may also be done by the network operator but can also be done by an independent partner. Revenues consist of fees for data traffic as well as service fees for SIM card supply and management. Additional costs for extra data volume over an existing network are very low.

Third-party software providers can be part of the value chain; however, this is not compulsory. They either supply an application bringing additional functions to the machinery or implement an own business model based on the data held in the portal.

The software is sold through the portal and is delivered to the machinery by the remote software update process described above. The revenues development per unit depends on the employed business model. When only software is sold, revenues per unit are constant. With additional business models, revenues may also develop progressively.

Costs are mostly one-time costs for software development as well as running costs for maintenance. However, additional costs may arise depending on the business model. The portal provider operates and manages the portal. Revenues consist of usage fees, revenues from third party app sales, fees for delivering software updates and other service fees. Costs are mainly for portal operation, support and data license fees. The end users' revenues come from savings due to increased process efficiency, while costs arise for additional deductions for machines, additional costs for higher skilled workforce, system usage fees and so on. Business potential is given for all partners involved in the value chain.

With applications developed by third-party software developers a variety of new business models can be implemented. One model is given by "pay-per-use" as well as "pay-how-you-use" insurance or leasing. Within this business model insurance or leasing companies are able to calculate insurance or leasing rates more adequate to risk depending on real-usage patterns. The insurance or leasing company is integrated in the value chain as a third-party software provider. For running the business model, data showing the usage pattern is needed. To gain this data, the third-party software provider needs to pay license fees.

13.6 Economic Analysis

Economic analysis of the system leads to a model consisting of linear equations. For visualizing the quantitative relations between different services, sub-services and partners of a so-called swimlane-gozintograph is used. Based on standard gozintograph methodology as described in [11] the resulting figure is adapted by including swimlane methodology [12] to show the involved partners. Figure 13.6 shows the corresponding swimlane-gozintograph. Columns represent the involved partners; transparent circles indicate different services delivered by the partners. Shaded circles represent business cases, i.e. services delivered externally.

The figure shows the relations between internal and external services and the share of each partner in the different business cases. From this gozintograph, mathematical equations can be derived, enabling the calculation of the gross margins for each business case.

From Figure 13.6, linear equations are derived, including transfer prices, amounts of service delivery and external sales prices for cost and gross margin calculation.

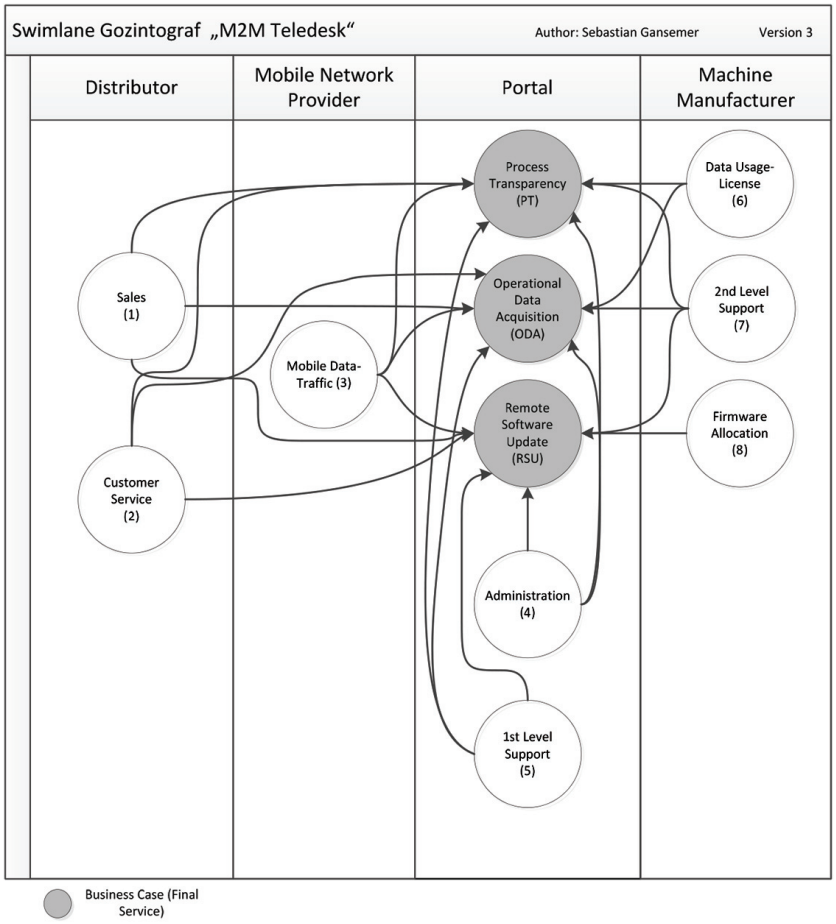

Figure 13.6 Service-links between delivering and receiving services.

Variable costs for the business cases can be calculated using Equation system (13.1).

$$\begin{aligned} c_1 &= a_{11} \cdot b_1 + a_{12} \cdot b_2 + \ldots + a_{1n} \cdot b_n \\ &\vdots \\ c_m &= a_{m1} \cdot b_1 + a_{m2} \cdot b_2 + a_{mn} \cdot b_n, \end{aligned} \tag{13.1}$$

where a_{ij} – amount of service j delivered for service i; b_j – transfer prices of service j; c_i – variable costs of finally receiving service i; m – number of finally receiving services; n – number of delivering services.

The system of linear equations yields relation matrix A=(a_{ij}) and transfer price vector B=(b_j). The vector C=(c_i) of variable costs can be represented by Equation (13.2).

$$\mathrm{C} = \mathrm{A} \cdot \mathrm{B}. \tag{13.2}$$

Using the vector D=(d_i) consisting of sales prices of finally receiving services Equation (13.3) leads to the vector M=(m_i) of gross margin per unit of all business cases, i.e. finally receiving services.

$$\mathrm{M} = \mathrm{D} - \mathrm{A} \cdot \mathrm{B}. \tag{13.3}$$

Figure 13.7 exemplifies the input matrix A and vectors B and D with estimated quantities. In matrix A, the rows indicate the business cases PT (row 1), ODA (row 2) and RSU (row 3). Columns represent delivering services indicated as white circles in Figure 13.6. The elements of vector B represent transfer prices of delivering services. Elements of the vector D represent sales prices of the three business cases.

The results of economic analysis are shown in Figure 13.8. Elements of the calculated vector C indicate variable costs of the three business cases. It

$$\mathrm{A} = \begin{pmatrix} 1 & 1 & 0.05 & 1 & 1 & 2 & 0 & 0 \\ 1 & 1 & 2.5 & 1 & 2 & 1 & 0.5 & 0 \\ 0 & 1 & 0.1 & 1 & 0.5 & 0 & 0 & 1 \end{pmatrix} \mathrm{B} = \begin{pmatrix} 50 \\ 25 \\ 240 \\ 12 \\ 11 \\ 150 \\ 150 \\ 0 \end{pmatrix} \mathrm{D} = \begin{pmatrix} 1000 \\ 1000 \\ 100 \end{pmatrix}$$

Figure 13.7 Relation matrix A, transfer price vector B and sales price vector D.

$$\mathrm{C} = \begin{pmatrix} 410 \\ 934 \\ 66.5 \end{pmatrix} \mathrm{M} = \begin{pmatrix} 590 \\ 66 \\ 33.5 \end{pmatrix}$$

Figure 13.8 Vector of variable costs C and vector of marginal return per unit M.

can be seen that the marginal return per unit is positive for all three business cases with the highest marginal return for business case Process Transparency.

13.7 Communication Security

Securing the communication channel against unauthorized access and manipulation is another important factor which has to be taken into account.

One has to consider the following communication scenarios: communication between machines and portal using mobile networks such as 3G/4G and WLAN, secure remote firmware update and covering dead spots.

The whole security concept is based on asymmetric encryption. Every participant in the communication chain (machines, machine manufacturer, M2M portal, provider) needs a key pair which should be created on the machine to keep the private key on the device.

This security concept was developed in the context of a bachelor thesis at the FH Dortmund [12]. The main target was the use of open and established standards [13, 14].

13.7.1 CA

The central instance of the security structure is a CA (Certificate Authority) which provides services like issuing certificates (by providing a CSR (Certificate Signing Request)), revoking certificates, checking certificates if they are rejected (through CRLs/OCSP). During the key creation process, a CSR is being created which will be passed to the PKI. The CSR is signed and the certificate is sent back to the device (machine).

13.7.2 Communicating On-the-Go

The communication between the machines and the portal is secured by means of a mutually authenticated HTTPS connection. The portal identifies itself to the machine by presenting its certificate and vice versa. During the initiation of the connection, every device has to check the presented certificate by the other part: 1) is the certificate signed by the M2M CA (this prevents man-in-the-middle-attacks)? If yes: 2) check the certificate of the counterpart against the CA if the certificate is revoked or not. This is done by using OCSP or CRLs (as a fallback in case OCSP is failing).

After the connection has been initiated, both partners can communicate securely, while the security of the underlying network(s) (like mobile 2G/3G, WLAN etc.) is no more important.

13.7.3 Covering Dead Spots

In case that a mobile communication is not possible due to lacking availability, the collected data has to be transferred using other methods. Here, other vehicles (such as transportation vehicles) have to deliver the data from the machine within the dead spot to areas with mobile network coverage from where they are sent to the portal. During the transportation, the data has to be secured against manipulation and unauthorized access.

Preparing a data packet for delivery involves the following steps: At first the data is encrypted using the portal's public key. In order to check if the public key is still valid, it is checked with the corresponding certificate against the CA (through OCSP/CRL). This prevents unauthorized access. In the next step, the signature of the encrypted data is created. Therefore, the checksum of the data is calculated and encrypted with the private key of the originating machine. Both the signature (encrypted checksum) and the encrypted data are sent to the vehicle.

The portal checks the signature by decrypting the checksum using the originating machine's public key (key/certificate is checked through OCSP/CRL) and by creating the checksum itself of the data package. If both checksums match, the data has not been manipulated and can be decrypted using the private key of the portal.

13.7.4 Securing WLAN Infrastructures

In the vicinity of a farm, a wireless LAN connection will be used instead of mobile network connection. The M2M project elaborated a reference WLAN network which can be installed on the farm premises. This network is designed and optimized for the M2M system. In order to guarantee that only authorized machines have access to the network, the authentication scheme is based on IEEE 802.1X with a RADIUS using AES/CCMP encryption (IEEE 802.11i RSN). Furthermore, a DHCP/DNS service is provided by the gateway which interconnects the network to the internet and acts as relay to the M2M portal. A machine connects to the M2M wireless network by using its X.509v2 certificate. The certificate is presented to the RADIUS server which performs checks (OCSP/CRL) against the CA whether it is revoked or not and whether the certificate is signed by the M2M CA. The machine itself has to check the RADIUS certificate whether it belongs to the M2M CA in order to avoid rogue access points. If all checks are passed successfully, the RADIUS server grants access to the network.

13.7.5 Firmware Update

It is necessary to periodically apply updates for the software systems on the machines. The updates are passed from the manufacturer of the machine through the portal to the destination machine.

Since the update packages may contain critical and confidential data, the provision of the update package has to be secured accordingly. Because of the file size (100MB and up), asymmetric encryption is not appropriate. Instead, a 256-bit symmetric AES key is generated and is used to encrypt the update. This key is secured using the public key encryption (after checking the corresponding certificate through OCSP/CRL). Here, the public key of the destination machine is used. In the next step, the signature of the encrypted update file is calculated by generating the hash value which then is encrypted with the private key of the manufacturer. Now the signature, the encrypted file and the encrypted AES key are sent to the destination machine.

On the latter, the signature is checked by generating the checksum of the encrypted file and by comparing it with the decrypted checksum. The checksum is decrypted with the public key of the manufacturer. The corresponding certificate has to be checked, too) checksum. If both checksums match, the update did not lose integrity. Finally, the AES key can be decrypt using the private key of the destination machine and the update can be decrypted (Figure 13.9).

13.8 Resume

This paper presents a concept for the optimization of process information chain to improve efficiency in agricultural harvesting process. Machine-to-machine communication plays a central role to synchronize data between diverse process partners.

The information gathered by sensors at agricultural machines plays the central role to build new business models. Business model analysis shows that all parties along the value chain gain good business potential. It has been shown that the three described business models can be operated with positive marginal return per unit under the assumptions made in the project.

However, security issues and business models play an important role for a successful system operation. With the described security measures, system operation can be done ensuring confidentiality, integrity as well as availability.

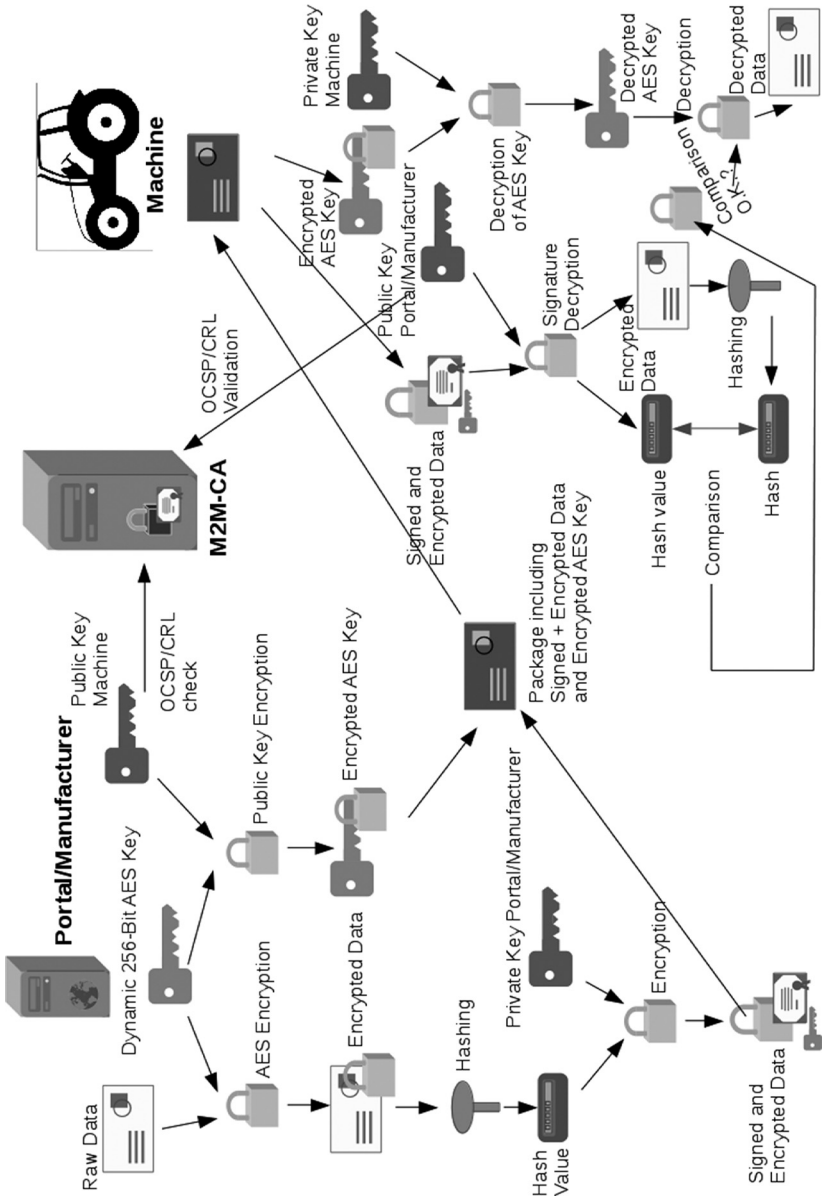

Figure 13.9 Large file encryption.

As the system is designed with an open and generic approach, adoption to other branches such as construction and the opportunity to bring in new functions and business models via third-party software brings additional market potential.

The concepts presented in this paper were developed within the project M2M-Teledesk. The project aims to implement a prototypical system following the concept described above.

13.9 Acknowledgement

The presented work was done in the research project "M2M-Teledesk" funded by the state government of North-Rhine-Westfalia and European Union Fund for regional development (EUROPÄISCHE UNION - Europäischer Fonds für regionale Entwicklung - Investition in unsere Zukunft). Project partners of M2M-Teledesk are University of Applied Sciences and Arts, Dortmund, VIVAI Software AG, Dortmund and Claas Selbstfahrende Erntemaschinen GmbH, Harsewinkel.

References

[1] K. Moummadi, R. Abidar and H. Medromi, 'Generic model based on constraint programming and multi-agent system for M2M services and agricultural decision support', In Multimedia Computing and Systems (ICMCS), 2011:1–6.

[2] G. Wu, S. Talwar, K. Johnsson, N. Himayat and K. Johnson, 'M2M: From Mobile to Embedded Internet', In IEEE Communications Magazine, 2011:36–42.

[3] Y. Daesub, C. Jongwoo, K. Hyunsuk and K. Juwan, 'Future Automotive Insurance System based on Telematics Technology', In 10th International Conference on Advanced Communication Technology (ICACT), 2008:679–681.

[4] A. Juliandri, M. Musida and Supriyadi, 'Positioning cloud computing in machine to machine business models', In Cloud Computing and Social Networking (ICCCSN), 2012:1–4.

[5] V. Goncalves and P. Dobbelaere, 'Business Scenarios for Machine-to-Machine Mobile Applications', In Mobile Business and 2010 Ninth Global Mobility Roundtable (ICMB-GMR), 2010.

[6] Y. Chang, T. Chi, W. Wang and S. Kuo, 'Dynamic software update model for remote entity management of machine-to-machine service capability', In IET Communications Journal, 2012.

[7] S. Blank, G. Kormann and K. Berns, 'A Modular Sensor Fusion Approach for Agricultural Machines', In XXXVI CIOSTA\& CIGR Section V Conference, Vienna, 2011.

[8] M. Mau, 'Supply Chain Management in Agriculture - Including Economics Aspects like Responsibility and Transparency', In X EAAE Congress Exploring Diversity in European Agriculture, 2002.

[9] S. Gansemer, U. Grossmann, B. Horster, T. Horster-Moeller and C. Rusch, 'Machine-to-machine communication for optimization of information chain in agricultural business', In 7th IEEE International Conference on Intelligent Data Acquisition and Advances Computing Systems, Berlin, 2013.

[10] K. Johansson, 'Cost efficient provisioning of wireless access: Infrastructure cost modeling and multi-operator ressource sharing', Thesis KTH School of Electrical Engineering, Stockholm, 2005.

[11] A. Vazsonyi, 'The use of mathematics in production and investory control', Management Science, 1 (1), Jan. 1955.

[12] R.K. Ko, S. S. G. Lee and E. W. Lee, 'Business process management (BPM) standards: a survey', Business Process Mansgement Journal, 15(5):744–791, 2009.

[13] J. Sell, 'Konzeption einer Ende-zu-Ende Absicherung für eine M2M-Telematik Anwendung für die Firma Claas', Thesis FH Dortmund, Dortmund, 2013.

[14] E. Eren and K. Detken, 'Mobile Security. Risiken mobiler Kommunikation und Lösungen zur mobilen Sicherheit', Wien, Carl Hanser Verlag, 2006.

[15] E. Eren and G. Aljabari, 'Virtualization of Wireless LAN Infrastructures', In 6th IEEE Workshop on Intelligent Data Acquisition and Advanced Computing Systems, Prague, 2011.